Buat paper dgn tema Proses Asesmen Resiko. Dengan ketentuan:

- Minimum kata 2000
- Struktur paper: Abstrak, Pendahuluan, Pembahasan, Kesimpulan, Dafar Pustaka

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **DITA RAHMAWATI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa orang untuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci: *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada website Hyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

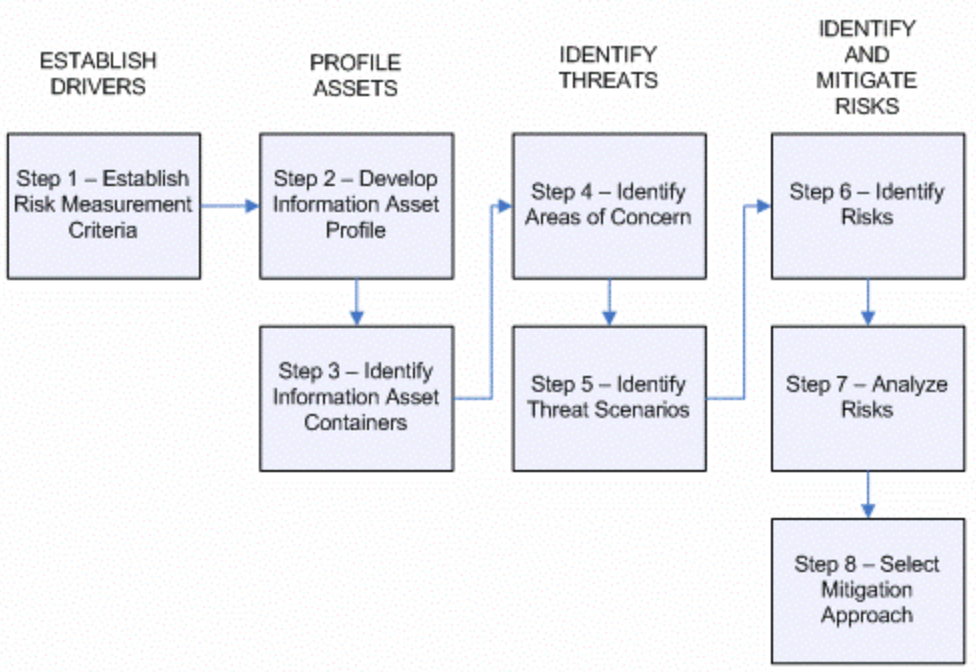
Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi. (Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang mengkontak calon pelamar perusahaan tersebut dan data harus diamankan	

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi

dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	**Area of Concern**
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**
Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	***Risk***			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1), 43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8 November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

Contoso

REVOLUSI INDUSTRI 4.0 : PELUANG DAN TANTANGAN BAGI MASYARAKAT MILENIAL

Contoso

KELOMPOK 3
RAJU SEPTA WIJAYA
ABI DAUD YUSUF
EVAN APRIADI D
RIAN AMANDA
ARVIAN SAPUTRA

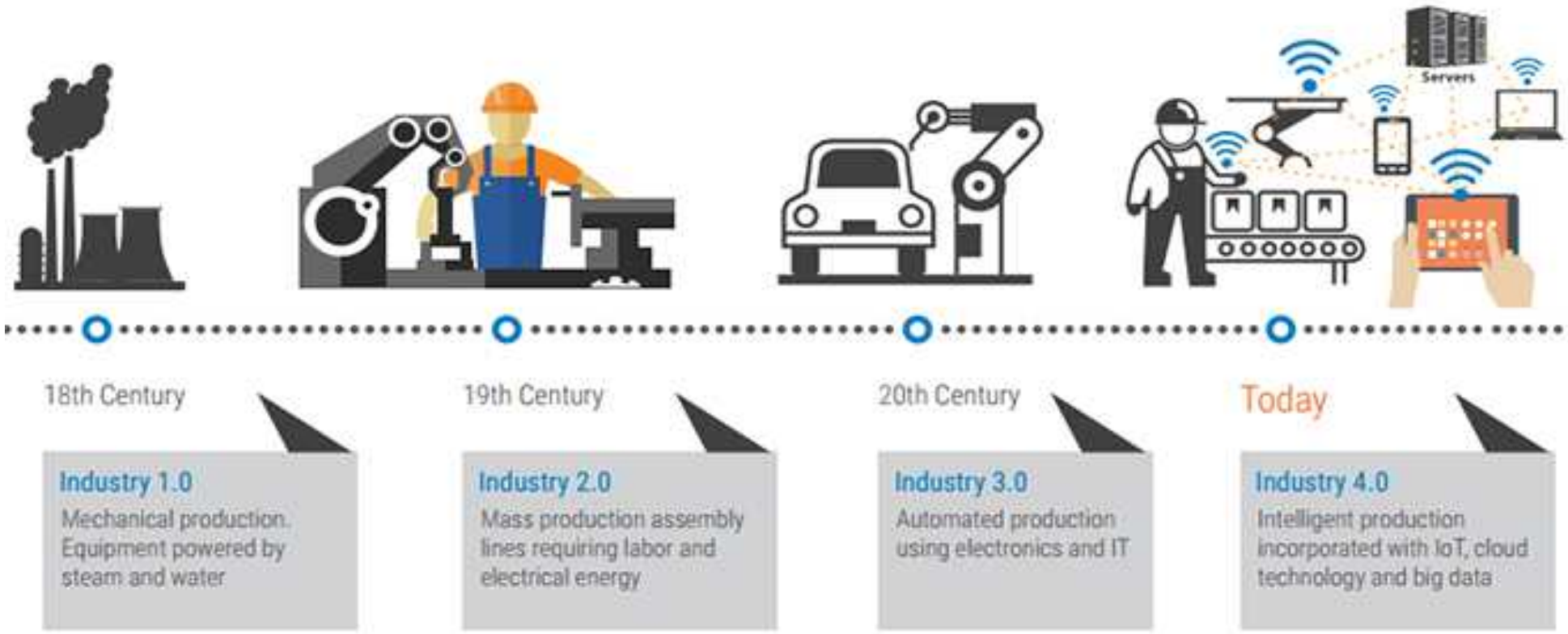
APA ITU REVOLUSI INDUSTRI 4.0?

Prof Schawab (2017) menjelaskan revolusi industri 4.0 telah mengubah hidup dan kerja manusia secara fundamental. Berbeda dengan revolusi industri sebelumnya, revolusi industri generasi ke-4 ini memiliki skala, ruang lingkup dan kompleksitas yang lebih luas. Bidang-bidang yang mengalami terobosoan berkat kemajuan teknologi baru diantaranya (1) robot kecerdasan buatan (*artificial intelligence robotic*), (2) teknologi nano, (3) bioteknologi, dan (4) teknologi komputer kuantum, (5) blockchain (seperti bitcoin), (6) teknologi berbasis internet, dan (7) printer 3D.

APA ITU REVOLUSI INDUSTRI 4.0?

Revolusi industri mengalami puncaknya saat ini dengan lahirnya teknologi digital yang berdampak masif terhadap hidup manusia di seluruh dunia. Teknologi internet yang semakin masif tidak hanya menghubungkan jutaan manusia di seluruh dunia tetapi juga telah menjadi basis bagi transaksi perdagangan dan transportasi secara online. Munculnya bisnis transportasi online seperti Gojek, Uber dan Grab menunjukkan integrasi aktivitas manusia dengan teknologi informasi dan ekonomi menjadi semakin meningkat.

Contoso



GAMBAR 1. REVOLUSI INDUSTRI 4.0 (SUMBER: WWW.KOMPASIANA.COM)

ERA DISRUPSI

Seperti yang disampaikan oleh Presiden Joko Widodo, revolusi industri 4.0 telah mendorong inovasi-inovasi teknologi yang memberikan dampak disrupsi atau perubahan fundamental terhadap kehidupan masyarakat. Kita menyaksikan pertarungan antara taksi konvensional versus taksi online atau ojek pangkalan vs ojek online. Dampaknya, publik menjadi lebih mudah untuk mendapatkan layanan transportasi dan bahkan dengan harga yang sangat terjangkau. layanan ojek online tidak sebatas sebagai alat transportasi alternatif tetapi juga merambah hingga bisnis layanan antar (*online delivery order*). Dengan kata lain, teknologi online telah membawa perubahan yang besar terhadap peradaban manusia dan ekonomi.

Contoso

PELUANG

Revolusi industri 4.0 membuka peluang yang luas bagi siapapun untuk maju. Teknologi informasi yang semakin mudah terakses hingga ke seluruh pelosok menyebabkan semua orang dapat terhubung didalam sebuah jejaring sosial. Informasi yang sangat melimpah ini menyediakan manfaat yang besar untuk pengembangan ilmu pengetahuan maupun perekonomian. *Karakteristik informasi sebagai kekayaan menunjukkan bahwa informasi yang diterima dan dikuasai seseorang dapat dimanfaatkan untuk sarana akumulasi kekayaan atau sumber komersialisasi. Dalam konteks ini, alumni atau mahasiswa dapat mempromosikan hasil kreasinya kepada publik melalui jejaring media social.*

Contoso

PELUANG

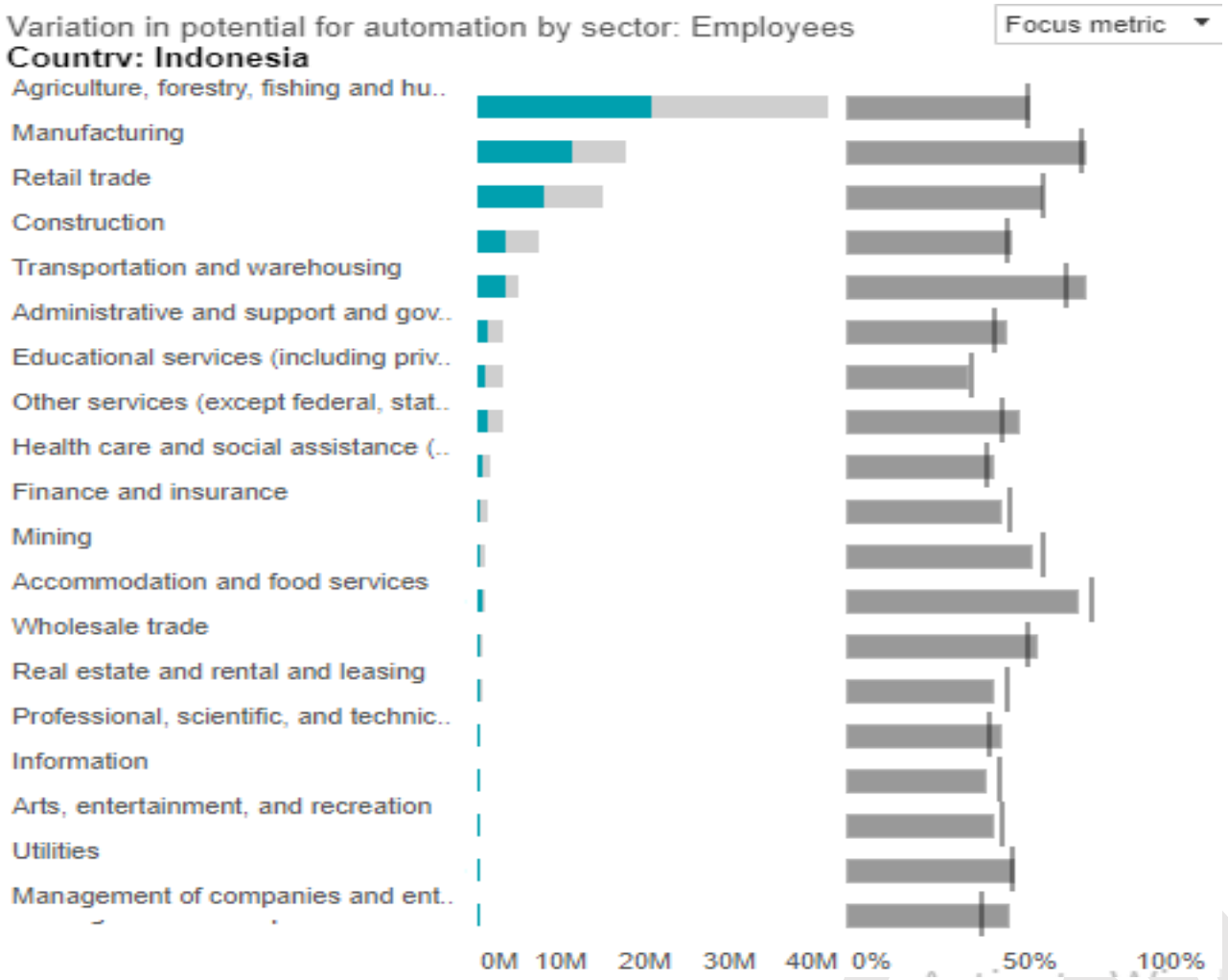
Kedua, satu dari empat orang mengakui durasi onlinenya lebih banyak daripada durasi tidurnya dalam setiap harinya. Ketiga, 1.500 responden di Inggris menghabiskan waktunya dengan bermedia sosial selama 62 juta jam per hari. Keempat, perempuan lebih sering berselancar di facebook daripada laki-laki. Kelima, tingkat kecanduan terhadap media sosial seperti twitter dan facebook lebih tinggi daripada merokok (sumber: http://www.beritasatu.com/gaya-hidup/ 232713-8-fakta-ketergantungan-pada-teknologi.html). Saat ini pasar atau toko secara fisik tidak lagi populer. Disamping ongkos pembangunan atau sewanya mahal, pasar konvensional makin sulit dijangkau.

TANTANGAN

Revolusi industri generasi empat tidak hanya menyediakan peluang, tetapi juga tantangan bagi generasi milineal. Kemajuan ilmu pengetahuan dan teknologi sebagai pemicu revolusi indutri juga diikuti dengan implikasi lain seperti pengangguran, kompetisi manusia vs mesin, dan tuntutan kompetensi yang semakin tinggi. Menurut Prof Dwikorita Karnawati (2017), revolusi industri 4.0 dalam lima tahun mendatang akan menghapus 35 persen jenis pekerjaan. Dan bahkan pada 10 tahun yang akan datang jenis pekerjaan yang akan hilang bertambah menjadi 75 persen. Hal ini disebabkan pekerjaan yang diperankan oleh manusia setahap demi setahap digantikan dengan teknologi digitalisasi program. Dampaknya, proses produksi menjadi lebih cepat dikerjakan dan lebih mudah didistribusikan secara masif dengan keterlibatan manusia yang minim,

TANTANGAN

- Gambar 2 menunjukkan bahwa lapangan pekerjaan yang potensial diotomatisasikan diantaranya usaha pengolahan (manufaturing), perdagangan ritel, transportasi dan pergudangan, tenaga administrasi, konstruksi, layanan makanan dan akomodasi, pertanian, perikanan, dan kehutanan, serta layanan kesehatan dan keuangan/asuransi. Dengan demikian, revolusi industri dapat mengancam makin tingginya pengangguran di Indonesia.



GAMBAR 2. JENIS PEKERJAAN YANG POTENSIAL DIOTOMATISASIKAN (SUMBER: HTTPS://PUBLIC.TABLEAU.COM/PROFILE/MCKINSEY.ANALYTICS#!/VIZHOME/INTERNATIONAL AUTOMATION/ WHEREMACHINESCANREPLACE HUMANS)

Contoso

TANTANGAN

Namun demikian, bidang pekerjaan yang berkaitan dengan keahlian Komputer, Matematika, Arsitektur dan Teknik akan semakin banyak dibutuhkan. Bidang-bidang keahlian ini diproyeksikan sesuai dengan tuntutan pekerjaan yang mengandalkan teknologi digital. Situasi pergeseran tenaga kerja manusia ke arah digitalisasi merupakan bentuk tantangan yang perlu direspon . terutama penguasaan teknologi komputer, keterampilan berkomunikasi, kemampuan bekerjasama secara kolaboratif, dan kemampuan untuk terus belajar dan adaptif terhadap perubahan lingkungan.

KESIMPULAN

Revolusi industri saat ini memasuki fase keempat. Perkembang ilmu pengetahuan dan teknologi yang sangat pesat memberika dampak yang besar terhadap kehidupan manusia. Banyak kemudahan dan inovasi yang diperoleh dengan adanya dukungan teknologi digital. Layanan menjadi lebih cepat dan efisien. Namun demikian, digitalisasi program juga membawa dampak negatif. Peran manusia setahap demi setahap diambil alih oleh mesin otomatis. Akibatnya, jumlah pengangguran semakin meningkat. Hal ini tentu saja akan menambah beban masalah lokal maupun nasional

Contoso

THANK YOU

Analisis Resiko Pada Akademik Management System STKIP Muhammadyah Bangka Belitung

Yuniarti Denita Sari[1], Zena Lusi[2], Reni Septiyanti[3], Anggari Ayu P[4], Gina Agiyani[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di STKIP Muhammadyah Bangka Belitung. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.
Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. STKIP Muhammadyah Bangka Belitung merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan

aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan STKIP Muhammadyah Bangka Belitung. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di STKIP Muhammadyah Bangka Belitung. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan

bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah

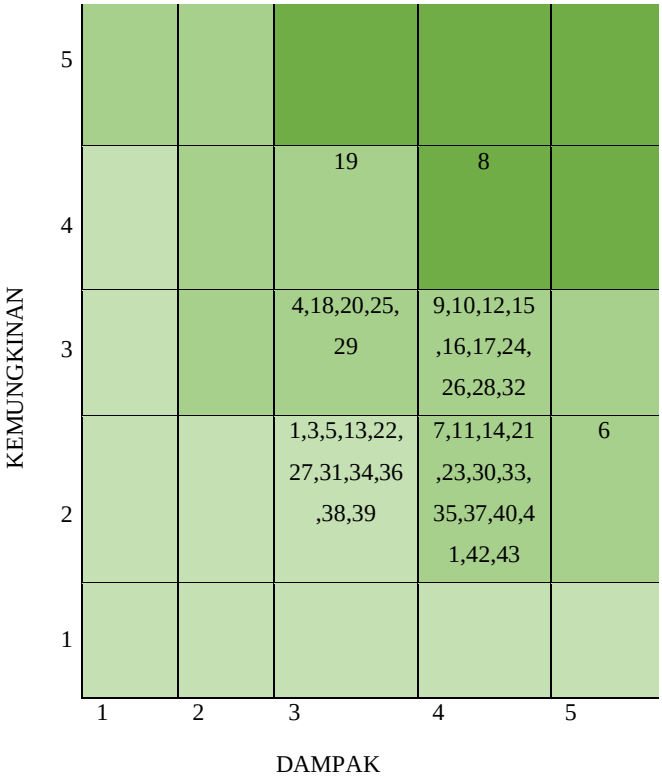
ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang

memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low /	1	Resiko Kerusakan akibat bencana alamt	NTP Server

Rendah)		seperti kebakaaran banjir, gempa	
	2	Pencurian Perangkat	NTP Server
	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya

merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dan lain-lain. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1. Apa pemicu terjadinya database server down pada sistem AMS?
2. Seberapa sering database server down tersebut terjadi pada sistem AMS?
3. Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

a) Overheat
b) Overcapacity
c) Overload
d) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
    - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin

sehingga perangkat terhindar dari resiko akibat overheat.

- Menghilangkan log yang menggunakan kapasitas yang besar
- Melakukan restart database service.
- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-

manajemen.[Accessed 16 November 2014].
[9] [Online].Available:http://dosen.guf ron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].
[10] [Online].Available:http://fisipuin.sa tugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.aca demia.edu/5170798/Uji_Validitas_ Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri0 1.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed 25 Februari 2015].
[15] [Online].Available:https://avicenna edu.wordpress.com/2013/03/26/resi komanajemen-risk-management/. [Accessed 10 Juni 2015].

RISK ASSESSMENT PADA MANAJEMEN RESIKO PENERAPAN TEKNOLOGI CLOUD COMPUTING BAGI PEMERINTAH DAERAH

Abstrak

Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus bermunculan. Adanya teknologi *Cloud Computing* memberikan harapan untuk mengoptimalkan layanan TI, infrastruktur TI, dan biaya. Berdasarkan Inpres No. 3/2003 tentang Kebijakan dan Strategi Nasional tentang Pengembangan e-Government, ada ketertarikan dari pemerintah untuk mengadopsi teknologi *Cloud Computing* ini. Dengan beragamnya infrastruktur dan sumber daya TI di daerah, perlu dilakukan analisis menyeluruh, misalnya analisis terhadap manajemen resiko sebelum pemerintah benar-benar akan mengadopsi dan menerapkan teknologi baru ini. Penilaian resiko atau *Risk Assessment* adalah salah satu langkah awal yang bisa dilakukan. Tujuannya adalah untuk mengidentifikasi resiko-resiko yang mungkin muncul dalam penerapan teknologi *Cloud* ini. Dengan mengacu pada *Risk Management Guide for Information Technology Systems* yang dikembangkan oleh *The National Institute of Standards and Technology* (NIST), diharapkan dalam makalah ini menghasilkan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud*.

Kata kunci : Teknologi *Cloud Computing*, Manajemen Resiko, *Risk Assessment*, NIST

1. Pendahuluan

Peran Teknologi Informasi (TI) dalam organisasi saat ini sangat penting sekali, dimana tingkat ketergantungan dunia usaha, badan-badan pemerintahan, dan organisasi, terhadap TI semakin tinggi. TI digunakan sebagai sarana untuk meningkatkan keunggulan kompetitif suatu organisasi melalui efektifitas dan efisiensi dalam otomasi, pengolahan, dan manipulasi data. Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus

bermunculan. Hal ini dibuktikan dengan munculnya berbagai alternatif teknologi yang bisa di adopsi untuk mencapai tujuan organisasi yaitu mempercepat dan mempermudah pekerjaan, misalnya di bidang pemerintahan telah mengadopsi aplikasi *e-Government* yang memanfaatkan jaringan internet dalam mendukung proses bisnis pemerintahan dan layanan publik.

Adanya Inpres No. 3/2003 tentang "Kebijakan dan Strategi Nasional tentang Pengembangan e-Government" yang bertujuan : Pengembangan e-government merupakan upaya untuk mengembangkan penyelenggaraankepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup 2 (dua) aktivitas yang berkaitan yaitu: 1) pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis; 2) pemanfaatan kemajuan teknologi informasi agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat di seluruh wilayah negara [1].

Cloud Computing adalah teknologi bidang TI yang memanfaatkan jaringan internet berupa model komputasi dimana sumberdaya-sumberdaya seperti *storage*, *processor*, *network*, dan *software* menjadi abstrak dan dijadikan sebagai layanan di jaringan menggunakan pola *remote access*. Konten yang ditawarkan seperti *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS) menjadi solusi TI yang praktis dan ekonomis. Sifat jangkauan layanan terbagi menjadi *Public Cloud*, *Private Cloud*, dan *Hybrid Cloud*. Ini adalah salah satu inovasi bidang TI terkini yang sejak tahun 2005 di tingkatkan kemampuannya sehingga bisa mendukung aplikasi e-Government dan diharapkan dengan mengadopsi teknologi ini untuk bidang pemerintahan dapat mengurangi biaya investasi TI, meningkatkan produktivitas pegawai, dan meningkatkan pelayanan pemerintah kepada masyarakat sekaligus mampu menyelaraskan proses bisnis dengan unit pemerintahan lainnya sehingga tercipta efektifitas dan efisiensi operasional pemerintahan. Keuntungan yang dapat diperoleh bagi pemerintah dalam mengadopsi *Cloud Computing* adalah ***A clean government with no corruption*** dimana Sistem SOA (*Service Oriented Architecture*) pada *cloud computing* yang memungkinkan kolaborasi otomatis di antara *software* yang dimiliki

dunia bisnis dengan *software* yang dimiliki pemerintah memungkinkan semua transaksi yang berhubungan dengan pemerintah dilakukan tanpa campur tangan manusia seperti perhitungan dan pembayaran pajak. Hal ini akan menghilangkan korupsi yang biasanya bisa terjadi karena terlibatnya begitu banyak manusia atau petugas didalam proses tersebut, selain itu keuntungan lainnya bagi pemerintah adalah ***A more responsive government services*** dimana setiap warga negara bisa mengakses pelayanan secara *online* dari mana dan kapan saja sehingga dapat meningkatkan kualitas pelayaran pemerintah.

Dengan adanya Inpres tersebut diatas semakin menguatkan alasan perusahaan layanan *Information Communication Technology* (ICT) tanah air untuk menggarap dan memberikan layanan *Cloud Computing* untuk pemerintahan, salah satunya adalah Telkom, perusahaan BUMN yang bergerak di bidang telekomunikasi. Melalui layanan G-Cloud, Telkom berharap dapat membantu efektifitas dan efisiensi operasional pemerintahan. G-Cloud merupakan sebuah layanan ICT yang bersifat *complete*, *affordable* dan *simple* yang menyediakan media untuk mengkolaborasikan melalui Telkom Collaboration antara modul aplikasi e-Government dan Portal Pemerintahan dalam model *Cloud Computing*. G-Cloud dilengkapi dengan 12 aplikasi e-Goverment penyelenggaraan pemerintahan di daerah yang telah memenuhi kriteria yang ditetapkan Menkominfo. Telkom menargetkan layanan G-Cloud meliputi 87 kota, 348 kabupaten, 5.224 kecamatan dan 6.890 kelurahan di Indonesia [2]. Berdasarkan informasi dalam Konferensi e-Indonesia Initiatives (e-II) Forum VII 2011 yang bertempat di kampus ITB tanggal 14-15 Juni 2011, pemerintah Jawa Barat adalah salah satu provinsi di Indonesia yang akan ikut mengadopsi layanan ini.

2. Permasalahan

Meskipun pemerintah daerah sudah menetapkan tujuannya untuk mengadopsi teknologi *cloud*, perlu disadari bahwa adopsi yang dilakukan tidak semudah yang dibayangkan. Perlu pertimbangan dan analisis menyeluruh mengenai adopsi ini karena adopsi teknologi *cloud* akan melibatkan pihak ketiga (*outsourcing*) sebagai penyedia layananan. Sifat dari layanan yang diberikan yaitu *multi-tenant* maka akan ada banyak pelanggan dalam satu *platform* sehingga kemampuan untuk kustomisasi akan menjadi terbatas.

Implementasi *Cloud Computing* memiliki keuntungan dan juga memiliki resiko yang harus dihadapi saat implementasi. Pihak yang terkait dan terlibat implementasi *cloud* perlu melakukan serangkaian tindakan yang mendukung keberhasilan penerapan *cloud computing* di organisasi. Aspek-aspek resiko yang mungkin timbul saat implementasi *cloud* seperti *Service Level*, *Privacy*, *Compliance*, *Data Ownership*, *Data Mobility* perlu dikelola dengan baik melalui manajemen resiko.

Oleh karena itu dalam makalah ini akan dibahas mengenai :

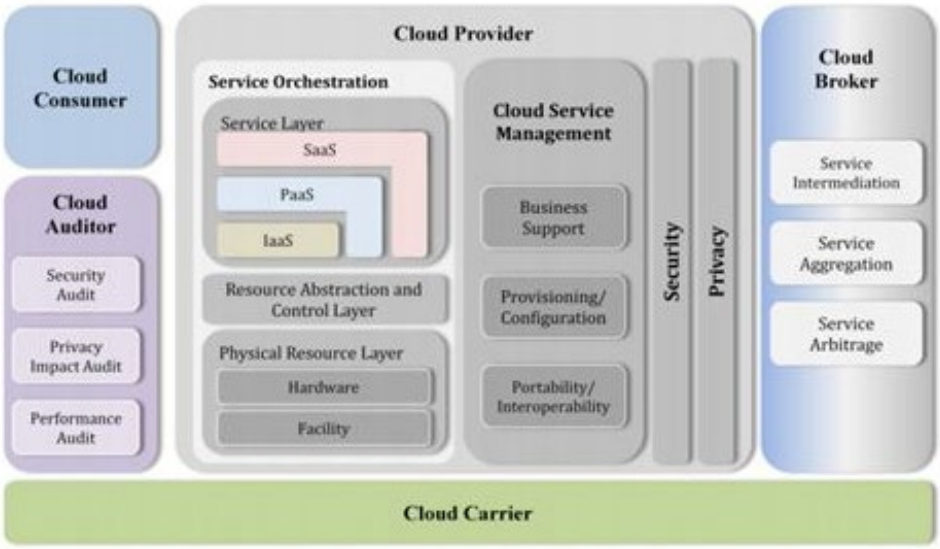
- Melakukan *Risk Assessment* atau penilaian resiko terhadap penerapan teknologi *Cloud Computing* bagi pemerintahan daerah menggunakan rekomendasi penilaian resiko yang disarankan oleh *National Institue of Standards and Technology* (NIST).
- Mendefinisikan karakteristik sistem pada teknologi *Cloud*.
- Melakukan identifikasi ancaman yang mungkin muncul saat implementasi teknologi *Cloud*.
- Melakukan identifikasi kelemahan dari teknologi *Cloud*.
- Memberikan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud*.

3. Landasan Teori

Dalam landasan teori pada makalah ini akan dijelaskan secara ringkas mengenai materi yang terkait dengan topik makalah yaitu *Cloud Computing*, *Manajemen Resiko*, dan *Risk Assessment*.

3.1 *Cloud Computing*

Cloud Computing di definisikan sebagai sebuah model yang memungkinkan kenyamanan, akses on-demand terhadap sekumpulan sumber daya komputasi (seperti jaringan, server, media penyimpanan, aplikasi, dan layanan komputasi) yang konfigurasinya dapat dilakukan dengan cepat dan hanya memerlukan sedikit usaha untuk mengelola dan berhubungan dengan penyedia layanan [3].

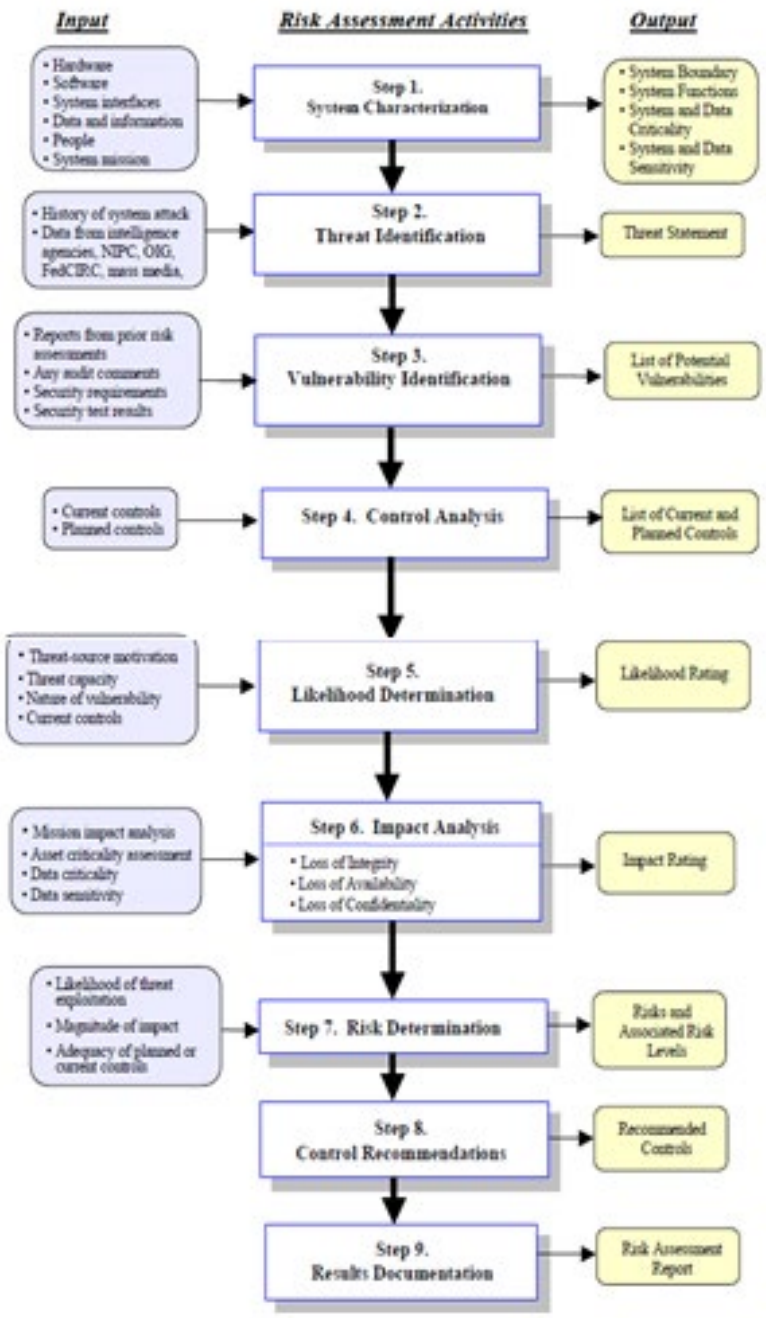


Gambar 1. Arsitektur Cloud Computing

3.2 Manajemen Resiko

Secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan. Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko [4].

Manajemen Resiko terdiri dari 3 proses yaitu, 1) *Risk Assessment*, 2) *Risk Mitigation*, 3) *Evaluation And Assessment*. Manajemen resiko adalah proses yang dilakukan para Manajer TI untuk menyeimbangkan kegiatan operasional dan pengeluaran biaya keuangan, dalam mencapai keuntungan dengan melindungi sistemIT dan data yang mendukung misi organisasinya [5].



Gambar 2. Aktifitas Risk Assessment

3.3 *Risk Assessment*

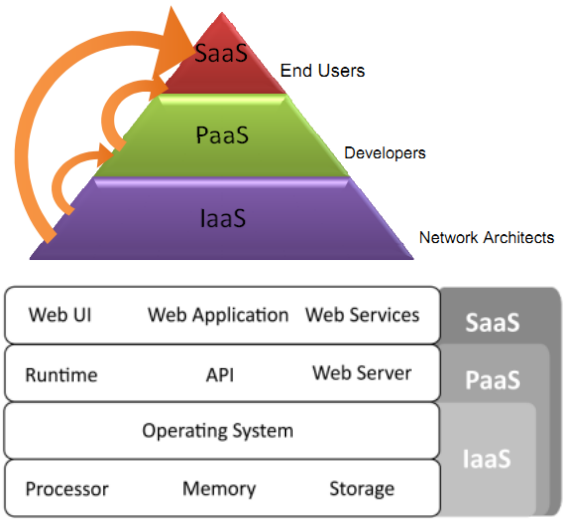
Risk Assessment atau Penilaian Resiko adalah proses pertama yang harus dilakukan dalam metodologi manajemen resiko. Risk Assessment digunakan untuk menentukan ancaman potensial dan resiko. Hasilnya adalah identifikasi kendali yang sesuai untuk mengurangi atau menghilangkan resiko. Proses ini terdiri dari 9 langkah, seperti yang diperlihatkan pada gambar 2 [5].

4. Pembahasan

Dalam pembahasan makalah ini, sebagaimana yang dijelaskan sebelumnya yaitu penilaian resiko akan mengikuti langkah-langkah yang disarankan oleh NIST, dengan pembahasan sebagai berikut :

4.1 *System Characterization*

Untuk menetapkan karakteristik sistem *Cloud Computing*, maka perlu dilihat terlebih dahulu dari layanan yang diberikannya yaitu *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS). IaaS berisi perangkat keras (Processor, memory, storage) dan sistem operasi yang merupakan antarmuka antara CPU dengan perangkat menjadi sebuah paket layanan. Layanan ini digunakan oleh konsumen melalui jaringan internet secara remote. PaaS memungkinkan developer untuk membangun suatu aplikasi diatas suatu platform yang dapat dikostumisasi sehingga spesifikasi perangkat Client tidak menjadi masalah untuk membangun dan menjalankan aplikasi dengan performansi apapun. SaaS merupakan layanan dimana pengguna dapat mengeksekusi suatu aplikasi tanpa perlu menginstal aplikasi tersebut, aplikasi yang dibutuhkan telah tersedia di vendor dan dapat diakses melalui jaringan internet [6].



Gambar 3. Services Model dan Layer

Dari layanan yang dapat diberikan oleh *Cloud* maka dapat diketahui karakteristik dari sistem yaitu [5] :

1. *On-demand Self Service*, pengguna dapat menambah dan mengatur layanan tanpa intervensi siapapun.
2. *Ubiquitous Network Access*, layanan *cloud* diakses dengan bantuan internet menggunakan mekanisme dan protokol standar dan dapat diakses setiap waktu.
3. *Resource Pooling*, sumberdaya *cloud* yang digunakan untuk layanan cloud menggunakan infrastruktur yang homogen dan layanan digunakan bersama dengan pengguna lain.
4. *Rapidly Elasticity*, sumber daya harus dapat ditingkatkan dengan cepat dan elastis.
5. *Measures Services*, sumberdaya dan layanan harus diukur, dukungan optimasi penggunaan sumber daya, memberikan laporan penggunaan dan harus memiliki model bisnis *pay-as-you-go* atau dibayar saat digunakan.

4.2 Threat Identification

Cloud Security Alliance [7] mendefinisikan beberapa ancaman dalam teknologi *Cloud* yaitu :

1. *Abuse and Nefarious Use of Cloud Computing*, penyalahgunaan teknologi *cloud* dimana ada kemungkinan terjadinya penyusupan terhadap layanan melalui kegiatan Hacking. Ini bisa terjadi karena layanan IaaS yang ditawarkan tanpa batas terhadap jaringan dan *storage* sering bersinggungan dimana siapapun yang membayar dengan cara legal ataupun illegal dapat memanfaatkan layanan. Beberapa vendor *cloud* bahkan menyediakan layanan percobaan secara gratis untuk periode waku tertentu. Celah ini dapat dimanfaatkan oleh orang dengan anonimitas yang tidak berkepentingan terhadap layanan untuk melakukan penyalahgunaan layanan *cloud*.
2. *Insecure Interface and APIs*, ketidakamanan antarmuka dan API karena layanan *cloud* tergantung pada keamanan dan ketersediaan layanan umum dari API dasar. Proses otentikasi, akses kontrol, dan log harus dirancang sedemikian rupa sehingga setiap proses selalu melalui *policy* yang ditetapkan.
3. *Malicious Insiders*, ancaman dari orang dalam dimana vendor sebagai penyedia layanan bisa diakatakan sebagai outsourcing dari perusahaan yang menyewa layanan. Adanya konvergensi layanan TI dan tidak adanya transparansi akan

menyulitkan bagi perusahaan memonitor kegiatan yang dilakukan vendor terhadap asset fisik dan virtual.

4. *Shared Technology Issues*, isu penggunaan teknologi bersama dimana vendor IaaS memberikan layanan mereka dengan cara berbagi infrastruktur. Seringkali, komponen dasaryang membentuk infrastruktur ini (misalnya, CPU cache, GPU) tidak dirancang dengan sifatisolasi yang kuat untuk arsitektur multi-penyewa. Kompartementalisasi yang kuat harus digunakan untuk memastikan bahwa pelanggan individu tidak mempengaruhi operasi penyewa lain yang berjalan pada vendor *cloud* yang sama. Pelanggan tidak memiliki akses ke data penyewa lain.
5. *Data Loss or Leakage*, kehilangan dan kebocoran data dimana ada banyak cara untuk mengelola data. Contohnya adalah penghapusan atau perubahan data tanpa backup data dari konten asli. Diperlukan adanya pencegahan untuk mengakses data-data sensitif oleh orang yang tidak berkompeten terhadap data tersebut.
6. *Account or Service Hijacking*, pembajakan *account* dan layananbukan hal baru. Aktifitas ini sudah ada sejak layanan internet ada. Maka aktifitas yang samapun dapat terjadii di layanan *cloud*.
7. *Unknown Risk Profile*, profil resiko yang tidak diketahui dimana salah satu prinsip dari kepemilikan perangkat *Cloud Computing* adalah pengurangan penggunaan perangkat lunak dan perangkat keras, sehingga perusahaan lebih fokus ke kekuatan usaha bisnis mereka tanpa harus mengelola infrastruktur IT dan proses pemeliharaannya. Faktor keamanan tetap menjadi hal utama yang harus diperhatikan dalam layanan *Cloud*.

Dari definisi diatas, maka dapat diidentifikasi ancaman yang mungkin timbul pada teknologi Cloud sebagaimana ditunjukkan oleh tabel 1, sebagai berikut :

Tabel 1. Threat Identification

Threat	Source Motivation	Threat Action
Hacker	*Data burglary, Data hijacking, Data destruction*	*Information bribery, Spoofing System Intrusion, Fraud, Computer crime, DDOS, Launching dynamic attack points, Botnet command and control, Building rainbow tables*

Threat	Source Motivation	Threat Action
User anonymity	*Thef of data*	*Spoofing, Hosting malicious data, Botnet command and control, Backdoor Trap, Sniffing*
Internal outsourcing	*Hacking hobies, Organized Crime, Corporate Espionage, Sponsored Intrusion*	*Hacking, Monitoring, Accessing asset, Data Modification*

4.3 *Vulnerability Identification*

Dari hasil identifikasi ancaman, selanjutnya dilakukan *vulnerability identification* atau mengidentifikasi kelemahan dari teknologi *Cloud*. Dalam pembahasan ini materi yang diuji diambil dari hasil identifikasi ancaman dimana ancaman yang teridentifikasi merupakan kelemahan dari sistem pada layanan *Cloud* sebagai berikut :

Tabel 2. *Vulnerability Identification*

Vulnerability	Threat Action
Abuse and Nefarious Use of Cloud Computing	Pendaftaran dan proses validasi yang ketat, Meningkatkan pemantauan dan koordinasi terhadap penipuan kartu kredit, Instropeksi komprehensif lalu lintas jaringan pelanggan, Pemantauan publik blacklist.
Insecure Interface and APIs	Menganalisa kelayakan model keamanan antarmuka layanan, Otentikasi dan kontrol akses dalam transmisi yang terenkripsi
Malicious Insiders	Supply chain management yang ketat, Melakukan kontrak secara hukum terhadap outsourcing sebagai penyelenggara layanan dalam hal ini vendor penyedia layanan, Transparansi dalam keamanan informasi secara keseluruhan, Memberikan dan meminta pelaporan pelanggaran keamanan.
Shared Technology Issues	Melakukan instalasi dan konfigurasi secara aman, Pemantauan lingkungan terhadap perubahan yang tidak sah, Audit konfigurasi
Data Loss or Leakage	Menerapkan control akses API yang ketat, Menjaga integritas data dalam jalur dengan enkripsi.
Account or Service Hijacking	Memperkerjakan pemantauan proaktif untuk mendeteksi aktivitas yang tidak sah.

Vulnerability	Threat Action
Unknown Risk Profile	Disahkannya pengungkapan log aktifitas dan data, pemantauan informasi.

4.4 *Risk Management Option*

Berdasarkan hasil pencarian yang dibahas sebelumnya, dengan melihat karakteristik sistem, hasil identifikasi ancaman, dan identifikasi kelemahan, maka dapat dibuat suatu rekomendasi yang dapat dijadikan bahan pertimbangan oleh Pemerintah Daerah dalam mengadopsi teknologi *Cloud*, sebagai berikut [8] :

1. Tidak menempatkan data-data yang bersifat sensitif dalam layanan *cloud*.
2. Untuk data-data yang bersifat kritis, harus dilakukan pengamanan ekstra pada saat data dikirimkan, saat data berada dalam jaringan, dan pada saat data berada dalam layanan *cloud* dengan cara otentikasi, validasi, dan enkripsi.
3. Setiap dokumen dalam layanan *cloud* sebaiknya disertai Digital Signature, untuk memberikan keyakinan bahwa dokumen tersebut aman.
4. Pengguna layanan *cloud* harus memahami secara jelas dan mendalam tentang kemampuan dan stabilitas dari vendor penyedia layanan *cloud*.
5. Memiliki alternatif kesiapan untuk menangani gangguan layanan melalui layanan backup data pada layanan *cloud* yang lain.
6. Memahami pasal-pasal yang relevan dalam kontrak perjanjian penggunaan layanan *cloud*.
7. Jika pelanggan tidak puas dengan layanan *cloud* dari vendor atau jika vendor menghentikan layanannya, maka biaya dan waktu peralihan harus dibicarakan dalam SLA (*Service Level Agreement*)
8. Adanya jaminan kemanan untuk transisi data, langkah-langkah keamanan, dan protokol yang dibicarakan dan dicantumkan dalam SLA (*Service level Agreement*).

5. Simpulan dan Saran

Pembahasan dalam makalah ini menitikberatkan pada tiga langkah dalam *Risk Assesment* yaitu *: System Characterization*, *Threat Identification*, dan *Vulnerability Identification*. Hasilnya adalah adanya gambaran mengenai bagaimana karakteristik dari sistem cloud, apa saja ancaman yang ada dalam teknologi *cloud*, dan kelemahan apa yang ada dalam teknologi ini.

Layanan yang diberikan dalam *cloud* sebenarnya sama saja seperti layanan yang ada di internet, yang membedakannya adalah dalam layanan cloud semua infrastruktur dan aplikasi yang seharusnya ada di sisi *Client*, kini semuanya berada di sisi *Server*. Artinya, pengguna cukup menyediakan infrastruktur untuk mengakses internet agar bisa terhubung dalam layanan *cloud* untuk menggunakan berbagai aplikasi yang ditawarkan. Karena sifatnya yang Multi-Tenant atau penggunaan beragam layanan secara bersama dalam satu platform, maka teknologi ini memiliki beberapa kelemahan.

Kelemahan yang paling penting untuk diperhatikan adalah masalah keamanan. Oleh karena itu, ada beberapa hal yang harus diperhatikan oleh pemerintah daerah apabila ingin mengadopsi teknologi untuk layanan publik, yaitu :

1. Menentukan layanan apa saja yang akan digunakan di *cloud* yang dapat mendukung proses bisnis dan layanan publik yang optimal.
2. Menentukan data apa saja yang layak dan aman untuk disimpan dan digunakan dalam layanan *cloud*.
3. Memiliki sumber daya manusia yang mengerti teknologi cloud dan layanannya.
4. Memiliki alternatif penanganan masalah apabila sewaktu-waktu ada gangguan dalam layanan dan mempersiapkan opsi apabila vendor menghentikan layanannya.

Daftar Pustaka :

[1] http://www.bappenas.go.id/node/133/2173/inpres-no3-tahun-2003-tentang-kebijakan-danstrategi-nasional-pengembangan-e-governmet/.

[2] http://www.wartaegov.com/berita-1365-cloudcomputing-untuk-pemerintahan-yangefektif.html.

[3] Mell, P., Grance, T., (2009). The NIST Definition of Cloud Computing. from NIST Information Technology Laboratory: http://www.nist.gov/itl/cloud/upload/clouddefv15.pdf.

[4] Bonham, Stephen S., (2005), IT Project Portfolio Management, Artech House, Boston.

[5] Stoneburner, G., Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems, Recommendation of The National Institute of Standards and Technology Special Publication 800-30, July, 2002.

[6] Fardani, A., Surendro, K., (2011), Strategi Adopsi Teknologi Informasi Berbasis Cloud Computing Untuk Usaha Kecil dan menengah di Indonesia, Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2011)

[7] Cloud Security Alliance, (2010), Top Threat to Cloud Computing V1.0, csathreat.v1.0.pdf http://www.cloudsecurityalliance.org/topthreats.

[8] Cloud Computing: Benefits, Risks and Recommendations for Information Security, (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

Analisis Resiko Pada Akademik Management System Universitas Bina Insani Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-

masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview.* Proses ini

dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden

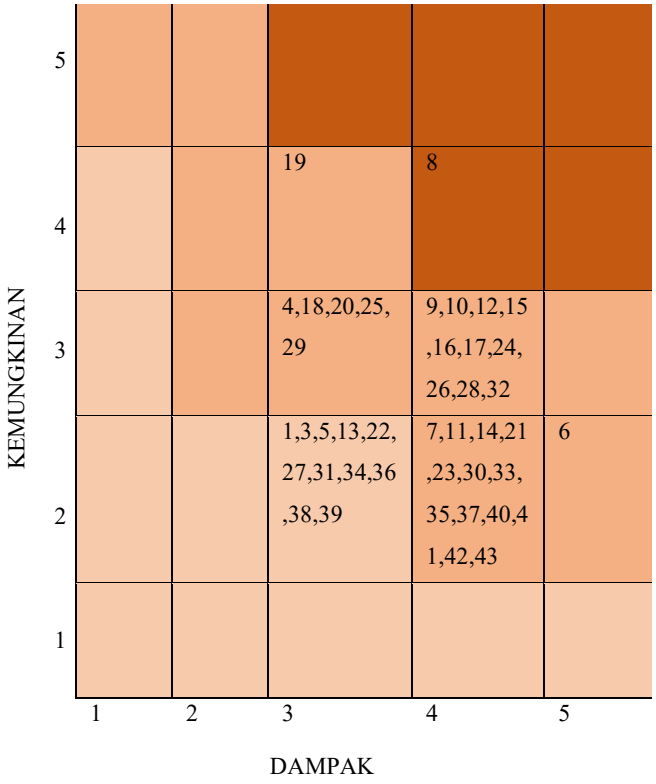
dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling

tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

Prosedur Penilaian Risiko Terhadap Audit Laporan Keuangan

Abstrak

Implementasi akuntabilitas pada sektor publik saat ini terus menerus diupayakan agar dilaksanakan secara konsisten oleh semua jajaran aparatur pemerintahan. Para pimpinan instansi juga didorong agar mereka berperan aktif dalam menciptakan tone at the top. Mereka dituntut untuk memberi contoh dalam menghindari praktek-praktek fraud, penyalahgunaan wewenang dan perbuatan melawan hukum yang mengarah pada perbuatan KKN. Upaya penciptaan lingkungan pengendalian dikembangkan sedemikian rupa sehingga pemahaman tentang fraud telah diberi batasan dan definisi yang lebih konkrit. Sementara upaya lainnya adalah memperluas kewenangan dalam tanggungjawab pembuatan kebijakan anti-fraud di level pimpinan institusi, termasuk langkah-langkah pencegahan (prevention) dan pendeteksian (detection) fraud. Bagi unit audit internal, lingkungan pengendalian yang mendukung upaya penciptaan lingkungan anti fraud dapat menempatkannya pada posisi kesempatan dan tantangan. Lingkungan pengendalian yag kondusif dapat mendorong peran auditor internal secara cepat membangun rencana tindak program pencegahan fraud, dan akan mendapatkan cara untuk memberi nilai tambah bagi organisasinya. Konsekuensinya pimpinan audit internal yang gagal mengantisipasi harapan/tuntutan para stakeholder-nya maka jabatan yang ia duduki menjadi taruhannya.

Key : auditor internal, fraud, audit internal.

Pendahuluan

prosedur penilaian risiko bertujuan untuk mengidentifikasi dan menilai risiko salah saji material dalam laporan keuangan. Tujuan ini dapat dicapai melalui pemahaman mengenai entitas dan lingkungannya, termasuk pemahaman mengenai pengendalian intern dari entitas tersebut.Prosedur penilaian risiko memberikan bukti audit untuk mendukung penilaian risiko pada tingkat laporan keuangan dan pada tingkat asersi. Namun, bukti itu saja tidak cukup. Bukti prosedur penilaian risiko harus dilengkapi dengan prosedur audit lanjutan yang merupakan tanggapan atas risiko yang diidentifikasi, seperi pengujian pengendalian dan/atau prosedur substantif.

Auditor wajib melakukan prosedur penilaian resiko untuk mengidentifikasi dan menilai risiko salah saji material pada tingkat laporan keuangan dan pada tingkat asersi. Pemahaman entitas merupakan upaya yang berkesinambungan dan proses dan proses yang dinamis dalam mengumpulkan dan menganalisis informasi selama audit berlangsung. Auditor menggunakan kearifan profesionalnya untuk menentukan prosedur penilaian risiko yang harus dilaksanakannya, dan seberapa dalam ia perlu memahami entitas itu. Auditor perlu melaksanakan prosedur penilaian risiko yang cukup untuk mengidentifikasi risiko bisnis dan risiko kecurangan yang bisa berdampak pada salah saji material. Auditor menyelidiki dengan seksama keadaan yang menimbulkan keraguan tentang kemampuan entitas melanjutkan usahanya. Ketika melaksanakan prosedur penilaian risiko,auditor wajib mempertimbangkan apakah ada peristiwa atau kondisi yang membuat kemampuan entitas untuk mempertahankan bisnisnya diragukan.

Analisis dan Pembahasan

Pertimbangan awal tentang prosedur penilaian audit

Ketika melaksanakan prosedur penilaian resiko dan kegiatan terkait untuk memperoleh pemahaman mengenai entitas dan lingkungannya, termasuk pengendalian internalnya. Auditor wajib melaksanakan prosedur untuk memperoleh informasi yang akan digunakan untuk mengidentifikasi risiko salah saji karena kecurangan. Untuk memperoleh pemahaman mengenai entitas dan lingkungannya, auditor wajib memperoleh pemahaman mengenai hal hal berikut :

1. Ketentuan mengenai estimasi akuntansi, termasuk pengungkapannya sesuai kerangka pelaporan keuangan yg diterapkan.

2. Bagaimana manajemen mengidentifikasi transaksi, peristiwa, dan keadaan yg mungkin membutuhkan estimasi akuntansi yang akan dimasukan atau diungkapkan dalam laporan keuangan. Auditor wajib menanyakan kepada manajemen tentang perubahan keadaan yang mungkin memerlukan estimasi akuntansi baru atau memerlukan revisi atas estimasi akuntansi yang ada.
3. Bagaimana manajemen membuat estimasi akuntansi dan pemahaman tentang data yang digunakan sebagai dasar, termasuk :
4. metode atau model yang digunakan untuk membuat estimasi akuntansi]
5. pengendalian yang relevan
6. apakah manajemen menggunakan tenaga ahli
7. asumsi yang mendasari estimasi akuntansi
8. apakah ada perubahan atau seharusnya ada perubahan dari tahun lalu dalam

Sebagai bagian prosedur penilaian risiko, auditor wajib melaksanakan prosedur audit untuk memperoleh informasi yang relevan guna mengidentifikasi risiko salah saji material berkaitan dengan hubungan istimewa (related-party relationship) dan transaksi di antara pihak pihak tersebut. Ketika melakukan prosedur penilaian risiko, auditor wajib mempertimbangkan apakah ada peristiwa atau kondisi yang membuat kemampuan entitas untuk mempertahankan hidupnya (atau melanjutkan bisnisnya sebagai *going concern*) diragukan.

Pentingnya prosedur penilaian risiko atas laporan keuangan

Tujuan prosedur penilaian risiko adalah mengidentifikasi dan menilai rrisiko salah saji material dalam pelaporan keuangan. Tujuan ini dapat dicapai dengan memahami tentang entitas dan lingkungannya, termasuk pemahaman tentang pengendalian intern dari entitas tersebut. Ada 3 prosedur penilaian resiko, yaitu :

1. Prosedur menanyakan kepada manajemen dan pihak lain (*inquiries of management and others*)
2. Pengamatan dan inspeksi (*observation and inspection*)
3. Prosedur analitikal (*analytical procedures*)

Prosedur ini membantu mengidentifikasi hal hal yang mempunyai implikasi terhadap laporan keuangan dan audit. Prosedur analitikal juga dapat digunakan sebagai prosedur audit dalam :

1. Memperoleh bukti mengenai asersi laporan keuangan atau dapat disebut sebagai prosedur analitikal substantif
2. Melakukan reviu menyeluruh atas laporan keuangan pada atau menjelang akhir audit.

Prosedur analitikal pada umumnya menggunakan data agregatif yang berarti hasil dari prosedur analitikal hanya memberi indikasi awal yang sangat luas/umum mengenai terjadinya salah saji yang bersifat material.

Kesimpulan

Ketiga prosedur tersebut dilakukan selama berlangsungnya audit. Dalam banyak situasi, hasil dari satu prosedur akan membawa pada prosedur lain. Ketiga prosedur tersebut merupakan hal yang penting yang harus dilaksanakan oleh auditor agar risiko salah saji material dapat teridentifikasi dan menjadikan informasi yang relevan bagi entitas maupun pengguna eksternal.

Daftar Pustaka

Buku Audit Berbasis ISA – Theodorus M. Tuankotta

http://kurniawanbudi04.wordpress.com/2013/01/14/perencanaan-audit/

http://www.slideshare.net/inapurmini/audit-berpeduli-risiko

http://srhyebiru.blogspot.com/2014/01/materialitas-dan-risiko-audit-dan.html

http://tensilatif31.blogspot.com/2012/07/resiko-audit.html

Analisis Resiko Pada Akademik Management System Universitas Bina Insani Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-

masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview.* Proses ini

dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden

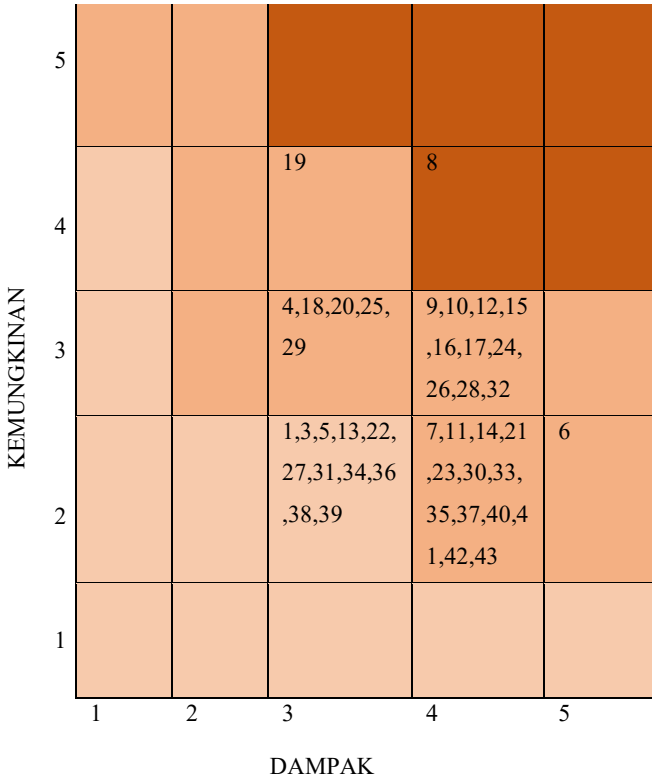
dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling

tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

PENILAIAN RISIKO KEAMANAN INFORMASI PADA PT XYZ DENGAN MENGGUNAKAN ISO 27001:2005

OLEH :

1. **DWI SEPTYA PUTRI**
2. **RIDUAN SYAHRI**
3. **RUMONDANG MARTHA A**
4. **TRI SUSANTI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Aset informasi memilki nilai tertentu bagi perusahaan sehingga harus dilindungi dari ancaman dan kerentanan keamanan informasi. Untuk pencegahan ancaman dan kerentanan keamanan informasi. Untuk itu, diperlukan penilaian risiko keamanan informasi terhadap aset informasi yang bertujuan untuk mengidentifikasi dan menilai risiko terkait keamanan aset informasi, serta memberikan rekomendasi perbaikan mengenai keamanan informasi yang harus diterapkan. PT XYZ memiliki aset informasi yang dikelola dan dilindungi terhadap ancaman dari pihak luar. Penilaian risiko dengan metode kuantitatif FMEA (*Failure Mode Effect Analysis*) untuk mengetahui nilai risiko berdasarkan tingkat kerentanan aset informasi pada PT XYZ, dan dengan pendekatan ISO 27001:2005 untuk menyesuaikan usulan kendali pengendalian dari risiko yang ditemukan berdasarkan aspek keamanan kerahasiaan, integritas, dan ketersediaan. Dengan begitu PT. XYZ mampu mengetahui nilai risiko dan risiko apa saja guna mencegah atau mengantisipasi risiko di masa yang akan datang.

Kata Kunci: aset informasi, penilaian risiko keamanan informasi, metode penilaian risiko FMEA (*Failure Mode Effect Analysis*), ISO 27001:2005

PENDAHULUAN

Data mempunyai peran yang sangat penting dalam sebuah sistem informasi karena merupakan salah satu komponen sistem informasi selain *software*, *hardware, people, procedures*, dan *networks* (Whitman dan Mattord, 2012). Oleh karena itu data yang disimpan dan diproses, kemudian disebarkan di dalam sistem komputer harus dilindungi keamanannya karena merupakan aset informasi yang paling berharga dalam sebuah perusahaan.

Pentingnya informasi membuat perusahaan perlu mengidentifikasi, mengukur, mengevaluasi, dan mengatur kegiatannya agar berfungsi dengan efektif. Sehingga tujuan dari penulisan paper ini adalah untuk mengidentifikasi dan menilai risiko pada aset informasi, agar dapat mengantisipasi, mencegah, dan membantu memperkirakan risiko apa saja yang berkemungkinan muncul terhadap kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya (Talabis & Martin, 2012).

Penilaian risiko keamanan informasi dilakukan dengan menggunakan pendekatan standar ISO 27001:2005. Karena ISO 27001:2005 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi (*IT Governance*, 2013). ISO 27001:2005 juga merupakan standar yang sangat fleksibel yang dikembangkan tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dari struktur organisasi serta menyediakan sertifikat Sistem Manajemen Keamanan Informasi (SMKI) yang diakui internasional, disebut dengan Information Security Management System Certification (ISMSC) (Sarno & Iffano, 2009).

Selain itu penilaian risiko didukung juga dengan Metode FMEA (*Failure Mode & Effect Analysis*). Metode FMEA adalah suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan nilai risiko dari kegagalan, dan skala prioritas untuk mengambil tindakan yang diperlukan. Di dalam FMEA juga terdapat pengendalian risiko menggunakan ISO terhadap keamanan informasi (Robin, Raymond , & Michael, 1996). Dengan demikian, penentuan level nilai risiko tersebut akan mempermudah dalam mendefinisikan aksi-aksi penanganan

risiko dengan tepat pada PT. XYZ. Metode FMEA juga dapat digunakan untuk menelusuri sumber-sumber penyebab dari suatu masalah (Lipol, 2011).

Berdasarkan dari permasalahan yang telah diuraikan di atas, maka tujuan dari penulisan paper adalah untuk melakukan analisis lebih lanjut di mana fokus utama dari penelitian yang akan dilakukan adalah mengidentifikasi dan memberikan penilaian risiko tiap-tiap aset informasi pada proses bisnis perkreditan mobil bekas di PT. XYZ.

PEMBAHASAN

A. PT. XYZ

PT. XYZ merupakan perusahaan yang bergerak di bidang pembiayaan sewa guna usaha, pembiayaan konsumen dan anjak piutang, yang memiilki beberapa cabang di Indonesia salah satunya di Palembang, dan memiliki kantor pusat yang berlokasi di Jakarta.

B. Penilaian risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, juga dikenal sebagai analisis risiko keamanan informasi, yaitu melibatkan identifikasi dan penilaian risiko terhadap kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya (Talabis & Martin, 2012). Hasil dari penilaian risiko adalah penentuan risiko, yaitu menentukan tingkat ancaman dan besar/kecilnya kemungkinan ancaman yang akan terjadi. Untuk mendukung komponen risiko, organisasi mengidentifikasi hal-hal sebagai berikut:

1. Ancaman terhadap organisasi (seperti operasi, aset, individu, atau ancaman yang langsung diarahkan organisasi terhadap organisasi lain.
2. Kerentanan internal atau eksternal organisasi.
3. Ancaman (yaitu, konsekuensi atau dampak) yang didapat dari ekspolitasi kelemahan sistem dalam organisasi.
4. Kemungkinan ancaman yang mungkin terjadi.
5. Bagaiaman penilaian risiko dilakukan dalam organisasi.
6. Frekuensi penilaian risiko.
7. Bagaimana ancaman diperoleh dari sumber atau metode. (National Institute of Standards and

Technology, 2011).

C. Identifikasi Risiko

Baik identifikasi maupun penilaian risiko merupakan rangkaian tahap dari manajemen risiko. Identifikasi risiko penting karena merupakan tahap pertama yang harus dilakukan karena dalam tahap ini dilakukan penentuan risiko – risiko beserta karakteristiknya yang mungkin akan mempengaruhi proyek.

D. Penilaian Risiko dengan FMEA

FMEA (*Failure Mode And Effects Analysis*) adalah metode yang akan digunakan untuk menilai dan menganalisis risiko secara kuantitatif. FMEA secara sistematis membantu untuk mengidentifikasi dan menilai pemicu (*modes*), probabilitas kejadian, dampak (*effects*) dari kegagalan dalam suatu sistem. Hasil analisis dan penilaian tersebut akan memberi peringkat dari setiap kegagalan sesuai dengan ketiga nilai tersebut.

a. Tingkat *severity*, yaitu suatu penilaian tingkat keparahan dari keseriusan *effect* yang ditimbulkan dari mode-mode kegagalan (*failure mode*), menghitung seberapa besar dampak/intensitas kejadian mempengaruhi output proses, maupun proses-proses selanjutnya.

b. Tingkat *occurrence*, yaitu suatu penilaian mengenai peluang (probabilitas) frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa penggunaan produk.

c. Tingkat *detection*, yaitu pengukuran terhadap kemampuan mengendalikan/ mengontrol kegagalan yang dapat terjadi. (Robin, Raymond , & Michael, 1996.)

Langkah-langkah dalam metode FMEA dapat dilihat pada gambar 2.2 di bawah ini:

Gambar 1 FMEA *Cycle* (Steven C. Legget, 2001)

Secara keseluruhan prosesnya, metode FMEA terdiri dari 6 langkah berikut ini (Steven C. Legget, 2001):

Yang pertama kali dilakukan pada langkah pertama adalah mengidentifikasi potensial pemicu kegagalan teknologi informasi (Steven, 2001). Pada langkah kedua yaitu menentukan tingkat nilai keparahan (*severity number*) sesuai dengan rentang skala. Pada langkah ketiga yang dilakukkan adalah menentukan tingkat nilai probabilitas (*ocurrance number*) sesuai dengan rentang skala. Dan pada langkah keempat menentukan tingkat nilai kontrol risiko (*detection number*) sesuai dengan rentang skala. *Level* tingkat risiko dijelaskan pada tabel 1 di bawah ini:

Tabel 1. *Level* tingkat risiko FMEA

Level	Severity	Occurance	Detection
1	*None* (Tidak ada efek)	*Remote* (Lebih dari 5 tahun)	*Almost Certain* (Kontrol pasti dapat dan berhasil mencegah kegagalan)
2	*Very Minor*	*Very Low*	*Very High*

	(Sumber daya tersedia/ efek yang kecil terhadap proses)	(Setiap 3-5 tahun)	(Kemampuan kontrol dalam mencegah kegagalan adalah tinggi)
3	*Minor* (Sumber daya tersedia/ efek yang kecil terhadap prosedur)	*Low* (Setiap 1-3 tahun)	*High* (Kemampuan kontrol dalam mencegah kegagalan adalah tinggi)
4	*Very Low* (Sumber daya tersedia/ efek yng kecil terhadap kebijakan)	*Moderately Low* (Setiap Tahun)	*Moderately High* (Kemampuan kontrol dalam mencegah kegagalan cukup tinggi)
5	*Low* (Sumber daya tersedia/ efek yang besar terhadap proses)	*Moderate* (Setiap 6 bulan)	*Moderate* (Kemampuan kontrol dalam mencegah kegagalan adalah rendah)
6	*Moderate* (Sumber daya tersedia/ efek yang besar terhadap prosedur)	*Moderately High* (Setiap 3 bulan)	*Low* (Kemampuan Kontrol dalam mencegah kegagalan adalah rendah)
7	*High* (Sumber daya tersedia/ efek yang besar terhadap kebijakan)	*High* (Setiap bulan)	*Very Low* (Kemampuan kontrol dalam mencegah kegagalan adalah sangat rendah)
8	*Very High* (Sumber daya tidak tersedia/ kegagalan diketahui dan dapat dikontrol)	*High* (Setiap bulan)	*Remote* (Kecil kemungkinan kontrol dapat mencegah kegagalan)
9	*Extremly High* (Sumber daya tidak tersedia/ kegagalan diketahui namun tidak dapat dikontrol)	*Very High* (Setiap 3-4 hari)	*Very Remote* (Sangat kecil kemungkinan dapat mencegah kegagalan)
10	*Catastrophic* (Sumber daya tidak	*Extremely High*	*Absolute Uncertainly* (Kontrol tidak dapat

	tersedia/ kegagalan tidak diketahui)	(Setiap Hari)	mencegah kegagalan)

Setelah mengetahui *level* tingkat risiko, langkah selanjutnya adalah menentukan nilai RPN (*Risk Priority Number*). RPN merupakan nilai batasan yang menunjukkan risiko-risiko dengan nilai tertinggi. Nilai RPN diperoleh dengan mengalikan nilai tingkat keparahan efek (*severity*), nilai tingkat probabilitas (*occurrence*), dan nilai tingkat deteksi kontrol risiko (*detection*).

Menurut ISO 27001, maka nilai RPN dapat diperoleh dengan rumus :

RPN = S x O x D

Dimana:

S : *Severity Number* (Angka Tingkat Keparahan)

O : *Occurance Number* (Angka Tingkat Probabilitas Kejadian)

D : *Detection Number* (Angka Tingkat Deteksi Kontrol Risiko)

Setelah mengetahui nilai dari RPN, langkah terakhir adalah menentukan *Level* dari hasil RPN yang diperoleh, selanjutnya akan dilakukan penentuan *level* risiko, apakah risiko termasuk ke dalam golongan risiko dengan *level* tinggi, sedang, atau rendah. Penentuan *level* risiko didasarkan pada standar skala FMEA yang dapat dilihat pada tabel 2 berikut ini:

Tabel 2. Skala Nilai RPN FMEA

Skala Nilai RPN FMEA	
Skala Nilai RPN	**Level Risiko**
0-19	*Very Low*
20-79	*Low*
80-119	*Medium*
120-199	*High*
>200	*Very High*

E. ISO 27001:2005

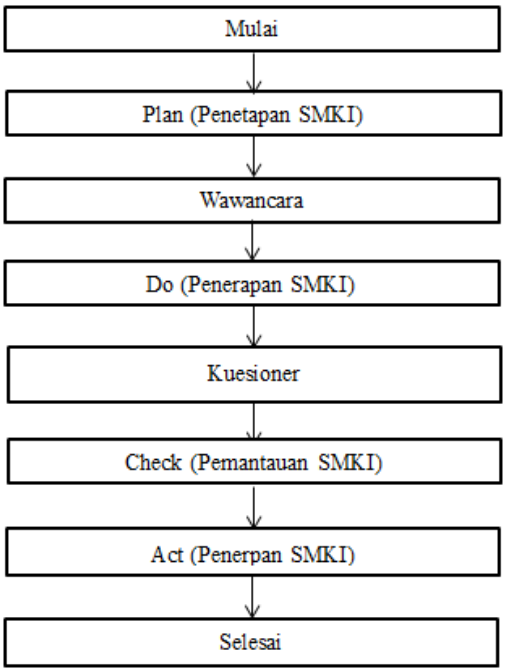
Standar ISO 27001:2005 ini sudah teruji dan direkomendasi oleh badan standar nasional Indonesia dan sudah diadopsi menjadi standar SNI ISO/IEC 27001:2009 "Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan" disusun secara adopsi identik terhadap standar ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management system - Requiretments*, dengan metode terjemahan oleh Panitia Teknis PK 03-02 Sistem Manajemen Mutu yang dibentuk BSN (SNI ISO/IEC, 2009).

Standar ISO 27001:2005 ini mengadopsi model "*Plan-Do_Check_Act*" (PDCA), yang diterapkan untuk membentuk seluruh proses SMKI. Konsep siklus PDAC ini pertama kali diperkenalkan oleh seorang ahli manajemen kualitas dari Amerika Serikat yang bernama Dr. William Edwards Deming.

a. *Plan* (penetapan SMKI) Menetapkan kebijakan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
b. *Do* (penerapan dan pengoperasian SMKI) Menerapkan dan mengoperasikan kebijakan, pengendalian, proses dan prosedur SMKI.
c. *Check* (pemantauan dan pengkajian SMKI) Mengases risiko (penilaian) dan, apabila berlaku, mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
d. *Act* (peningkatan dan pemeliharaan SMKI) Mengambil tindakan korektif dan pencegahan berdasarkan hasil SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

F. Tahapan Penilaian Risiko

Tahapan-tahapan penilaian risiko diuraikan pada **Gambar 3** di bawah ini.



Gambar 3 Tahapan Penilaian Risiko

1. **Penetapan SMKI :**
   - Keamanan informasi di lakukan pada PT.XYZ. SMKI dilakukan terkait penilaian risiko pada proses perkreditan mobil bekas terhadap aset informasi.
2. **Penerapan SMKI:**
   - Pendekatan penilaian risiko menggunakan FMEA. FMEA digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan nilai

risiko dari kegagalan, dan skala prioritas untuk mengambil tindakan yang diperlukan.

3. **Pemantauan SMKI** :

- Identifikasi Status Aset Pada Kelompok Aset Informasi

  Identifikasi status aset informasi terhadap kelompok aset informasi. Apakah Aset informasi yang terdapat pada PT. Clipan Finance Cabang Palembang pada proses perkreditan mobil bekas berstatus Utama atau Pusat.

- Analisis Aset Data Dan Informasi Kritis

  Pada tahap ini, penulis menganalisis dan membuat penetapan aset yang dinilai berdasarkan tingkat kritis terhadap kerentanan dan kekritisan data. Penulis meganalisis data yang paling kritis yang harus dilindungi keamananannya.

- Identifikasi Aspek Keamanan Aset Kritis

  Pada tahap ini, penulis akan mengidentifikasi kebutuhan aspek keamanan aset informasi terhadap CIA. Dimana C adalah *Confidentiality*, I adalah *Integrity*, A adalah *availability.* CIA merupakan prinsip-prinsip dasar yang digunakan dalam keamanan informasi.

- Identifikasi Potensial *Causes*

  Pada tahap ini, penulis melakukan identifikasi potensial causes, dimana penyebab dari timbulnya risiko yang terjadi dan didapatkan identifikasi kerentanan dan ancaman dari aset informasi perkreditan mobil bekas.

- Penilaian Risiko setiap aset informasi dengan metode FMEA

  Pada tahap ini, penulis melakukan penilaian risiko terhadap aset informasi dengan menggunakan FMEA. Identifikasi penilaian berdasarkan hasil RPN. Dimana RPN didapat dari hasil perkalian SxOxD.

- Hasil Analisis Penilaian Risiko

  Hasil analisis penilaian risiko didapat berdasarkan identifikasi aset yang terlibat, hasil kuesioner, status aset informasi, aspek keamanan informasi, identifikasi potensial *causes,* serta penilaian risiko dengan FMEA.

4. **Penerapan SMKI :**

- Rekomendasi Perbaikan Kendali Usulan Berdasarkan Klausul 27001:2005

  Rekomendasi perbaikan berisikan rekomendasi terhadap kondisi hasil penilaian risiko tiap-tiap aset informasi mengenai perkreditan mobil bekas didasari usulan kendali Standar ISO 27001:2005. Usulan kendali klausul dari klausul A5 sampai dengan A15 disesuaikan dengan kebutuhan dan hasil penilaian risiko terhadap rekomendasi perbaikan.

KESIMPULAN

Failure Mode and Effect Analysis (FMEA) merupakan salah satu teknik analisis kegagalan yang memiliki tujuan untuk mencermati proses maupun produk untuk mengetahui kemungkinan kegagalan yang terjadi dengan mengidentifikasi potensi kegagalan, akibat serta kemungkinan munculnya (Firdaus & Widianti, 2015). Dalam melakukan evaluasi kegagalan, FMEA menggunakan tiga indikator yaitu severity (S), occurence (O), dan detection (D). Setelah menentukan nilai ketiga indikator, selanjutnya yaitu menentukan nilai prioritas mode kegagalan berdasarkan nilai Risk Priority Number (RPN).

ISO 27001:2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001:2005 merupakan dokumen standar SMKI yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh suatu organisasi untuk bisa mengimplementasikan konsep-konsep keamanan informasi pada organisasi.

DAFTAR PUSTAKA

Badan Standardisasi Nasional Indonesia. SNI ISO/IEC 27001:2005.

Whitman, ME, Mattord, HJ. 2012. *Principes of Information Security*. Boston (US): Course Technology, Thomson.

Talabis, M., & Martin, J. (2012). *Information Security Risk Assessment: Risk Assessment. In Information Security Risk Assessment Toolkit* (pp. 147–175).http://doi.org/http://dx.doi.org/10.1016/B978-1-59-749735-0.00005-1

Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

IT Governance. 2013. *Information Security & ISO 27001*. IT Governance Green Paper. United Kingdom.

Mcdermott, Robin E., Mikulak, Raymond J., Beauregard, Michael R. 1996. The Basic of FMEA. New York: 444 Park Avenue South, 7th floor.

L. S. Lipol. 2011. Risk Analysis Method: FMEA in the Organizations. International Journal of Basic & Applied Sciences IJBAS, vol XI, no 5, pp. 49-57.

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **UCI SURIANI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa orang untuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci: *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada website Hyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

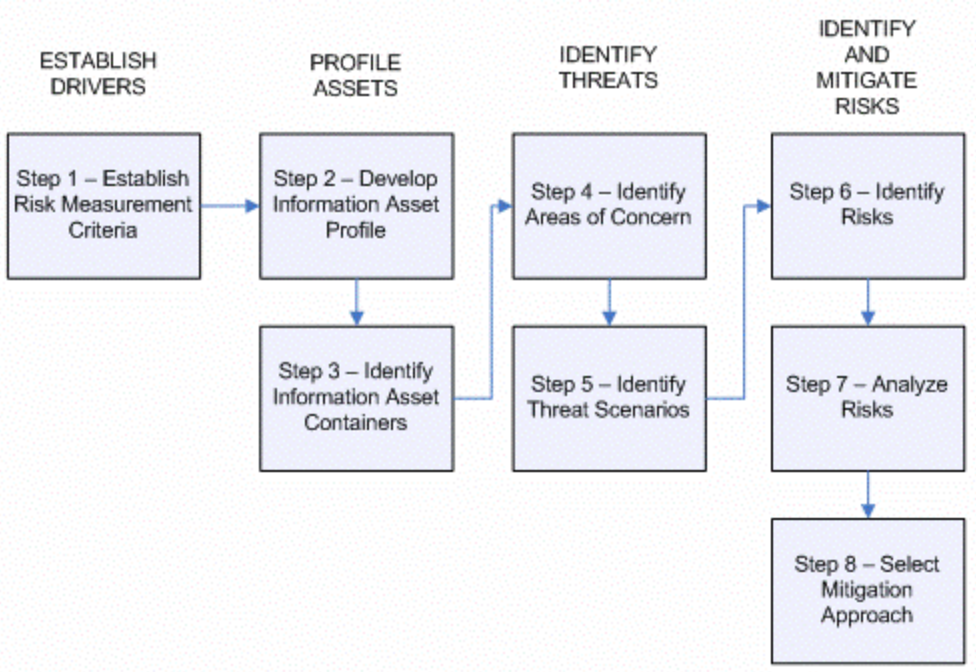
Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi. (Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang mengkontak calon pelamar perusahaan tersebut dan data harus diamankan	

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi

dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	**Area of Concern**
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**
Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	***Risk***			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1), 43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8 November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

Analisis Resiko Pada Akademik Management System Universitas Bina Insani Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-

masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview.* Proses ini

dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden

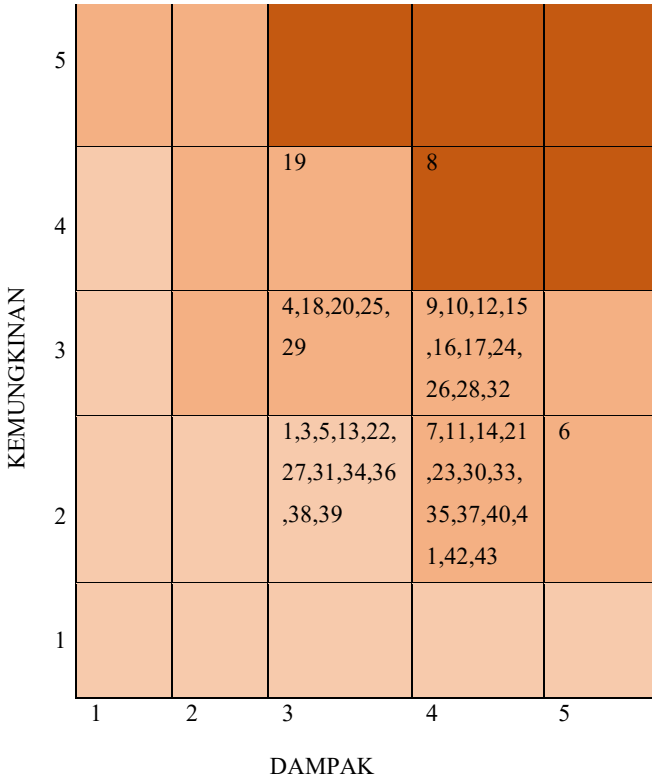
dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling

tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

Analisis Resiko Pada Akademik Management System STKIP Muhammadyah Bangka Belitung

Yuniarti Denita Sari[1], Zena Lusi[2], Reni Septiyanti[3], Anggari Ayu P[4], Gina Agiyani[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di STKIP Muhammadyah Bangka Belitung. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.
Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. STKIP Muhammadyah Bangka Belitung merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan

aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan STKIP Muhammadyah Bangka Belitung. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di STKIP Muhammadyah Bangka Belitung. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan

bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah

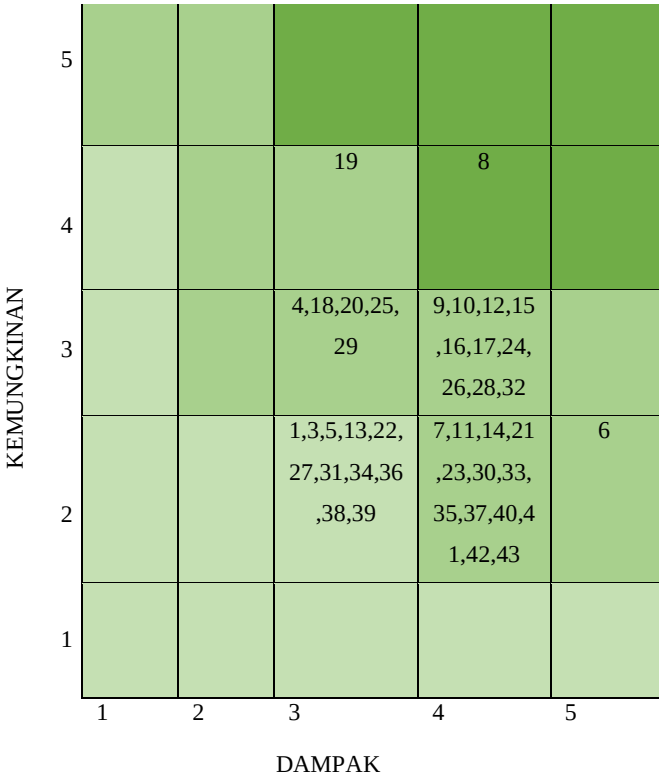
ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang

memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low /	1	Resiko Kerusakan akibat bencana alamt	NTP Server

Rendah)		seperti kebakaaran banjir, gempa	
	2	Pencurian Perangkat	NTP Server
	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya

merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dan lain-lain. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1. Apa pemicu terjadinya database server down pada sistem AMS?
2. Seberapa sering database server down tersebut terjadi pada sistem AMS?
3. Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

a) Overheat
b) Overcapacity
c) Overload
d) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
    - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin

sehingga perangkat terhindar dari resiko akibat overheat.

- Menghilangkan log yang menggunakan kapasitas yang besar
- Melakukan restart database service.
- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-

manajemen.[Accessed 16 November 2014].
[9] [Online].Available:http://dosen.guf ron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].
[10] [Online].Available:http://fisipuin.sa tugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.aca demia.edu/5170798/Uji_Validitas_ Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri0 1.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed 25 Februari 2015].
[15] [Online].Available:https://avicenna edu.wordpress.com/2013/03/26/resi komanajemen-risk-management/. [Accessed 10 Juni 2015].

Analisis Resiko Pada Akademik Management System STKIP Muhammadyah Bangka Belitung

Yuniarti Denita Sari[1], Zena Lusi[2], Reni Septiyanti[3], Anggari Ayu P[4], Gina Agiyani[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di STKIP Muhammadyah Bangka Belitung. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.
Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. STKIP Muhammadyah Bangka Belitung merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan

aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan STKIP Muhammadyah Bangka Belitung. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di STKIP Muhammadyah Bangka Belitung. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan

bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah

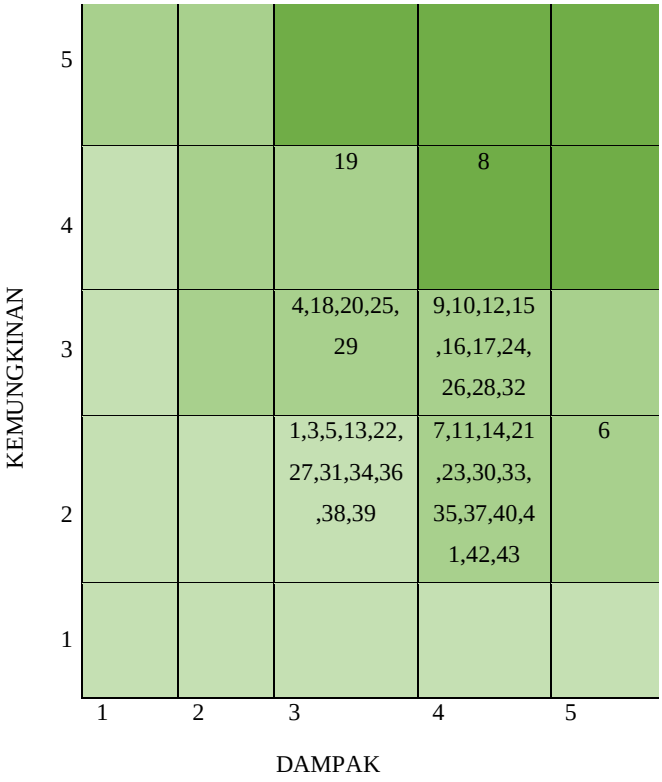
ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang

memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low /	1	Resiko Kerusakan akibat bencana alamt	NTP Server

Rendah)		seperti kebakaaran banjir, gempa	
	2	Pencurian Perangkat	NTP Server
	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya

merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dan lain-lain. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1. Apa pemicu terjadinya database server down pada sistem AMS?
2. Seberapa sering database server down tersebut terjadi pada sistem AMS?
3. Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

a) Overheat
b) Overcapacity
c) Overload
d) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
    - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin

sehingga perangkat terhindar dari resiko akibat overheat.

- Menghilangkan log yang menggunakan kapasitas yang besar
- Melakukan restart database service.
- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-

manajemen.[Accessed 16 November 2014].
[9] [Online].Available:http://dosen.guf ron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].
[10] [Online].Available:http://fisipuin.sa tugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.aca demia.edu/5170798/Uji_Validitas_ Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri0 1.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed 25 Februari 2015].
[15] [Online].Available:https://avicenna edu.wordpress.com/2013/03/26/resi komanajemen-risk-management/. [Accessed 10 Juni 2015].

TUGAS

“Proses Asesment Resiko”

Mata Kuliah : *Ethical Issues in Electronic Information*

Dosen Pengasuh : M. Izman Herdiansyah, M.M., Ph.D

Disusun oleh :

1. **ABI DAUD YUSUF**

Reguler B Angkatan 19 (Sembilan Belas)

Program Pascasarjana Magister Teknik Informatika

Universitas Bina Darma Palembang

2019

ABSTRACK

Identifikasi Potensi Bahaya dan Penilaian Risiko merupakan bagian dari program keselamatan dan kesehatan kerja dalam tahapan manajemen risiko, yang dilakukan sebagai upaya untuk mencegah terjadinya kecelakaan kerja dan penyakit akibat kerja (PAK). Tujuan dari penelitian adalah mempelajari Penerapan Identifikasi Potensi Bahaya dan Penilaian Risiko di Unit Utility. Berdasarkan sifat masalah dan analisa datanya, penelitian ini merupakan penelitian deskriptif, ditinjau dari segi waktu penelitian ini termasuk penelitian cross sectional. Lokasi dan waktu penelitian. Obyek penelitian adalah penerapan Identifikasi Potensi Bahaya dan Penilaian Risiko. Metode yang digunakan oleh peneliti dalam melakukan Penilaian Risiko mengacu pada metode yang telah digunakan oleh Perusahaan. Data yang digunakan dalam penelitian adalah data primer hasil dari observasi dan wawancara serta

Kata Kunci:

1.Pendahuluan

Risk assessment (penilaian risiko) adalah metode yang sistematis untuk menentukan apakah suatu organisasi memiliki resiko yang dapat diterima atau tidak. *Risk assessment* merupakan kunci dalam perencanan pemulihan bencana. Penilaian risiko, proses menganalisis dan menafsirkan risiko terdiri dari tiga kegiatan dasar yaitu: (1) menentukan ruang lingkup dan metodologi penilaian, (2) mengumpulkan dan menganalisis data, dan (3) menafsirkan hasil analisis risiko..

2.Pembahasan

Menentukan Ruang Lingkup dan Metodologi Penilaian

Langkah pertama dalam melakukan risk assessment adalah mengidentifikasi sistem yang sedang dipertimbangkan, bagian sistem yang akan di analisis, dan metode analisis yang akan digunakan.

Assessment dapat difokuskan pada area tertentu baik yang tingkat risikonya tidak diketahui maupun yang tingkat risikonya tinggi. Mendefinisikan ruang lingkup dan batasan dapat membantu peghematan biaya.

Faktor yang mempengaruhi ruang lingkup:

· Fase dalam siklus hidup sistem, misalnya lebih baik mengembangkan sistem baru daripada meng-upgrade sistem yang sudah ada.

· Kepentingan relatif dari sistem di bawah pemeriksaan, sistem yang lebih penting seharusnya di analisis lebih menyeluruh.

· Besar dan jenis sistem yang mengalami perubahan sejak analisis risiko terakhir.

Metodologi bisa berbentuk formal atau informal, rinci atau sederhana, tingkat tinggi atau rendah, kuantitatif atau kualitatf, atau kombinasi dari semuanya. Tidak ada metode tunggal yang terbaik untuk semua pengguna dan semua lingkungan.

Cara menentukan batasan, ruang lingkup, dan metodologi akan memiliki konsekuensi besar dalam jumlah total usaha yang dihabiskan pada manajemen risiko dan jenis serta kegunaan dari hasil penilaian itu. Batasan dan ruang lingkup harus dipilih dengan cara yang akan memberikan hasil yang jelas, spesifik, dan berguna untuk sistem dan lingkungan.

B.Mengumpulkan dan Menganalisis Data

Risiko mempunyai banyak perbedaan komponen, diantaranya aset, ancaman, kerentanan, perlindungan, konsekuensi, dan kemungkinan. Pemeriksaan mencakup pengumpulan data tentang daerah yang terancam dan mensintesis serta menganalisis informasi agar berguna.

Untuk menghindari adanya kemungkinan pengumpulan informasi yang banyak namun hanya sedikit yang dapat di analisis, maka perlu diambil langkah untuk membatasi pengumpulan informasi dengan cara penyaringan. Sebuah upaya manajemen risiko harus fokus pada bidang-bidang yang menghasilkan konsekuensi terbesar bagi organisasi seperti menyebabkan kerugian yang besar. Hal ini dapat dilakukan oleh ancaman dan aset.

Sebuah metodologi manajemen risiko tidak selalu perlu menganalisis komponen risiko secara terpisah. Misalnya, aset dan konsekuensi atau ancaman dan *likelihoods* dapat di analisa bersama-sama.

·**Penilaian Aset (*Asset Valuation*)**

Yang termasuk dalam penilaian aset yaitu informasi, software, personl, hardware, dan aset fisik. Nilai aset terdiri dari nilai intrinsik, dampak jangka pendek, dan konsekuensi jangka panjang dari kompromi tersebut.

·**Penilaian Konsekuensi (*Consequence Assessment*)**

Penilaian konsekuensi memperkirakan tingkat kesukaran atau kerugian yang bisa terjadi. Konsekuensi mengacu pada bahaya secara keseluruhan bukan hanya untuk jangka pendek atau dampak langsung. Sementara damapk seperti itu sering mengakibatkan pengungkapan, modifikasi, perusakan atau penolakan layanan. Konsekuensi jangka panjang memiliki efek yang lebih signifikan seperti hilangnya bisnis, kegagalan untuk melakukan misi sistem, hilangnya reputasi, pelanggaran privasi, cedera, atau korban jiwa. Semakin parah konsekuensi dari ancaman, semakin besar risiko sistem.

·**Identifikasi Ancaman (*Threat Identification*)**

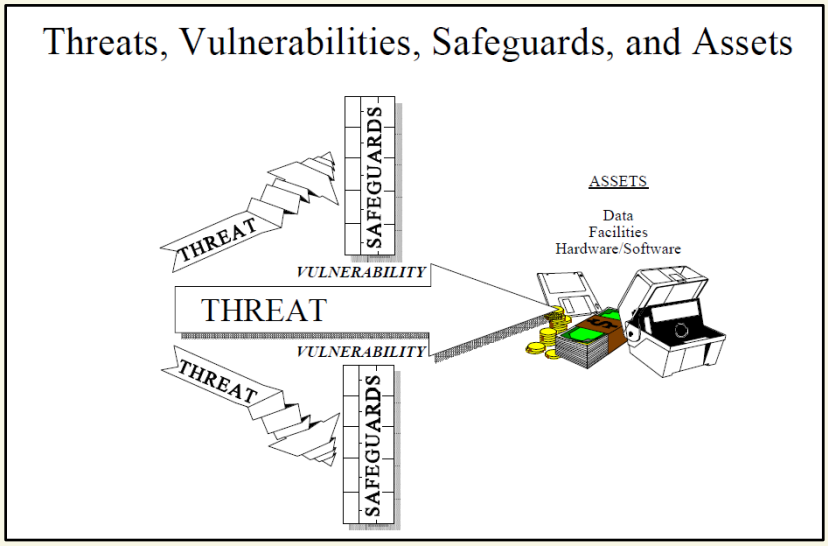
Ancaman adalah suatu entitas atau peristiwa yang berpotensi membahayakan sistem. Yang termasuk dalam ancaman tipikal adalah kesalahan, penipuan, karyawan yang tidak puas, kebakaran, kerusakan air, hacker, dan virus. Ancaman harus diidentifikasi dan dianalisis untuk menentukan kemungkinan terjadinya ancaman tipikal dan potensinya untuk merusak aset. Analisis risiko harus berkonsentrasi pada ancaman-ancaman yang paling mungkin terjadi dan yang bisa mempengaruhi aset penting.

· **Analisis Perlindungan (*Safeguard Analysis*)**

Perlindungan adalah setiap tindakan, perangkat, prosedur, teknik atau ukuran lain yang mengurang kerentanan sistem dari ancaman. Analisis perlindungan harus mencakup pemeriksaan dari efektifitas kebijakan keamanan yang ada. Hal ini juga dapat mengidentifikasi perlindungan baru yang diterapkan dalm sistem, namun biasanya dilakukan belakangan dalam proses manajemen risiko.

· **Analisis Kerentanan (*Vulnerability Analysis*)**

Kerentanan adalah kondisi tidak adanya prosedur keamanan, kontrol teknik, kontrol fisik, atau kontrol lain yang dapat dieksploitasi oleh ancaman. Kerentanan sering di analisis dalam hal hilangnya pengamanan. Kerentanan berkontribusi mengambil risiko karena memungkinkan ancaman untuk membahayakan sistem. Keterkaitan kerentanan, ancaman, dan aset sangat penting untuk analisis risiko. Keterkaitan ini dapat dilihat pada gambar 1. Namun, ada hubungan timbal balik lain seperti adanya kerentanan yang mendorong ancaman.



Gambar 1 Keterkaitan antara ancaman, kerentanan, pengamanan, dan aset.

Penilaian Kemungkinan (*Likelihood Assessment*)

Kemungkinan adalah perkiraan frekuensi atau kesempatan terjadinya ancaman. Sebuah penilaian mungkin mempertimbangkan keberadaan, keuletan, dan kekuatan dari ancaman serta efektifitas perlindungan. Secara umum, banyak informasi tentang ancaman lemah, terutama yang berkaitan dengan ancaman manusia. Dengan demikian, pengalaman di bidang ini sangat penting. Semakin besar kemungkinan ancaman terjadi, semakin besar pula risikonya.

C. Menafsirkan Hasil Analisis Risiko

Penilaian risiko digunakan untuk mendukung dua fungsi terkait yaitu penerimaan risiko dan pemilihan biaya kontrol yang hemat. Untuk mencapai fungsi-fungsi tersebut, penilaian risiko harus menghasilkan output yang berarti, yang mencerminkan apa yang benar-benar penting bagi organisasi. Membatasi kegiatan interpretasi risiko untuk risiko yang paling signifikan adalah cara lain dalam proses manajemen risiko yang difokuskan untuk mengurangi upaya menyeluruh sementara masih menghasilkan hasil yang bermanfaat. Jika risiko diinterpretasikan secara konsisten di seluruh organisasi, hasilnya dapat digunakan untuk memprioritaskan sistem yang harus diamankan

DAFAR PUSTAKA

http://aliphoemarley.blogspot.com/2012/02/risk-assessment-computer-security.html

PENILAIAN RISIKO KERJA PADA PROSES PRODUKSI

Ahkmad Ipandy[1], Erin Efriansyah[2], Fero Triando[3], Tri Akhyari Romadhon[4]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Penilisan ini dilakukan karena ditemukan berbagai bahaya dan risiko pada pekerja di bagian proses produksi. Penelitian ini bertujuan untuk mengetahui besaran risiko keselamatan dan kesehatan kerja pada pekerja di bagian proses produksi *spin pack*. Hasil telitian menunjukkan bahwa pada *basic risk* terdapat 6 aktivitas yang termasuk dalam level *very high*. Pada *existing risk*, terdapat 2 aktivitas dengan risiko tinggi yang termasuk dalam level *priority 1*, yaitu pada proses pencetakan dan proses *pressing* produk yang menggunakan mesin *press*. Dalam penelitian ini juga diberikan *predictive risk* dengan rekomendasi pengendalian, sehingga risiko-risiko yang ada dapat diturunkan sampai pada level *acceptable*.

Kata kunci: Penilaian risiko, resiko kerja , proses produksi

1. PENDAHULUAN

Keselamatan dan kesehatan kerja (K3) merupakan promosi dan pemeliharaan tertinggi tingkat fisik, mental dan kesejahteraan sosial dari semua pekerjaan, pencegahan efek kesehatan yang disebabkan oleh kondisi kerja pekerja, perlindungan bagi pekerja dari resiko akibat faktor yang merugikan bagi kesehatan, menempatkan dan pemeliharaan pekerja dalam lingkungan kerja disesuaikan pada fisiologis dan psikologis dan untuk meringkas adaptasi bekerja untuk manusia dan masing-masing pekerjaannya (*ILO/WHO Join and Health Committee, 1950*). Berdasarkan definisi tersebut dapat dikatakan bahwa K3 merupakan salah satu faktor yang paling penting dan sangat dibutuhkan untuk menjamin keselamatan hidup manusia.

Kecelakaan merupakan sebuah kejadian tak terduga yang menyebabkan cedera atau kerusakan (Ridley, 2004). Kecelakaan akibat kerja adalah kecelakaan yang berkaitan dengan hubungan kerja dengan perusahaan. Hubungan kerja disini dapat berarti bahwa kecelakaan dapat terjadi dikarenakan oleh pekerjaan atau pada waktu melakukan pekerjaan (Suma'mur, 1989). Dalam hal ini kita dapat melihat bahwa kecelakaan adalah salah satu risiko yang cukup besar karena menyebabkan cedera dan kerugian yang dapat terjadi kapan saja terutama bagi pekerja.

Setiap tahunnya di dunia terjadi sekitar 340 juta kecelakaan kerja dan 160 juta korban penyakit akibat kerja (ILO, 2011). Angka ini menunjukkan bahwa kecelakaan kerja masih tergolong tinggi dan butuh tindakan pencegahan sesegera mungkin agar angka tersebut tidak

terus bertambah. Di Indonesia pun, angka kecelakaan kerja masih terus meningkat dari tahun ke tahun. Ini terbukti dari data Jamsostek selama 5 tahun terakhir. Berikut data Jamsostek mengenai angka kecelakaan kerja di Indonesia dalam kurun waktu 5 tahun terakhir.

Table 1. Angka Kecelakaan Kerja dan Klaim Kecelakaan Tahun 2008-2012

Tahun	Angka Kecelakaan Kerja (kasus)	Klaim Kecelakaan Kerja (rupiah)
2012	103.000	646,2 milyar
2011	99.491	504 milyar
2010	98.711	401,2 milyar
2009	96.314	328,5 milyar
2008	94.763	297,9 milyar

Sumber: Jamsostek

Berdasarkan data diatas kita dapat melihat bahwa angka kecelakaan kerja di Indonesia terus meningkat setiap tahunnya. Hal ini tentu menunjukkan bahwa masih lemahnya sistem keselamatan dan kesehatan kerja untuk melindungi pekerja-pekerja di Indonesia. Jika kondisi ini tidak segera ditangani, maka pengingkatan jumlah kecelakaan kerja akan cenderung untuk terjadi di tahun-tahun yang akan datang. Menurut Suma'mur (1989), kecelakaan menyebabkan lima kerugian yaitu kerusakan, kekacauan organisasi, keluhan dan kesedihan, kelainan dan cacat serta kematian.

Disamping kerugian-kerugian tersebut, perusahaan juga harus menanggung biaya-biaya lainnya yang timbul dari kecelakaan tersebut. Salah satunya adalah biaya klaim asuransi kecelakaan kerja. Berdasarkan tabel 1.1 dapat dilihat bahwa peningkatan angka kecelakaan tentunya juga diiringi dengan peningkatan klaim asuransi untuk pekerja yang mengalami kecelakaan. Selain itu perusahaan juga diharuskan untuk memberikan ganti rugi atau kompensasi kepada pekerja yang mengalami kecelakaan pada saat bekerja atau di tempat kerja. Hal ini telah diatur dalam Undang-Undang No. 34 tahun 1947 Tentang Kecelakaan Kerja dan Undang-Undang No.2 tahun 1992 tentang Jaminan Sosial Tenaga Kerja. Biaya-biaya tersebutlah yang harus ditanggung oleh perusahaan jika kecelakaan kerja masih terus terjadi.

Selain banyaknya biaya yang harus dikeluarkan perusahaan untuk kompensasi dan mengganti kerugian, kecelakaan kerja juga menyebabkan perusahaan akan dirugikan oleh hilangnya hari kerja dan menurunnya produktivitas pekerja. Jika kasus kecelakaan terus bertambah dari waktu ke waktu dapat memberikan citra buruk bagi perusahaan karena tidak

dapat menjamin keselamatan pekerjanya.

Salah satu aspek penting yang harus diperhatikan perusahaan untuk meminimalisir terjadinya kecelakaan adalah dengan melakukan manajemen risiko. Menurut AS/NZS 4360, Manajemen Risiko adalah "*the culture, process and structures that are directed towards the effective management of potential opportunities and adverse effect*". Manajemen risiko menyangkut budaya, proses dan struktur dalam mengelola suatu risiko secara efektif dan terencana dalam suatu sistem manajemen yang baik (Ramli, 2010).

Manajemen risiko tidak terlepas dari berbagai risiko-risiko K3 yang dapat timbul dari setiap kegiatan di tempat kerja. Menurut OHSAS 18001, risiko K3 adalah kombinasi dari kemungkinan terjadinya kejadian berbahaya atau paparan dengan keparahan dari cedera atau gangguan kesehatan yang disebabkan oleh kejadian atau paparan tersebut (Ramli, 2010).

Maka secara sederhana dapat dikatakan bahwa manajemen risiko merupakan proses untuk mengelola risiko yang ada dalam setiap kegiatan (Ramli, 2010).

Manajemen pengelolaan risiko dilakukan dengan sebuah prinsip utama yang disebut *Calculated Risk* atau risiko yang diperhitungkan (Ramli, 2010). *Calculated risk* dilakukan untuk mengetahui seberapa besar tingkat risiko terhadap suatu *task* atau kegiatan yang dilakukan pekerja di tempat kerja. Apabila sebuah pekerjaan telah diketahui tingkat risikonya, maka akan dapat dilakukan pengendalian risiko terhadap pekerjaan tersebut sebelum terjadi kecelakaan. Hal ini tentu akan sangat bermanfaat bagi perusahaan untuk mencegah berbagai kerugian yang mungkin terjadi apabila risiko tersebut tidak segera dikelola dan dikendalikan.

Manajemen risiko meliputi identifikasi bahaya dan risiko, analisis dan penilaian risiko dan evaluasi risiko serta tindakan pengendalian yang dilakukan selama proses kerja berlangsung. Apabila aspek-aspek dalam manajemen risiko ini tidak diperhatikan dan dikelola dengan baik maka akan menimbulkan kerugian bagi perusahaan. Tidak hanya kecelakaan pada pekerja, namun dampak lainnya dapat berpengaruh pada kerugian finansial yang harus ditanggung oleh perusahaan serta kerugian yang harus diterima perusahaan akibat citra buruk yang ditimbulkan karena tidak melaksanakan manajemen risiko dengan baik. Oleh karena itu, perusahaan perlu melaksanakan manajemen risiko dengan baik khususnya dalam mengidentifikasi bahaya dan risiko serta melakukan penilaian risiko untuk dapat menentukan pengendalian yang dapat dilakukan sehingga dapat mencegah dan mengurangi kerugian (*loss*) yang dapat timbul.

Prinsip manajemen risiko berupa penilaian risiko tentu harus diterapkan oleh seluruh

industri maupun perusahaan. Terutama bagi perusahaan-perusahaan atau industri yang mempunyai tingkat risiko K3 yang tinggi dalam proses kerjanya. Salah satu perusahaan dengan tingkat risiko K3 yang cukup tinggi adalah PT BAF. PT BAF merupakan perusahaan manufaktur yang bergerak dalam bidang produksi filter. Salah satu filter yang diproduksi oleh PT BAF adalah filter yang digunakan untuk memisahkan uap maupun gas pada industri-industri kimia. Selain itu PT BAF juga memproduksi filter untuk gas panas yang digunakan pada industri pertambangan serta masih banyak jenis filter yang telah diproduksi oleh PT BAF. Namun dari semua filter yang diproduksi, produksi paling banyak dan yang paling rutin dilakukan oleh PT BAF adalah pembuatan *screen filter* atau sering disebut *spin pack*. *Spin pack* terbuat dari bahan dasar logam, alumunium atau *wire mesh* yang diproduksi berdasarkan pesanan dari berbagai industri sesuai dengan kebutuhannya masing-masing. Pembuatan *spin pack* baik yang berbahan dasar logam, alumunium maupun *wire mesh*, tentu membutuhkan proses dan rangkaian kerja yang cukup kompleks. Proses kerja yang kompleks dan rumit serta menggunakan alat-alat dan mesin mekanis tentunya akan menimbulkan risiko kecelakaan yang cukup besar bagi pekerja. Oleh karena itu perlu dilakukan analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF untuk mengetahui tingkat risiko yang ada serta rekomendasi pengendalian yang dapat dilakukan guna mencegah dan meminimalisir terjadinya kecelakaan. Adapun tujuan dari penelitian ini adalah:

1. Tujuan Umum

   Untuk memperoleh gambaran mengenai analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF tahun 2013
2. Tujuan Khusus
   1. Mengetahui proses atau tahapan kerja apa saja yang terdapat pada proses produksi *spin pack* di PT BAF.
   2. Mengetahui bahaya yang terdapat pada tahapan kerja pada proses produksi *spin pack* di PT BAF.
   3. Mengetahui nilai *consequence, likelihood, exposure* dan *basic risk* dari risiko-risiko K3 tanpa mempertimbangkan pengendalian yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   4. Mengetahui pengendalian risiko K3 yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   5. Mengetahui nilai *consequence, likelihood, exposure* dan *existing risk* dari risiko-risiko K3 dengan mempertimbangkan pengendalian yang sudah dilakukan pada

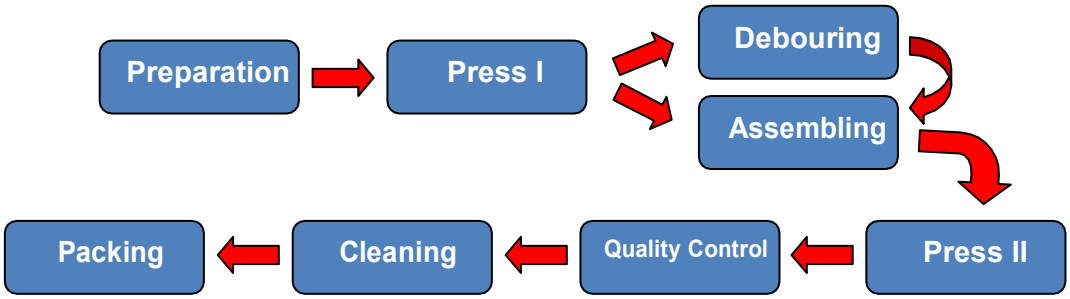
proses produksi *spin pack* di PT BAF.

6. Mengetahui nilai dari *risk reduction* pada proses produksi *spin pack* di PT BAF.
7. Mengetahui rekomendasi pengendalian yang masih memungkinkan dapat dilakukan untuk menurunkan risiko saat ini (*existing risk*) pada proses produksi *spin pack* di PT BAF.
8. Mengetahui nilai risiko prediksi (*predictive risk*) setelah ada rekomendasi pengendalian pada proses produksi *spin pack* di PT BAF.

2. HASIL PENELITIAN DAN PEMBAHASAN

2.1 Identifikasi Hazard dan Risiko

Tahap-tahap proses produksi *Spin Pack*



Gambar 1. Alur Proses Produksi *Spin Pack*

Identifikasi *hazard* dan risiko pada kegiatan proses produksi *spin pack* dilakukan dengan menggunakan *job hazard analysis* (JHA). JHA dibuat berdasarkan jenis pekerjaan dan bagiannya masing-masing. Tujuannya agar diketahui dengan jelas bahaya dan risiko disetiap masing-masing bagian.

1. Hazard dan Risiko pada Bagian *Preparation*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *preparation*, yaitu :

1. *Hazard* Mekanik : Sepihan material, mesin pemotong dan mesin perata.
   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk seprihan material, terjepit mesin calendaring, terpotong mesin pemotong material.
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban (material)

2. Hazard dan Risiko pada Bagian *Press I*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *press I*, yaitu:

1. *Hazard* Mekanik

   Risiko yang dapat ditimbulkan berupa terjepit dan tertimpa tooling, terpukul benda keras saat memasang tooling, terpotong mesin press, tergores dan tertusuk material

2. *Hazard* Fisik : Panas, bising, pencahayaan kurang baik, serpihan material.

   Risiko yang dapat ditimbulkan berupa ketidaknyamanan, kurangnya konsentrasi, kelelahan mata karena pencahayaan yang kurang baik, dan terkena percikan serpihan material. *azard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive*

   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

3. Hazard dan Risiko pada Bagian *Debouring*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *debouring*, yaitu :

1. *Hazard* Mekanik : serpihan material

   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk serpihan material

2. *Hazard* Fisik : Bising

   Risiko yang dapat ditimbulkan berupa ketdaknyamanan, kurangnya konsentrasi dan penurunan fungsi pendegaran.

3. *Hazard* Ergonomi : Postur janggal saat membawa beban

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban.

4. Hazard dan Risiko pada Bagian *Assembling*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *assembling*, yaitu :

1. *Hazard* Mekanik : produk dari logam bersisi tajam

   Risiko yang dapat ditimbulkan berupa tersayat produk

2. *Hazard* Ergonomi : Postur janggal saat membawa beban dan saat duduk terlalu lama.

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban dan duduk terlalu lama.

5. Hazard dan Risiko pada Bagian *Press II*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian

preparation, yaitu :

1. *Hazard* Mekanik : mesin press bertekanan tinggi.
   Risiko yang dapat ditimbulkan berupa terpotong mesin press.
2. *Hazard* Fisik : Panas, bising, pencahayaan yang kurang baik, serpihan material.
   Risiko yang dapat ditimbulkan berupa kelelahan mata karena, terkena percikan serpihan material
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive* serta mengangkat beban.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengangkat beban berat, duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

6. Hazard dan Risiko pada Bagian *Quality Control*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *quality control*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk
2. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

7. Hazard dan Risiko pada Bagian *Cleaning*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *cleaning*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk.
2. *Hazard* Fisik : zat kimia pembersih, getaran, radiasi gelombang *ultrasonic,* panas
   Risiko yang dapat ditimbulkan berupa terpapar zat kimia pembersih, terkena pajanan getaran dan radiasi *ultrasonic,* serta terbakar oleh panas dari *oven*.
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

8. Hazard dan Risiko pada Bagian *Packing*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *packing*, yaitu :

1. *Hazard* Mekanik : pisau mesin pemotong platik, mesin vacuum
   Risiko yang dapat ditimbulkan berupa tersayat mesin pemotong plastic dan terjepit mesin *vacuum*
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengemas produk ke dalam kardus.

2.2 Penilaian Risiko

Berikut ini penilaian beberapa risiko yang cukup signifikan dalam proses produksi:

1. Jari terpotong mesin pemotong material

   Risiko yang cukup besar pada bagian *preparation* adalah jari terpotong mesin pemotong material. Nilai *basic risk* untuk risiko tersebut adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat mengakibatkan kehilangan jari dan cacat permanen pada pekerja. *Exposure* (E) = 10 (*continuously*) karena pekerjaan tersebut dilakukan secara terus menerus dan berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena peristiwa ini memiliki kemungkinan kecil untuk terjadi.

   Pengendalian yang sudah dilakukan oleh pihak perusahaan adalah adanya program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign*, dan menyediakan sarung tangan untuk pekerja. Dari pengendalian tersebut maka nilai *existing risk* adalah 150 dengan kategori *substantial*. Penurunan risiko (*risk reduction*) sebesar 40%.

   Untuk mengurangi nilai risiko tersebut maka diberikan rekomendasi yaitu dengan pembuatan *Standard Operating Procedure (SOP)* untuk mesin pemotong, pengawasan rutin, pengecekan berkala untuk mesin, menggunakan mesin secara hati-hati dan sesuai prosedur serta disiplin dalam menggunakan alat pelindung diri (sarung tangan). Dari rekomendasi tersebut maka nilai *predictive risk* untuk risiko tersebut adalah 50 dengan kategori *priority 3.*

2. Terpotong mesin press

   Risiko yang cukup besar saat menggunakan mesin press adalah tangan atau jari dapat terpotong saat melakukan pencetakan produk. Hal ini disebabkan karena kekuatan mesin

yang cukup besar dan intensitas penggunaannya yang cukup tinggi. Nilai *basic risk* untuk risiko ini adalah 1500 (*very high*) dengan nilai *Consequences* (C) = 25 (*very serious*) karena dapat menyebabkan cacat permanen pada pekerja seperti kehilangan jari atau tangan. *Exposure* (E) = 10 (*continuously*) karena dilakukan secara terus menerus sepanjang hari selama jam kerja. *Likelihood/Probability* (P) = 6 (*likely*) karena kemungkinan untuk terjadinya kecelakaan adalah 50%-50%.

Pengendalian yang dilakukan perusahaan untuk mengurangi risiko tersebut adalah dengan menggunakan sensor otomatis pada mesin press. Sensor tersebut akan mendeteksi jika terdapat benda-benda yang melewatinya dan secara otomatis menghentikan kerja mesin press. Selain itu terdapat program pengawasan yang bernama *Bekaert Observation Program* dan pekerja juga dilengkapi dengan sarung tangan selama menggunakan mesin press. Berdasarkan risiko tersebut maka nilai *existing risk* adalah 250 dengan kategori *priority 1*. Penurunan risiko (*risk reduction*) sebesar 83,3%.

Untuk mengurangi risiko tersebut maka peneliti merekomendasikan dibuatnya *Standard Operating Procedure (SOP)* yang jelas dan ketat untuk penggunaan mesin press. Selain itu perlunya pengawasan rutin secara berkala pada pekerja. Pengecekan dan perawatan mesin dan fungsi sensor juga sangat diperlukan serta perlunya *guarding* di sisi kanan dan kiri mesin yang disesuaikan dengan kondisi dan posisi kerja karena sensor hanya berfungsi mendeteksi benda dari arah depan mesin. Berdasarkan rekomendasi tersebut maka didapatkan nilai *predictive risk* sebesar 50 dengan kategori *priority 3*.

3. Bising

Risiko bising terjadi ketika mesin *debouring* sedang beroperasi menghaluskan permukaan produk. Nilai *basic risk* untuk risiko ini adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat merusak kualitas pendengaran pekerja dan bersifat permanen. Selain itu juga menimbulkan ketidaknyamanan saat bekerja. *Exposure* (E) = 10 (*frequently*) karena terjadi lebih dari satu kali dalam sehari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya cukup kecil karena mesin dapat bekerja sendiri secara otomatis.

Pengendalian yang telah dilakukan oleh perusahaan adalah membatasi pekerja dengan cara meletakkan mesin *debouring* di dalam ruang tertutup. Program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign* di depan ruangan *debouring* serta pekerja diharuskan untuk menggunakan alat pelindung diri (*earmuff*)

ketika memasuki ruang *debouring*. Berdasarkan pengendalian tersebut maka didapatkan nilai *existing risk* sebesar 90 dengan kategori priority 3, Penurunan risiko (*risk reduction*) sebesar 64%.

Rekomendasi yang diberikan adalah membuat *Standard Operating Procedure (SOP)* dan *work permit* untuk memasuki ruang *debouring*. Selain itu diperlukan pengawasan secara rutin dan kedisplinan pekerja dalam menggunakan alat pelindung diri ketika berada di dalam ruang *debouring*. Berdasarkan rekomendasi tersebut maka didapatkan nilai predictive risk sebesar 15 dengan kategori *acceptable*.

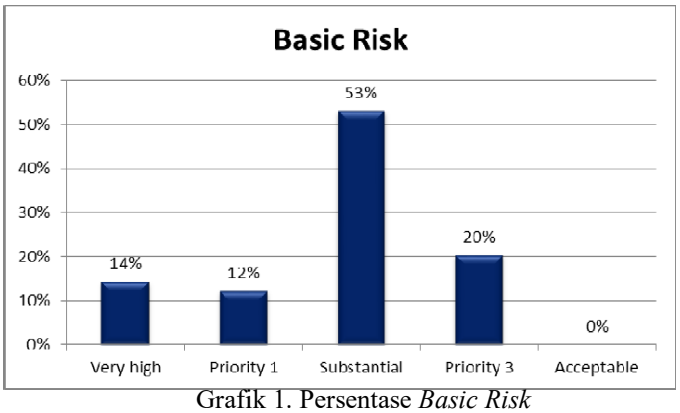
4. Postur janggal

Postur janggal dapat terjadi ketika pekerja melakukan pengemasan produk ke dalam kardus-kardus sebelum dikirimkan. Pengemasan produk dilakukan dalam bungkuk untuk memasukkan dan mengatur posisi produk di dalam kardus. Nilai *basic risk* untuk risiko ini adalah 150 dengan kategori *substantial* dengan nilai *Consequences* (C) = 15 (*serious*) karena dapat mengakibatkan nyeri dan cedera pada tulang pinggang. *Exposure* (E) = 10 (*frequently*) karena dilakukan pekerja secara berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya risiko ini cukup kecil. Belum terdapat pengendalian yang dilakukan perusahaan untuk risiko ini. Maka nilai *existing risk* sama dengan nilai *basic risk* yaitu 150 dengan kategori *substantial.*

Untuk mengurangi risiko postur janggal karena posisi bungkuk, maka peneliti merekomendasikan agar pekerja melakukan *stretching* 1 kali dalam 1 jam untuk melemaskan otot-otot tubuh agar tidak kaku. Selain itu sebaiknya pengemasan dilakukan dengan posisi yang benar agar pekerja tidak harus terlalu membungkuk. Nilai *predictive risk* dari rekomendasi tersebut adalah 15 dengan kategori *acceptable*.

Persentase Nilai *Basic Risk, Existing Risk* dan *Predictive Risk*

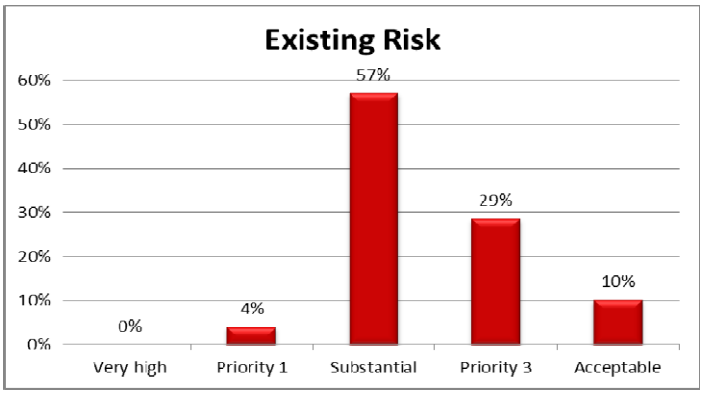
1. Basic Risk



Grafik 1. Persentase *Basic Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *basic risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 14% (7 aktivitas), kategori *priority 1* sebesar 12% (6 aktivitas), kategori *substantial* sebesar 53% (23 aktivitas), kategori *priority 3* sebesar 20% (10 aktivitas) dan kategori *acceptable* sebesar 0% (0 aktivitas).

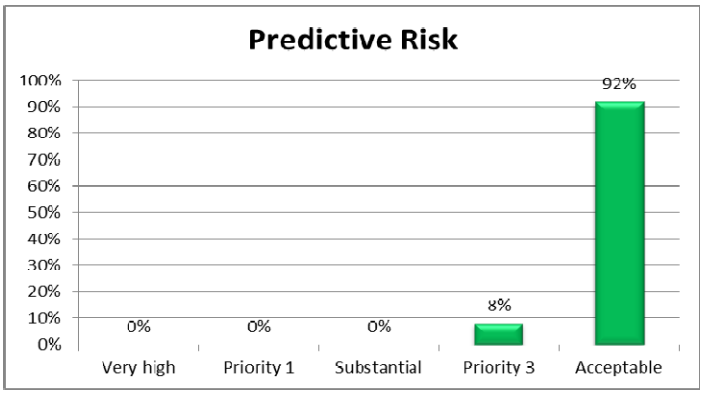
2. Existing Risk



Grafik 2. Persentase *Existing Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *existing risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 4% (2 aktivitas), kategori *substantial* sebesar 57% (28 aktivitas), kategori *priority 3* sebesar 29% (14 aktivitas) dan kategori *acceptable* sebesar 10% (5 aktivitas).

3. Predictive Risk



Grafik 3. Persentase *Predictive Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *predictive risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 0% (0 aktivitas), kategori *substantial* sebesar 0% (0 aktivitas), kategori *priority 3* sebesar 8% (4 aktivitas) dan kategori *acceptable* sebesar 92% (45 aktivitas).

3. SIMPULAN

Berdasarkan hasil dan analisis penelitian mengenai risiko keselamatan dan kesehatan kerja pada proses produksi *spin pack* di PT BAF tahun 2013, maka didapatkanlah simpulan sebagai berikut:

1. Terdapat 8 proses kerja pada proses produksi *spin pack*. Proses kerja tersebut terdiri dari *preparation* (persiapan material), *press I* (pencetakan), *debouring* (penghalusan), *assembling* (perakitan), *press II* (pressing), *quality control* (pengecekan), *cleaning* (pembersihan), *packing* (pengemasan).
2. Jenis bahaya paling dominan pada aktivitas proses produksi *spin pack* adalah bahaya mekanis seperti tertusuk, tergores, tersayat dan terpotong.
3. Ditemukan 7 risiko dalam 6 aktivitas dengan kategori *very high* pada *basic risk* di proses produksi *spin pack*. Aktivitas tersebut adalah pengambilan *tools*, pemasangan *tools,* pencetakan produk, membuka dan mengembalikan *tools* serta pada proses *pressing*.
4. Untuk *existing risk*, tidak ditemukan aktivitas dengan kategori *very high* namun terdapat 2 aktivitas dengan kategori *priority 1* yang membutuhkan perbaikan sesegera mungkin. Aktivitas tersebut yaitu pada proses pencetakan dan proses *pressing*.
5. Secara umum pengendalian yang sudah dilakukan oleh perusahaan adalah dengan

mengadakan program pengawasan yang disebut dengan *Bekaert Observation Program,* pemasangan *safety sign* dan penyediaan alat pelindung diri.

6. Berdasarkan program pengendalian yang sudah dilakukan perusahaan, berbagai risiko yang ada dapat dikurangi dengan persentase *risk reduction* antara 40% - 93,3%.
7. Pada *predictive risk*, sebagian besar risiko dapat diturunkan pada kategori *acceptable*. Namun masih terdapat 4 aktivitas yang berada pada kategori *priority 3*.

4. DAFTAR PUSTAKA

Alfiah, Suzi. 2012. *Penilaian Risiko Keselamatan dan Kesehatan Kerja pada Kegiatan Operasi dan Produksi PT Pertamina Geothermal Energy Area Lahendong Tahun 2012*. Skripsi. Depok: Fakultas Kesehatan Masyarakat Universitas Indonesia.

"Angka Kecelakaan Kerja Lima Tahun Terakhir Meningkat". http://www.poskotanews.com/2012/06/01/angka-kecelakaan-kerja-lima-tahun-terahir-cendrung-naik/ (diakses pada 14 Maret 2013 pukul 15.33 WIB)

European Agency for Safety and Health at Work. "Definitions". https://osha.europa.eu/en/topics/riskassessment/definitions

Jamsostek. "Setiap Hari Ada 9 Peserta Jamsostek Tewas Kecelakaan Kerja". http://www.jamsostek.co.id/content/news.php?id=3957

IMPLEMENTASI PENILAIAN RISIKO
DALAM MENUNJANG PENCAPAIAN TUJUAN INSTANSI PENDIDIKAN

Ahmad Dief Aritzah
182420049

1. Abstrak

Penelitian ini dilakukan dalam rangka memberikan informasi bagi kepala lembaga pendidikan untuk mengantisipasi risiko yang dihadapi oleh lembaga mereka. Lembaga pendidikan perlu melakukan penilaian risiko karena lembaga akan selalu menghadapi perubahan signifikan yang terjadi karena perubahan internal dan eksternal. Langkah penilaian risiko dimulai dari menetapkan tujuan lembaga. Penting untuk membagi tujuan lembaga menjadi lebih spesifik dengan merumuskan tujuan untuk setiap program. Langkah kedua penilaian risiko adalah identifikasi risiko. Pada langkah ini, risiko perlu diidentifikasi dan dikategorikan. Selain itu, faktor-faktor yang menyebabkan risiko juga harus dianalisis. Langkah terakhir penilaian risiko adalah menganalisis risiko. Di sini, lembaga akan mencoba menentukan status risiko dan peta risiko sehingga respons yang tepat dapat diambil untuk menangani risiko tersebut

Kata kunci : Penilaian risiko, Perumusan tujuan, Identifikasi risiko, Analisis risiko

2. Pendahuluan

Instansi pendidikan sebagaimana halnya dengan organisasi dan instansi lainnya pasti akan selalu berhadapan dengan perubahan, baik itu perubahan yang berasal dari dalam maupun dari luar instansi pendidikan. Perubahan pengelolaan pendidikan yang tidak lagi terpusat, perubahan kurikulum hingga berubahnya peraturan pemerintah kesemuanya menuntut perhatian serius dari instansi pendidikan. Perubahan dalam dunia pendidikan terjadi begitu cepat dimana semua perubahan ini diharapkan dapat meningkatkan kualitas pendidikan di Indonesia.

Kualitas pendidikan di Indonesia saat ini banyak sekali menjadi sorotan publik. Banyaknya permasalahan yang membelenggu dunia pendidikan mulai dari pengelolaan aset dan keuangan oleh instansi pendidikan hingga rendahnya mutu lulusan yang dihasilkan dari setiap jenjang sekolah kesemuanya membawa efek negatif bagi dunia pendidikan di Indonesia. Kualitas lulusan sarjana di Indonesia baik itu S1, S2 maupun S3 dipandang jauh lebih rendah kualitasnya daripada lulusan negara tetangga, seperti Malaysia. Selain itu, era globalisasi juga menuntut perhatian lebih dari instansi pendidikan karena instansi pendidikan di Indonesia harus

bersaing dengan instansi pendidikan dari negara lain yang bebas membuka cabangnya di Indonesia. Kesemua perubahan ini pada akhirnya akan menjadi risiko yang harus dihadapi oleh instansi pendidikan. Jika risiko ini tidak diolah dengan baik, maka tujuan yang telah ditetapkan oleh setiap instansi pendidikan bisa jadi tidak akan bisa tercapai. Oleh karena itu, penting kiranya bagi setiap instansi pendidikan untuk mengelola risiko sehingga keefektifan tujuan instansi pendidikan bisa diwujudkan.

Penilaian risiko merupakan salah satu unsur dalam Sistem Pengendalian Intern Pemerintah (SPIP) dimana pemerintah telah menetapkan aturan yang jelas mengenai pentingnya SPIP bagi instansi pemerintah dengan dikeluarkannya Peraturan Pemerintah No. 60 Tahun 2008. Dalam peraturan tersebut, SPIP didefinisikan sebagai proses yang integral pada tindakan dan kegiatan yang dilakukan secara terus menerus oleh pimpinan dan seluruh pegawai untuk memberikan keyakinan memadai atas tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan aset negara dan ketaatan terhadap peraturan perundang-undangan yang diselenggarakan secara menyeluruh pada lingkungan pemerintah pusat dan pemerintah daerah. Instansi pendidikan terutama yang berada dalam lingkup pemerintah hendaknya juga turut serta mematuhi peraturan tersebut dengan mengimplementasikan SPIP dalam lingkup organisasinya.

Berdasarkan definisi SPIP di atas, dapat dilihat bahwa terdapat 4 tujuan yang hendak dicapai oleh SPIP yaitu, (i) efisiensi dan keefektifan pencapaian tujuan negara, (ii) keandalan pelaporan keuangan, (iii) pengamanan aset negara dan (iv) ketaatan terhadap peraturan perundang-undangan. Tujuan tersebut diharapkan dapat dicapai dengan memperhatikan unsur-unsur pembentuk SPIP, yaitu (i) lingkungan pengendalian yang kondusif, (ii) penilaian risiko, (iii) aktivitas pengendalian, (iv) informasi dan komunikasi, dan (v) pemantauan.

Mengingat banyaknya perubahan dan tuntutan yang tinggi akan kualitas pendidikan Indonesia, instansi pendidikan-khususnya yang berada di bawah naungan pemerintah-perlu melakukan penilaian risiko. Hal ini penting untuk dilakukan dengan segera karena penilaian risiko akan membantu instansi pendidikan untuk mengelola risiko tersebut dan meminimalisir dampak yang dapat menghambat pencapaian tujuan instansi pendidikan. Dengan adanya penilaian risiko, efisiensi dan keefektifan dalam memberikan pelayanan akan meningkat sehingga instansi pendidikan dapat memberikan pelayanan yang berkesinambungan kepada *stakeholders*. Penilaian risiko juga menjadi dasar bagi instansi pendidikan dalam menyusun rencana strategis dan membantu menghindari pemborosan karena seluruh risiko yang mungkin terjadi telah diantisipasi dan dikendalikan oleh instansi pendidikan.

3. Pembahasan

A. Risiko dan Proses Penilaian Risiko

David Mc Namee & Georges Selim (1998) mendefinisikan risiko sebagai konsep yang digunakan untuk menyatakan ketidakpastian atas kejadian dan atau akibatnya yang dapat berdampak secara material bagi tujuan organisasi. Definisi yang hampir sama disampaikan oleh Bringham (1999) yang menyatakan bahwa risiko adalah bahaya, petaka; kemungkinan menderita rugi atau mengalami kerusakan. Pemerintah Indonesia melalui melalui Bank Indonesia dan Peraturan Pemerintah juga memberikan definisi risiko. Risiko adalah potensi timbulnya suatu kerugian akibat terealisasinya suatu kejadian tertentu yang diperkirakan (Bank Indonesia, 2003). Sedangkan, pengertian risiko berdasarkan Peraturan Pemerintah No. 60 Tahun 2008 yaitu kemungkinan kejadian yang mengancam pencapaian tujuan dan sasaran instansi pemerintah.

Dari pengertian tersebut dapat ditarik kesimpulan bahwa risiko mengandung tiga unsur pembentuk risiko, yaitu (i) kemungkinan kejadian atau peristiwa, (ii) dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi, dan (iii) kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas). Ketiga unsur tersebut harus selalu dipenuhi oleh instansi pendidikan ketika akan mengidentifikasi risiko.

Risiko bisa timbul dari sumber internal dan sumber eksternal dari suatu instansi pendidikan. Risiko yang berasal dari sumber eksternal mencakup munculnya peraturan perundang-undangan baru, perkembangan teknologi, bencana alam dan gangguan keamanan. Sementara itu, sumber internal risiko terdiri atas keterbatasan dana operasional, sumber daya manusia yang tidak kompeten, peralatan yang tidak memadai, kebijakan prosedur yang tidak jelas, dan suasana kerja yang tidak kondusif. Selain kedua sumber di atas, risiko juga bisa disebabkan oleh faktor lain, misalnya pengeluaran program yang tidak tepat, pelanggaran terhadap pengendalian dana, ketidaktaatan terhadap peraturan perundang-undangan, risiko yang melekat pada sifat misinya atau pada signifikansi (BPKP, 2010). Peraturan Pemerintah No. 60 Tahun 2008 menegaskan bahwa pimpinan instansi pemerintah wajib melakukan penilaian risiko. Pihak pimpinan instansi pemerintah wajib melakukan penilaian risiko atas faktor-faktor yang mengancam tercapainya tujuan yang telah ditetapkan, baik itu tujuan instansi pendidikan secara keseluruhan maupun tujuan dari setiap kegiatan yang dilakukan oleh instansi pendidikan.

Penilaian resiko adalah metode sistematis dalam melihat aktivitas kerja, memikirkan apa yang dapat menjadi buruk, dan memutuskan kendali yang cocok untuk mencegah terjadinya kerugian, kerusakan, atau cedera di tempat kerja. Penilaian ini harus juga melibatkan pengendalian yang diperlukan untuk menghilangkan, mengurangi,atau meminimalkan resiko (NSH Health Scotland, 2010). Definisi lain tertuang dalam Peraturan Pemerintah No. 60 Tahun 2008 yang menyatakan bahwa penilaian risiko adalah proses yang dilakukan oleh suatu instansi atau organisasi dan merupakan bagian yang integral dari proses pengelolaan risiko dalam pengambilan keputusan risiko dengan melakukan tahap identifikasi rasio, analisis rasio dan evaluasi risiko. Penilaian risiko bertujuan untuk (i) mengidentifikasi dan menguraikan semua risiko-risiko potensial yang berasal baik dari faktor internal maupun faktor eksternal, (ii) memeringkat risiko-risiko yang memerlukan perhatian manajemen instansi dan yang memerlukan penanganan segera atau tidak memerlukan tindakan lebih lanjut, dan (iii) memberikan suatu masukan atau rekomendasi untuk meyakinkan bahwa terdapat risiko-risiko yang menjadi prioritas paling tinggi untuk dikelola dengan efektif (BPKP, 2010).

Penilaian risiko dilakukan terhadap faktor-faktor yang mengancam tercapainya tujuan instansi pendidikan. Oleh karena itu, penetapan tujuan baik itu tujuan instansi maupun tujuan kegiatan merupakan langkap awal dalam melakukan penilaian risiko. Setelah tujuan ditetapkan, instansi pendidikan akan melakukan identifikasi terhadap risiko-risiko yang bisa menghambat pencapaian tujuan tersebut. Identifikasi risiko bisa dilakukan baik terhadap sumber risiko internal, sumber risiko eksternal maupun sumber risiko yang lain. Terhadap setiap risiko yang berhasil diidentifikasi, instansi pendidikan kemudian menganalisis risiko tersebut untuk

mengetahui pengaruhnya terhadap pencapaian tujuan. Hasil analisis risiko bisa dijadikan patokan bagi pimpinan instansi pendidikan untuk melakukan pengendalian terhadap risiko tersebut sehingga kemungkinan dan efek terjadinya risiko tersebut dapat diminimalisir.

B. Perumusan Tujuan

Langkah pertama dalam proses penilaian risiko adalah penetapan tujuan baik itu tujuan strategik dari suatu instansi maupun tujuan operasional. Dalam kaitannya dengan instansi pemerintah, Peraturan Pemerintah No. 60 Tahun 2008 mengatur bahwa tujuan strategik instansi pemerintah harus memuat pernyataan dan arahan yang spesifik, terukur, dapat dicapai, realistis dan terikat waktu. Tujuan strategik ini harus disampaikan kepada seluruh pegawai. Untuk mencapai tujuan tersebut, pimpinan instansi pemerintah wajib menetapkan strategi operasional yang konsisten dan strategi manajemen terintegrasi serta rencana penilaian risiko. Sedangkan, tujuan pada tingkat kegiatan harus ditetapkan dengan mempertimbangkan hal-hal sebagai berikut: (i) berdasarkan pada tujuan dan rencana strategis instansi pemerintah, (ii) saling melengkapi, saling menunjang, dan tidak bertentangan satu dengan lainnya, (iii) relevan dengan seluruh kegiatan utama instansi pemerintahan, (iv) mengandung unsur kriteria pengukuran, (v) didukung sumber daya yang cukup, dan (vi) melibatkan seluruh tingkat pejabat dalam proses penetapannya.

C. Identifikasi Risiko

Identifikasi risiko adalah proses menetepkan apa, dimana, kapan, mengapa dan bagaimana sesuatu dapat terjadi sehingga dapat berdampak negatif terhadap pencapaian tujuan (PP No 60 Tahun 2008). Identifikasi risiko bisa dilakukan secara retrospektif dan prospektif (BPKP, 2010). Instansi pemerintah dapat melakukan identifikasi risiko retrospektif dengan cara mengidentifikasi risiko-risiko yang sebelumnya pernah terjadi dalam instansi tersebut. Karena risiko ini pernah terjadi, risiko tersebut lebih mudah untuk ditetapkan dan dikendalikan oleh instansi pemerintah. Identifikasi risiko secara retrospektif bisa dilakukan dengan mencari informasi dari beberapa sumber, seperti daftar risiko yang dibuat pada periode sebelumnya, dokumen dan laporan yang disimpan perusahaan, laporan audit dan hasil evaluasi lainnya, informasi dari sumber eksternal. Berkebalikan dengan risiko retrospektif, risiko prospektif lebih sulit untuk diidentifikasi karena risiko ini belum pernah dialami suatu instansi. Instansi berusaha untuk membuat prediksi tentang kemungkinan-kemungkinan buruk yang akan dihadapi oleh instansi baik apakah risiko tersebut dapat dikendalikan maupun sulit dikendalikan. Brainstorming dan analisis SWOT merupakan dua metode penting yang bisa dilakukan untuk mengidentifikasi risiko prospektif.

Salah satu tujuan dari identifikasi risiko adalah untuk menetapkan risiko (BPKP, 2010). Dalam menetapkan risiko, setiap divisi dalam instansi pemerintah harus berusaha untuk mengetahui di mana risiko bisa timbul pada divisi tersebut serta mengidentifikasi penyebab munculnya risiko dan bagaimana risiko tersebut dapat menghambat pencapaian tujuan. BPKP (2010) memberikan panduan beberapa kejadian yang bisa menghambat pencapaian tujuan, yaitu (i) tujuan menjadi lebih lama tercapainya, (ii) tujuan tercapai hanya sebagian (< 100%),

(iii) tujuan tidak tercapai sama sekali, (iv) tujuan tercapai namun dengan biaya yang lebih tinggi, dan (v) tujuan melenceng dari yang telah ditetapkan.

Tujuan kedua dari identifikasi risiko adalah mengkategorisasikan risiko (BPKP, 2010). Risiko dapat dikelompokkan atas dasar (i) jenis risiko, misalkan risiko teknologi, risiko keuangan/ekonomi, risiko sumber daya manusia, risiko kesehatan, risiko politik, risiko hukum, risiko keamanan, (ii) sumber risiko, misalkan risiko eksternal (politik, ekonomi, bencana alam) dan risiko internal (reputasi, keamanan, manajemen, informasi untuk pengambilan keputusan), (iii) penerima risiko, misalkan orang, risiko reputasi, hasil program, bangunan dan aset, lingkungan, pelayanan, (iv) dampak risiko, misalkan risiko rendah, risiko menengah, dan risiko tinggi, (v) kemampuan mengendalikan, misalnya risiko yang sangat terkendali, kurang

terkendali, dan tidak/sangat sulit dikendalikan, dan (vi) hirarki risiko, misalnya risiko strategik, risiko program, risiko proyek, dan risiko operasional.

Setelah risiko ditetapkan dan dikelompokkan, identifikasi rasio ini pada akhirnya akan menghasilkan daftar risiko. Daftar risiko merupakan suatu tabel yang berisi sumber risiko dan penyebab terjadinya risiko. Daftar risiko akan menjadi dasar dalam membuat model pernyataan risiko. Ada dua pilihan model pernyataan risiko yang dikembangkan oleh BPKP

(2010), yaitu:

Gambar 1. Model Pernyataan Risiko 1

Untuk mencapai ketiga tujuan di atas, maka proses identifikasi risiko dilakukan dengan melalui tahap-tahap sebagai berikut: (i) penetapan unit risiko, yaitu penetapan organisasi atau unit mana yang akan diidentifikasi risikonya dan tingkatan risikonya, (ii) pemahaman terhadap tupoksi organisasi/unit yang bersangkutan, (iii) pemahaman terhadap aktivitas utama dari organisasi, (iv) reviu atas kriteria risiko yang ada, mencakup tingkat tolerasi risiko, kriteria dampak, kriteria kemungkinan, dan kriteria tingkat keefektifan pengendalian yang sudah ada, (v) pembuatan daftar risiko, dan (vi) pembuatan peta atau profil risiko (BPKP, 2010)

D. Analisis Risiko

Peraturan Pemerintah No. 60 Tahun 2008 mendefinisikan analisis risiko sebagai proses penilaian terhadap risiko yang telah teridentifikasi dalam rangka mengestimasi kemungkinan munculnya dan besaran dampaknya untuk menetapkan level atau status risikonya. Status risiko ditentukan berdasarkan kombinasi antara kemungkinan (probabilitas/frekuensi) terjadinya risiko dan dampak (efek) jika risiko terjadi. BPKP (2010) memberikan panduan bagaimana instansi pemerintah melakukan analisis risiko. Langkah-langkah analisis risiko tersebut adalah sebagai berikut:

1. Menetapkan kemungkinan/probabilitas/frekuensi terjadinya risiko
   Tabel 1: Kerangka Pengukuran Probabilitas

Probabilitas		**Kriteria**
Rating	**%**	
1	0–10	Sangat tidak mungkin/hampir mustahil
2	10–30	Kecil kemungkinan tapi tidak mustahil
3	30–50	Kemungkinan terjadi
4	50–90	Sering terjadi
5	>90	Hampir pasti terjadi

Sumber: BPKP, 2010

Tabel 2: Ukuran Kualitatif Kemungkinan/Frekuensi

Level	Deskriptor	Contoh Deskripsi Rinci	Frekuensi
1	Sangat jarang	Kejadiannya muncul hanya dalam keadaan tertentu	Kurang dari sekali dalam 10 tahun
2	Jarang	Kejadiannya dapat muncul pada saat yang sama	Paling sedikit sekali dalam 10 tahun
3	Moderat	Kejadiannya seharusnya muncul pada saat yang sama	Paling sedikit sekali dalam 5 tahun
4	Sering	Kejadiannya mungkin muncul pada kebanyakan situasi	Paling sedikit sekali dalam 1 tahun
5	Hampir pasti /Sangat sering	Kejadiannya diharapkan muncul pada kebanyakan situasi	Lebih dari satu kali dalam setahun

Sumber: BPKP, 2010

2. Menentukan dampak dan besaran dari setiap risiko.
   Tabel 3: Kerangka Pengukuran Dampak

Level	Rating Dampak	Keterangan
5	Sangat tinggi/ katastropik	Mengancam program dan organisasi serta *stakeholders*. Kerugian sangat besar bagi organisasi dari segi keuangan maupun politis.
4	Besar	Mengancam fungsi program yang efektif dan organisasi. Kerugian cukup besar bagi organisasi dari segi keuangan maupun politis.
3	Menengah/medium	Mengganggu administrasi program. Kerugian keuangan dan politis cukup besar.
4	Kecil	Mengancam efisiensi dan keefektifan beberapa aspek program. Kerugian kurang material dan sedikit mempengaruhi *stakeholders.*
5	Sangat rendah/tidak signifikan	Dampaknya dapat ditangani pada tahap kegiatan rutin. Kerugian kurang material dan tidak mempengaruhi *stakeholders*.

Sumber: BPKP, 2010

3. Menetapkan status risiko dan peta risiko

Formula untuk menghitung status risiko menurut BPKP (2010) adalah sebagai berikut: Status Risiko = Probabilitas x Dampak

Berikut adalah tabel untuk menentukan peta risiko. Tabel 4: Peta Risiko

Matriks Analisis Risiko			**Dampak**				
			1	**2**	**3**	**4**	**5**
Deskripsi	**Prob.**	**Frek.**	**Tidak Signifikan**	**Kecil**	**Medium**	**Besar**	**Katas-tropik**
Hampir pasti	90%	5	Moderat	Tinggi	Ekstrim	Ekstrim	Ekstrim
Kemungkinan besar	70%	4	Rendah	Moderat	Tinggi	Ekstrim	Ekstrim
Mungkin	50%	3	Rendah	Moderat	Moderat	Tinggi	Ekstrim
Kemungkinan kecil	30%	2	Sangat rendah	Rendah	Moderat	Moderat	Tinggi
Sangat jarang	10%	1	Sangat rendah	Sangat rendah	Rendah	Rendah	Moderat

Sumber: BPKP, 2010

Tabel 5: Rating Risiko

Deskripsi	**Level**	**Level dimulai dari status**
Ekstrim	5	15
Tinggi	4	10
Moderat	3	5
Rendah	2	3
Sangat rendah	1	1

Sumber: BPKP, 2010.

4. Menentukan respon terhadap risiko
   Tabel 6: Kriteria Respon Risiko

Status Risiko	**Kriteria untuk Manajemen Risiko**		**Yang Bertanggung Jawab**
1 – 3	Dapat diterima	Dengan pengendalian yang cukup	Manajer Operasi
4 – 5	Dipantau	Dengan pengendalian yang cukup	Manajer Operasi
6 – 9	Diperlukan pengendalian manajemen	Dengan pengendalian yang cukup	Manajer Operasi
10 – 14	Harus menjadi perhatian manajemen (*urgent*)	Dapat Diterima hanya dengan Pengendalian yang sangat baik	CEO
15 – 25	Tak dapat diterima	Dapat diterima hanya dengan pengendalian yang sangat baik	Komisaris

Sumber: BPKP, 2010

5. Memberi informasi kepada pimpinan
   Tabel 7: Informasi Pengelolaan Risiko

Status Risiko	**Apa yang Terjadi**	**Apa yang Harus Dilakukan**
Ekstrim	□ Tujuan dan hasil tidak tercapai. □ Mengakibatkan kerugian keuangan yang besar. □ Mengurangi kapabilitas instansi. □ Reputasi instansi sangat menurun.	□ Pengelolaan bersifat urgen dan aktif yang melibatkan pimpinan tingkat tinggi. □ Strategi risiko wajib dilaksanakan secepatnya. □ Pendekatan yang segera dan tepat serta pelaporan secara rutin
Tinggi	□ Beberapa tujuan dan hasil tidak tercapai.	□ Perlu pengelolaan aktif dan reviu rutin.

	□ Mengakibatkan kerugian keuangan yang cukup besar. □ Mengurangi kapabilitas instansi. □ Cukup menurunkan reputasi	□ Strategi harus dilaksanakan terutama difokuskan pada pemeliharaan kendali yang sudah baik. □ Pendekatan yang tepat.
Medium	□ Mengganggu kualitas atau ketepatan waktu dari tujuan dan hasilnya. □ Mengakibatkan kerugian	□ Perlu pengelolaan dan reviu secara rutin. □ Perlu pengendalian intern yang efektif dan pemantauan.

	keuangan yang dapat diterima dengan wajar. □ Mengurangi kapabilitas instansi dalam tingkatan normal. □ Menurunkan reputasi dalam tingkat wajar.	□ Strategi risiko harus dilaksanakan.
Rendah	□ Mengganggu kualitas, kuantitas, dan ketepatan waktu dari tujuan dan hasil. □ Mengakibatkan kerugian keuangan, penurunan kapabilitas dan reputasi yang tidak besar.	□ Prosedur rutin yang cukup untuk menanggung dampak. □ Perlu pengendalian intern yang efektif dan pemantauan. □ Strategi yang fokus pada pemantauan dan reviu terhadap prosedur pengendalian yang sudah ada
Sangat Rendah	□ Dampak terhadap pencapaian tujuan adalah sangat kecil. □ Kerugian keuangan, penurunan kapabilitas, dan reputasi adalah sangat kecil.	□ Hanya perlu pemantauan singkat. □ Pengendalian normal sudah mencukupi. □ Jika sama sekali tidak diperhatikan, risiko-risiko ini dapat meningkat statusnya/prioritasnya.

Sumber: BPKP, 2010

E. Implementasi Penilaian Risiko pada Instansi Pendidikan

Penilaian risiko perlu dilakukan oleh instansi pendidikan mengingat terdapat banyak perubahan terjadi dalam dunia pendidikan dimana dampak dari perubahan perlu dikelola untuk meminimalisir kegagalan pencapaian tujuan yang telah ditetapkan. Berikut ini adalah gambaran bagaimana instansi pendidikan bisa mengimplementasikan penilaian risiko yang tahapannya dimulai dari menetapkan tujuan instansi dan tujuan tingkat kegiatan, identifikasi risiko dan analisis risiko.

1) Merumuskan Tujuan Instansi dan Tujuan Tingkat Kegiatan

Tujuan instansi pendidikan hendaknya terkait dengan visi dan misi yang telah ditetapkan karena tujuan merupakan implementasi dari visi dan misi. Visi, misi dan tujuan yang akan disajikan dalam makalah ini akan mengadopsi visi dan misi dari salah satu universitas pendidikan di Indonesia, yaitu Universitas Negeri Yogyakarta

2) Identifikasi Risiko

Identifikasi risiko dilakukan dengan melalui tiga tahap penting, yaitu menetapkan risiko, mengkategorisasikan risiko dan membuat daftar risiko.

Menetapkan Risiko

Direktorat Jenderal Pendidikan Tinggi memberikan panduan kriteria-kriteria yang harus dipenuhi dalam menerbitkan jurnal ilmiah berskala internasional. Kriteria tersebut adalah sebagai berikut:

1. Bahasa yang digunakan adalah bahasa PBB (Inggris, Perancis, Spanyol, Arab, Cina)
2. Pengelolaan naskah sedemikian rupa sehingga naskah yang diterima cepat terbit (rapid review) dan ada keteraturan terbit
3. Jurnal berkualitas (prestisius), bisa dilihat dari daftar penelaah naskahnya dan *Editorial Board*-nya yaitu pakar di bidangnya dalam dan luar negeri.
4. Dibaca oleh banyak orang di bidangnya, bisa dilihat dari distribusi/peredarannya (*circulation*).
5. Menjadi acuan bagi banyak peneliti (citation).
6. Tercantum dalam *Current Content* dan sejenisnya.
7. Artikel yang dimuat berkualitas, bisa dilihat dari kemutakhiran topik dan daftar acuannya.
8. Penyumbang artikel/naskah berasal dari banyak negara
9. Penelaah berasal dari banyak negara yang terkemuka di bidangnya.
10. Menawarkan *off-prints/reprints*.
11. Terbit teratur sesuai dengan jadwal yang ditentukan.
12. Penerbitan jurnal tidak terkendala oleh dana.
13. Bukan jurnal Jurusan, Fakultas, Universitas atau Lembaga yang mencerminkan derajat kelokalan. Seyogyanya diterbitkan oleh himpunan profesi.
14. Memberi kesempatan penulis artikel membaca contoh cetak
15. Artikel yang dominan (kalau bisa > 80%), berupa artikel orisinil (hasil penelitian), bukan sekadar review atau ulasan.
16. Kadar sumber acuan primer >80%, derajat kemutakhiran acuan >80%.
17. Tersedia Indeks di setiap volume.
18. Ketersediaan naskah tidak menjadi masalah (ITB, 2009)

Dengan melihat pada kriteria-kriteria di atas, maka beberapa kriteria tersebut bisa membawa risiko kegagalan UNY menerbitkan jurnal ilmiah berskala internasional. Tidak semua kriteria di atas menjadi risiko bagi UNY untuk mencapai tujuannya karena untuk bisa disebut sebagai risiko harus memenuhi tiga unsur pembentuk risiko, yaitu

1. Kejadian atau peristiwa
2. Kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas).
3. Dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi) Berikut adalah ilustrasi risiko yang bisa menghambat UNY dalam menerbitkan jurnal internasional.

Tabel 8: Ilustrasi Risiko

No.	**Uraian Risiko**	**Kejadian /Peristiwa**	**Kemungkinan Kejadian/Peristiwa**	**Dampak /Konsekuensi**
1	Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Ya	Ya Kejadian/peristiwa ini baru merupakan kemungkinan karena bisa saja pengelola di kemudian hari mendapatkan *paper* berkualitas tinggi.	Jurnal tidak bisa terbit teratur atau terlambat terbit.
2	Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Ya	Ya Ada kemungkinan pengelola akan menghadapi peristiwa tersebut karena masih terbatasnya jaringan kerja sama antara UNY dengan universitas di luar negeri.	Tidak memenuhi kriteria penerbitan jurnal internasional yang ditetapkan Dikti.
3	Kesulitan dalam	Ya	Ya	Tidak memenuhi

	mencari penulis artikel dari luar negeri.		Terbatasnya ruang lingkup kerja sama dengan civitas akademika serta peneliti luar negeri	kriteria penerbitan jurnal internasional yang ditetapkan Dikti.

			kemungkinan bisa menghambat pengelola dalam mendapatkan artikel dari penulis luar negeri	
4	Keterbatasan distribusi/pemasaran jurnal.	Ya	Ya Belum dikenalnya UNY di dunia internasional kemungkinan bisa menjadi faktor penghambat distribusi jurnal ke luar negeri.	Artikel di jurnal tidak dibaca dan tidak dikutip (disitasi) oleh peneliti lain

Dari 18 kriteria penerbitan jurnal internasional, hanya 4 faktor yang bisa ditetapkan sebagai risiko. Faktor lain bukan merupakan risiko karena tidak memenuhi salah satu unsur pembentuk risiko sebagaimana dijelaskan dalam uraian di bawah ini.

1. Bahasa yang digunakan yaitu bahasa PBB bukan merupakan risiko karena ada banyak peneliti yang memiliki potensi kemampuan berbahasa asing terutama bahasa Inggris.
2. Keteraturan dan tepat waktu dalam penerbitan merupakan akibat yang timbul karena risiko sedikitnya naskah yang diterima oleh pengelola. Dengan demikian keteraturan dan tepat waktu dalam penerbitn bukan merupakan risiko bagi pengelola melainkan dampak dari risiko keterbatasan naskah.
3. Acuan bagi banyak peneliti bukan merupakan risiko melainkan dampak dari risiko tidak dibacanya jurnal yang diterbitkan pengelola UNY karena keterbatasan distribusi jurnal.
4. Ketersediaan *current content*, *offprint/reprint* dan indeks di setiap volume penerbitan bukan merupakan risiko yang dihadapi pengelola karena pengelola memiliki kapabilitas memadai untuk memenuhi kriteria tersebut.
5. Keterbatasan dana merupakan masalah yang dihadapi oleh pengelola jurnal UNY saat ini sehingga hal ini bukan merupakan risiko. Unsur pembentuk risiko yang kedua adalah kemungkinan peristiwa/kejadian terjadi di masa mendatang dan unsur ini tidak dipenuhi sehingga keterbatasan dana tidak tepat jika diidentifikasi sebagai risiko.
6. Jurnal diterbitkan oleh himpunan profesi juga bukan merupakan risiko bagi pengelola karena UNY telah memiliki kerjasama dengan himpunan profesi.
7. Penulis artikel bisa melihat contoh cetak jurnal juga bukan merupakan risiko karena sebagian besar jurnal di UNY selama ini didistribusikan kepada penulis artikel.

Mengkategorisasikan Risiko

Pengelompokkan risiko dilakukan dengan mengidentifikasi jenis risiko, sumber risiko, penerima risiko, level risiko, pengendalian risiko dan hierarki risiko. Tabel 9 di bawah ini memuat kategorisasi risiko terhadap risiko yang berhasil diidentifikasi dari tahap penetapan risiko.

Membuat Daftar Risiko

Langkah terakhir dalam proses identifikasi risiko adalah membuat daftar risiko. Untuk keperluan penyusunan daftar risiko, faktor-faktor yang menyebabkan risiko tersebut terjadi harus ditemukan. Tabel di bawah ini memuat contoh daftar risiko dari risiko yang telah diidentifikasi dan dikelompokkan pada langkah sebelumnya:

Tabel 10: Daftar Risiko

No.	Risiko Teridentifikasi	Faktor Penyebab
1	Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Budaya penelitian masih terbatas dimana penelitian selama ini dilakukan oleh akademisi untuk memenuhi persyaratan kenaikan pangkat dan jabatan fungsional. Akibatnya, kualitas paper yang dihasilkan cenderung rendah dan belum layak untuk dipublikasikan dalam lingkup internasional.
2	Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Pengelola kurang aktif dalam mengikuti konferensi/seminar internasional sehingga jaringan kerja dengan akademisi/peneliti luar negeri menjadi terbatas. Padahal, konferensi/seminar internasional merupakan sarana untuk mendapatkan reviewer secara langsung.
3	Kesulitan dalam mencari penulis artikel dari luar negeri	Pengelola kurang aktif dalam mengikuti konferensi/seminar internasional sehingga jaringan kerja dengan akademisi/peneliti luar negeri menjadi terbatas. Padahal, konferensi/seminar internasional merupakan sarana untuk memperoleh jaringan akademisi dari luar negeri sehingga bisa terjadi saling tukar artikel untuk dipublikasikan pada jurnal masing-masing.
4	Keterbatasan distribusi/pemasaran jurnal.	Pengelola maupun akademisi UNY belum banyak yang berpartisipasi dalam acara-acara lingkup internasional sehingga hal ini

3) Analisis Risiko

Langkah terakhir dalam proses penilaian risiko adalah analisis risiko. Analisis risiko dilakukan dengan melalui beberapa tahapan yaitu menetapkan kemungkinan/frekuensi terjadinya risiko, menentukan dampak yang timbul dari setiap risiko, menetapkan status risiko dan peta risiko, menentukan respon terhadap risiko dan member informasi kepada pimpinan. Setiap tahapan dilakukan dengan menggunakan panduan yang telah diberikan oleh BPKP dimana hasil analisis risiko ditunjukkan pada tabel di bawah ini:

Tabel 11: Kemungkinan/Frekuensi Terjadinya Risiko

Risiko	Keterangan	Level
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional	Risiko ini berada dalam kategori jarang terjadi. UNY memiliki beberapa dosen yang cukup sering menerbitkan artikel/paper pada jurnal internasional yang diterbitkan universitas lain di luar negeri. Jika pengelola kesulitan mendapatkan artikel, pengelola bisa menghubungi dosen-dosen tersebut untuk bisa mengirimkan artikel ke jurnal internasional UNY.Selainitu,dosen-dosen UNY diperkirakan juga akan bersemangat dalam mengirimkan artikel ke jurnal ini karena penerbitan artikel dalam jurnal sendiri relatif lebih mudah dibandingkan pada jurnal milik penerbit lain.	2
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Risiko ini berada dalam kategori mungkin terjadi. Kendala yang dihadapi jurnal-jurnal yang diterbitkan UNY untuk mendapatkan akreditasi nasional adalah sulitnya memperoleh mitra bestari. Kendala yang sama besar kemungkinan juga terjadi dalam menerbitkan jurnal internasional. Akan tetapi, UNY telah memiliki kerjasama dengan beberapa universitas di luar negeri sehingga kerjasama ini bisa digunakan sebagai sarana untuk mendapatkan reviewer dari luar negeri.	3
Kesulitan dalam mencari penulis artikel dari luar negeri	Risiko ini berada dalam kategori mungkin terjadi. Beberapa dosen UNY ada yang menempuh studi lanjut di luar negeri dan mengikuti seminar internasional walaupun jumlahnya relatif sedikit jika dibandingkan dengan total	3

	dosen yang dimiliki UNY. Dosen-dosen tersebut sekiranya bisa mendapatkan artikel dari jaringan yang telah mereka bentuk selama	

	mengikuti kuliah/seminar di luar negeri.	
Keterbatasan distribusi/pemasaran jurnal.	Risiko ini berada dalam kategori jarang terjadi. Pengelola bisa secara kontinyu mengirimkan jurnal internasional kepada lembaga atau instansi pendidikan dan penelitian baik dalam maupun luar negeri sehingga pengelola bisa menyusun daftar pelanggan jurnal internasional UNY.	2

Tabel 12: Dampak Risiko

Risiko	Keterangan	Level
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional	Dampak risiko berada pada kategori sedang. Kualitas artikel yang masih belum memenuhi target jurnal internasional bukan menjadi hambatan serius dalam menerbitkan jurnal untuk penerbitan awal. Yang terpenting pada awal pertama penerbitan bukan terletak pada kualitas artikel melainkan pada kontinuitas penerbitan. Setelah kontinuitas terjaga, maka untuk lebih meningkatkan status akreditasi internasional, kualitas artikel ditingkatkan.	3
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Dampak risiko berada pada kategori besar. Reviewer luar negeri merupakan kriteria penting dalam menerbitkan jurnal berskala internasional sehingga dengan tidak terpenuhinya kriteria ini bisa mengakibatkan jurnal internasional gagal diterbitkan.	4
Kesulitan dalam mencari penulis artikel dari luar negeri	Dampak risiko berada pada kategori sedang. Penulis luar negeri memang merupakan kriteria penerbitan jurnal internasional yang memberatkan pengelola pada awal penerbitan. Akan tetapi, hal ini tidak menghambat Pengelola untuk menerbitkan jurnal internasional karena pengelola di awal	3

	penerbitan bisa meminta artikel dengan komposisi sebagian besar dari dalam negeri. Segera setelah kontinuitas penerbitan terjaga dan jurnal sudah mulai dikenal, komposisi penulis dari luar negeri diharapkan dapat meningkat secara bertahap.	
Keterbatasan distribusi/pemasaran jurnal.	Dampak risiko berada pada kategori kecil. Dampak dari risiko ini kurang begitu signifikan dan tidak menghambat penerbitan jurnal karena pengelola bisa mempelajari bagaimana strategi pemasaran jurnal sebaiknya dilakukan untuk mendapatkan pasar pembaca dan pelanggan jurnal.	2

Tabel 13: Status Risiko dan Respon Risiko

Risiko	**Frekuensi**	**Dampak**	**Status dan**	**Respon Risiko**

	Risiko	Risiko	Peta Risiko	
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Jarang Terjadi (2)	Sedang (3)	Moderat (6)	Dapat diterima hanya dengan pengendalian yang cukup.
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Mungkin Terjadi (3)	Besar (4)	Tinggi (12)	Dapat diterima dengan pengendalian yang sangat baik.
Kesulitan dalam mencari penulis artikel dari luar negeri	Mungkin Terjadi (3)	Sedang (3)	Moderat (9)	Dapat diterima dengan pengendalian yang cukup.
Keterbatasan distribusi/pemasaran jurnal.	Jarang Terjadi (2)	Kecil (2)	Rendah (4)	Dapat diterima dengan pengendalian yang cukup

Tabel 14: Informasi kepada Pimpinan

Risiko	Pihak yang Bertanggung Jawab	Informasi
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pemantauan terhadap risiko yang timbul
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Pimpinan Universitas	Pimpinan universitas perlu memberi perhatian serius terhadap risiko yang terjadi.
Kesulitan dalam mencari penulis artikel dari luar negeri	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pengendalian manajemen terhadap risiko yang terjadi.

Keterbatasan distribusi/pemasaran jurnal.	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pemantauan terhadap risiko yang timbul

Keseluruhan tabel tersebut pada akhirnya akan memberikan informasi kepada pimpinan baik itu pimpinan jurnal maupun universitas mengenai risiko yang dihadapi dalam rangka menerbitkan jurnal internasional dan apa yang harus dilakukan oleh kedua pimpinan tersebut untuk mengatasi risiko yang terjadi. Pimpinan jurnal hendaknya perlu melakukan pengelolaan, pengendalian dan pemantauan terhadap operasional penerbitan jurnal. Sedangkan, pimpinan universitas perlu melakukan merumuskan strategi yang ditujukan untuk meningkatkan kualitas penelitian dan penerbitan dengan memberikan dukungan insentif yang memadai. Selain itu, pimpinan universitas juga sekiranya bisa merumuskan pendekatan yang tepat untuk memperluas jaringan kerjasama dengan lembaga/institusi pendidikan di luar negeri.

4. Kesimpulan

Instansi pendidikan sebagaimana instansi yang lain akan dihadapkan pada risiko dimana risiko ini menghambat instansi pendidikan dalam mencapai tujuan yang telah ditetapkan. Oleh karena itu, penting kiranya bagi instansi pendidikan untuk melakukan penilaian risiko. Penilaian risiko diawali dengan proses perumusan tujuan baik itu tujuan instansi maupun tujuan kegiatan. Setelah tujuan dirumuskan, mulailah dilakukan proses pengidentifikasian terhadap risiko serta analisis risiko. Keseluruhan langkah tersebut pada akhirnya akan memberi informasi kepada pimpinan baik itu pimpinan instansi maupun pimpinan kegiatan untuk melakukan pendekatan yang tepat guna meminimalisir dampak dari risiko.

5. Daftar Pustaka

Badan Pengawasan Keuangan dan Pembangunan, 2010, *Penilaian Risiko*, Pusat Pendidikan dan Pelatihan Pengawasan, Jakarta.

Bank Indonesia, 2003, Peraturan Bank Indonesia *No 5/8/PBI/2003, tentang Penerapan Manajemen Risiko Bagi Bank*, Bank Indonesia, Jakarta

Bringham, EF., & Gapenski, LC., Daves, PR., 1999, *Intermediate Financial Management*, The Dryden Press, New York

Institut Teknologi Bandung, 2009, *Panduan Bagi Pengelola Jurnal Ilmiah*, Lembaga Penelitian dan Pengabdian Kepada Masyarakat, Bandung.

Namee, David Mc, et all, *Risk Management: Changing The Internal Auditor's Paradigm*, Institute Of Internal Auditors Research Foundation, Altamore, Sping Florida, 1998, hal.186.

NSH Health Scotland. 2010. *Risk Assessment*.

http://www.healthyworkinglives.com/advice/minimising-workplace-risks/risk-assessment.aspx#what. Diakses pada tanggal 11 februari 2012.

Pemerintah Indonesia, 2008, *Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah*, Biro Peraturan Perundang-undangan Bagian Politik dan Kesejahteraan Rakyat, Jakarta.

Analisis Resiko Pada Akademik Management System STKIP Muhammadyah Bangka Belitung

Yuniarti Denita Sari[1], Zena Lusi[2], Reni Septiyanti[3], Anggari Ayu P[4], Gina Agiyani[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di STKIP Muhammadyah Bangka Belitung. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.
Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. STKIP Muhammadyah Bangka Belitung merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan

aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan STKIP Muhammadyah Bangka Belitung. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di STKIP Muhammadyah Bangka Belitung. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan

bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah

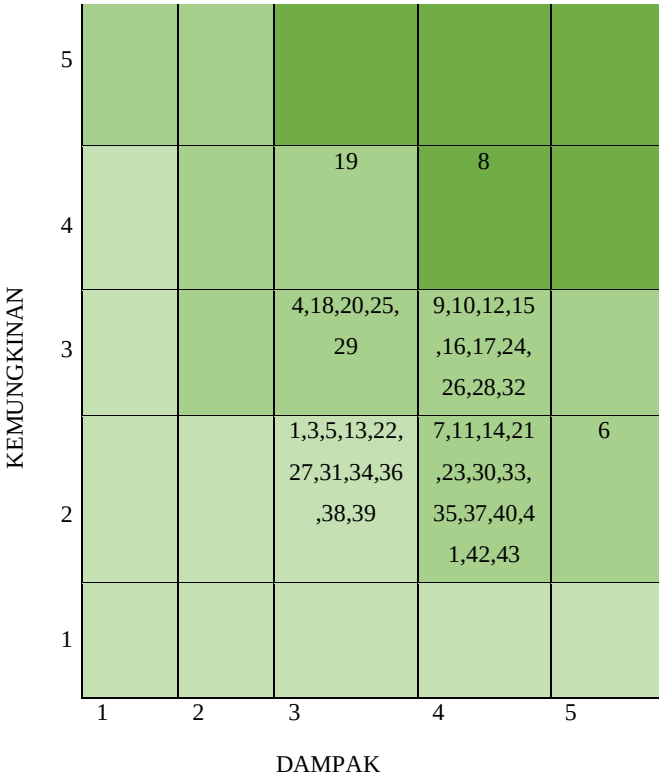
ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang

memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low /	1	Resiko Kerusakan akibat bencana alamt	NTP Server

Rendah)		seperti kebakaaran banjir, gempa	
	2	Pencurian Perangkat	NTP Server
	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya

merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dan lain-lain. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1. Apa pemicu terjadinya database server down pada sistem AMS?
2. Seberapa sering database server down tersebut terjadi pada sistem AMS?
3. Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

a) Overheat
b) Overcapacity
c) Overload
d) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
    - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin

sehingga perangkat terhindar dari resiko akibat overheat.

- Menghilangkan log yang menggunakan kapasitas yang besar
- Melakukan restart database service.
- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-

manajemen.[Accessed 16 November 2014].
[9] [Online].Available:http://dosen.guf ron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].
[10] [Online].Available:http://fisipuin.sa tugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.aca demia.edu/5170798/Uji_Validitas_ Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri0 1.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed 25 Februari 2015].
[15] [Online].Available:https://avicenna edu.wordpress.com/2013/03/26/resi komanajemen-risk-management/. [Accessed 10 Juni 2015].

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

Oleh:

Kelompok I:

1. **Muhammad Irvai (182420063)**
2. **M. Apriliansyah**
3. **Pamuji Muhammad Jakak**
4. **Anshori (182420051)**

Dosen Pengampu: M. Izman Herdiansyah, M.M., Ph.D.

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat pada saat ini mendorong Universitas Bina Insan Lubuklinggau untuk menerapkan sistem *e-learning* sebagai sistem pembelajaran berbasis elektronik yang mempermudah proses transformasi atau pertukaran informasi antara pihak Universitas Bina Insan dengan mahasiswa. Namun dalam pemanfaatan aplikasi *e-learning*itu sendiri, terkadang pihak Universitas kesulitan dalam mengidentifikasikan kemungkinan resiko-resiko yang terjadi. Adapun tujuan dari penelitian ini adalah melakukan suatu analisis resiko yang berkaitan dengan penerapan aplikasi *e-learning* di Universitas Bina Insan Lubuklinggau dengan menggunakan metode *OCTAVE Allegro.* Metode ini terdiri dari 8 tahap yang diklasifikasikan menjadi 4 kategori untuk mendapatkan tindakan pencegahan atau pengendalian pada Universitas Bina Insan. Hasil dari penelitian ini berupa pertimbangan strategi bagi Universitas Bina Insanmengenai penyimpanan aset informasi yang kritis dan pengembangan terhadap fitur aplikasi *e-learning* secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat dan pemanfaatan aplikasi *e-learning* menjadi lebih efektif.

Kata kunci: analisis resiko, manajemen resiko, *OCTAVE Allegro, e-learning.*

1. PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan sistem dan teknologi informasi saat ini, banyak organisasi yang memanfaatkan kemajuan tersebut untuk mendorong proses bisnisnya. Organisasi menyusun dan merencanakan strategi bisnis maupun teknologi informasi untuk menghasilkan kinerja yang lebih baik. Dengan adanya pemanfaatan teknologi informasi, informasi yang dihasilkan dapat digunakan lebih lanjut untuk proses pengambilan keputusan yang cepat dan tepat. Selain itu, teknologi informasi ini juga membantu organisasi dalam pengelolaan data-data secara akurat dan *real-time*. Banyak organisasi yang

menerapkan teknologi informasi yang *up-to-date* dan terbaru, termasuk perguruan tinggi. Salah satu perkembangan teknologi informasi yang sering digunakan dalam suatu perguruan tinggi adalah penerapan *e-learning* sebagai sistem pembelajaran berbasis elektronik. Pembelajaran seperti ini lebih praktis dilakukan karena *e-learning* dapat memberikan keuntungan bagi suatu perguruan tinggi dalam memperlancar pengaksesan informasi kepada mahasiswa. Hal ini juga bermanfaat untuk mempermudah proses transformasi atau pertukaran informasi antara kedua pihak.

Aktivitas-aktivitas akademik yang berkaitan dengan sistem *e-learning* dapat memberikan kemudahan pengaksesan materi perkuliahan bagi mahasiswa. Selain itu, mahasiswa dapat melakukan *download* dan *upload* tugas, melakukan *post* terhadap forum diskusi, dan mengakses kuis. *E-learning* Universitas Bina Insan dapat membantu pihak Universitas dalam memberikan informasi berupa pengumuman-pengumuman yang berkaitan dengan proses perkuliahan yang berlangsung. Selain itu, mahasiswa Universitas Bina Insan dapat mendalami penggunaan *e-learning* terkait dengan perkuliahannya. Mahasiswa dapat berfokus pada penguasaan materi perkuliahan yang diberikan oleh dosen secara langsung. Sistem pembelajaran ini dapat memfokuskan mahasiswa pada pengerjaan tugas-tugas secara mandiri dan dapat memberikan pengetahuan tambahan terkait dengan penerapan teknologi informasi yang berkaitan dengan pendidikan.

E-learning ini juga memberikan dampak positif terhadap dosen yang memberikan pengajaran dalam perkuliahan yang berlangsung sesuai dengan penetapan jadwal perkuliahan. Setiap dosen dapat mengetahui seberapa jauh pemahaman mahasiswa terhadap perkuliahan yang diberikan di Universitas Bina Insan Lubuklinggau. Dosen juga dapat menerima *feedback* dari mahasiswa secara langsung dan dosen dapat memberikan tanggapan kepada mahasiswa tanpa terhalang oleh batasan lokasi dan waktu. Selain dampak **positif** yang dihasilkan dari penerapan *e-learning* di Universitas Bina Insan, maka selalu terdapat risiko yang nantinya dapat memberikan dampak **negatif**. Adapun kemungkinan **risiko-risiko** yang dapat terjadi selama proses

perkuliahan berlangsung dalam *e-learning*, seperti terjadinya *down server* karena banyak mahasiswa yang melakukan pengaksesan *e-learning* secara bersamaan dan terdapat keterbatasan sumber daya dalam penanganan dan pemeliharaan *e-learning*. Selain itu, *e-learning* juga terdapat keterbatasan kapasitas terhadap *file* yang bisa di-*upload* dan penyimpanan data mahasiswa dalam sistem *e-learning*. Ada kemungkinan terdapat keterbatasan fitur-fitur dalam *e-learning* yang memiliki tingkat kompleksitas yang berbeda-beda. Hal ini dapat menyebabkan dosen dan mahasiswa bisa kesulitan menggunakan *e-learning*.

Dengan adanya kemungkinan **risiko-risiko** yang muncul selama proses implementasi *e-learning*, maka diperlukan manajemen risiko di Universitas Bina Insan untuk mengelola dan meminimalkan risiko tersebut. Oleh karena itu, diperlukan adanya tindakan pengendalian maupun pengawasan sistem *e-learning* yang dilakukan secara teratur. Proses-proses pengelolaan terhadap kemungkinan risiko di Universitas dapat dilakukan metodologi manajemen risiko. Untuk mengidentifikasikan kemungkinan risiko-risiko secara akurat, maka digunakan metode ***OCTAVE Allegro***. Metode ini menjabarkan identifikasi terhadap penilaian risiko dan dapat memberikan tindakan mitigasi terhadap risiko tersebut. Hal ini dapat membantu Universitas Bina Insan untuk menghadapi permasalahan-permasalahan yang terjadi pada *e-learning*.

1.2 Rumusan Masalah

Adapun rumusan permasalahan yang dilakukan dalam penelitian ini adalah

1. pihak Universitas Bina Insan kesulitan mengidentifikasikan tentang kemungkinan risiko-risiko yang dapat terjadi selama implementasi *elearning* di Universitas dengan metode *OCTAVE Allegro*
2. Evaluasi tindakan pengelolaan risiko sebagai tindakan pencegahan atau pengendalian pada Universitas Bina Insan

1.3 Tujuan Penelitian

Tujuan dilakukan proses penelitian ini adalah untuk melakukan analisis terhadap proses pengelolaan risiko sebagai bentuk manajemen risiko dalam hal implementasi *e-learning* di Universitas Bina Insan Lubuklinggau.

2. Tinjauan Pustaka

2.1 Sistem *E-Learning*

Sistem *E-learning* merupakan pendekatan inovatif dalam hal pengiriman pembelajaran untuk bidang pendidikan yang lebih tinggi dan menyediakan alternatif bagi mahasiswa untuk belajar tanpa adanya keterbatasan waktu dan tempat (Al-Samarraie et al., 2017). *E-learning* yang diterapkan dalam perguruan tinggi merupakan salah satu strategi pembelajaran yang efektif dan efisien yang memanfaatkan sistem dan teknologi informasi sehingga dapat menggantikan pembelajaran *face-to-face*. Penggunaan *e-learning* dalam perguruan tinggi yang digunakan oleh dosen sebagai *workplace tool* memiliki potensi dalam hal transformasi pengajaran dan pengalaman pembelajaran (King & Boyatt, 2014).

2.2 Manajemen Resiko

Setiap penggunaan sistem dan teknologi informasi selalu terdapat risiko yang muncul sebagai bentuk ancaman dan ketidakpastian yang dapat memberikan dampak negatif dalam suatu perusahaan atau perguruan tinggi. Tingkat probabilitas atau peluang terjadinya risiko dalam suatu organisasi berbeda-beda tergantung dari faktor-faktor pemicu munculnya risiko tersebut, seperti pengetahuan para pakar dan data-data histori dari setiap aktivitas yang telah selesai dilakukan (Aqlan & Lam, 2015). Risiko dapat terjadi pada pengelolaan aset dalam suatu organisasi karena aset bisa mengalami kerusakan ataupun kesalahan penggunaan aset tersebut oleh pihak terkait (Tobing & Puspa, 2015). Selain itu, terdapat faktor-faktor internal dalam suatu perguruan tinggi yang dapat memunculkan berbagai risiko sehingga penggunaan *e-learning* yang

memengaruhi hubungan antara dosen dengan mahasiswa. Tingkat pengetahuan dan pengalaman yang terdapat masing-masing dosen sebagai pihak pengajar dan penyampaian materi perkuliahan kepada mahasiswa bisa memunculkan kesalahpahaman penyampaian informasi kepada mahasiswa (Mackay & Tymon, 2014).

2.3 Metode OCTAVE Allegro

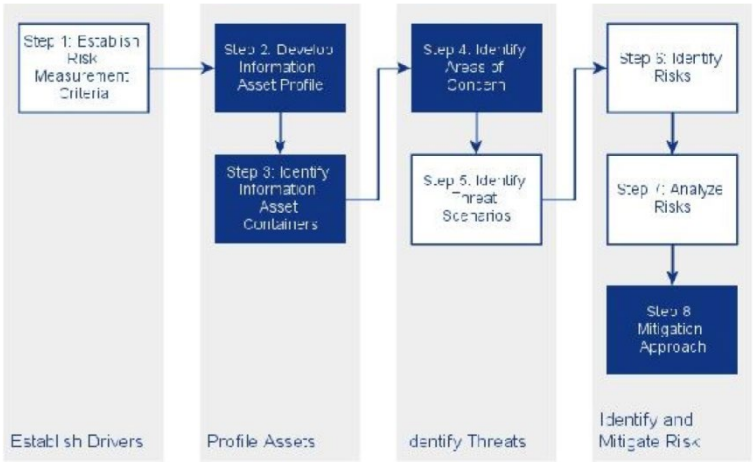
Metode OCTAVE merupakan singkatan dari *the Operationally Critical Threat, Asset, and Vulnerability Evaluation* adalah seperangkat alat, teknik, dan metode untuk menilai strategi keamanan informasi yang berbasis risiko dan perencanaan. Metode OCTAVE terdiri dari tiga prinsip dasar administrasi keamanan, yaitu: *confidentiality, integrity,* dan *availability* (Pandey & Mustafa, 2012). Metode penilaian OCTAVE Allegro yang dilakukan oleh *Carnegie Mellon University Software Engineering Institute (SEI)* yang memiliki kemampuan untuk memberikan hasil penilaian risiko yang kuat, dengan investasi yang relatif kecil dalam waktu dan sumber daya, bahkan untuk organisasi-organisasi yang tidak memiliki keahlian manajemen risiko yang luas (Keating, 2014). Metode OCTAVE Allegro dinilai sesuai untuk digunakan oleh individu yang ingin melakukan penilaian risiko secara komprehensif tanpa keterlibatan organisasi, ahli, atau sumber daya lainnya sehingga metode ini direkomendasikan untuk penilaian risiko *container* informasi (Maček, Magdalenić, & Ivković, 2011).

Metode *OCTAVE Allegro* terdiri dari delapan tahap yang diklasifikasikan menjadi empat kategori yaitu sebagai berikut (Caralli et al., 2007).

a. Menetapkan apa yang menjadi arahan organisasi dan mengembangkan kriteria pengukuran risiko didalamnya
b. Membuat profil aset yang dimiliki organisasi dengan mengidentifikasi persyaratan keamanan, dan mengidentifikasi semua lokasi dimana aset tersebut disimpan, diangkut, atau diproses

c. Mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadah aset tersebut
d. Mengidentifikasi, analisis dan mitigasi risiko terhadap aset informasi dan pengembangan terhadap pendekatan mitigasi

Berikut ini adalah gambar kategori-kategori dalam metode *OCTAVE Allegro* (Caralli et al., 2007).



Gambar 1. Pendekatan Metode *OCTAVE Allegro*

Terdapat delapan langkah-langkah yang terdapat dalam mdetode OCTAVE Allegro (Caralli et al., 2007).

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini terdapat *organizational driver* yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling prioritas. Kriteria pengukuran risiko didokumentasikan dalam bentuk *Risk Measurement Criteria Worksheets* dan pemberian nilai prioritas *impact area* dalam bentuk *Impact Area Ranking Worksheet.*

Langkah 2 – Mengembangkan Profil Aset Informasi

Langkah ini dilakukan dengan identifikasi aset informasi dimana profil tersebut merupakan representasi aset yang menggambarkan fitur, kualitas, karakteristik,

dan nilai yang unik. Langkah ini berguna untuk memastikan bahwa deskripsi aset sudah jelas dan konsisten sehingga dapat mempermudah penyusunan kebutuhan keamanan yang paling penting untuk aset informasi.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Langkah ini mengacu pada identifikasi faktor internal dan eksternal yang penting dilakukan terhadap kontainer sebagai tempat penyimpanan, pengiriman, dan pemrosesan aset informasi.

Langkah 4 – Mengidentifikasi Area Masalah yang Diperhatikan

Langkah ini dilakukan dengan proses pengembangan profil risiko dari aset informasi melalui pertukaran pikiran. Pertukaran pikiran/ *brainstorming* mengenai kondisi atau situasi tertentu untuk mengetahui komponen ancaman yang akan dihadapi. Dengan berpedoman pada dokumen *information asset risk environment maps* dan *information asset risk worksheet* maka dilakukan pencatatan *area of concern.* Setelah itu, dilakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Langkah ini dilakukan dengan identifikasi skenario ancaman tambahan yang lebih jauh dari area-area pada langkah sebelumnya berfokus pada properti ancaman. Aktivitas ini dapat menggunakan *Threat Scenario Questionnaries* dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Langkah ini digunakan untuk menentukan *threat scenario* terhadap gambaran risiko secara terperinci. *Threat scenario* didokumentasikan dalam bentuk *information asset risk worksheet* yang dapat memberikan dampak bagi organisasi.

Langkah 7 – Menganalisis Risiko

Langkah ini mengacu pada dokumentasi yang terdapat pada *information asset risk worksheet.* Setelah itu, dilakukan review dan menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis seberapa jauh dampak risiko tersebut dan memutuskan strategi terbaik dalam menghadapi risiko.

Langkah 8 – Memilih Pendekatan Pengurangan

Langkah ini dilakukan dengan mengurutkan setiap risiko yang diidentifikasi berdasarkan nilai risikonya sehingga dapat ditentukan pendekatan mitigasi terhadap risiko tersebut. Hal ini dilakukan dengan memprioritaskan risiko-risiko diikuti dengan pendekatan pengembangan strategi penanganan risiko. Strategi tersebut juga harus mempertimbangkan nilai aset dan kebutuhan keamanan, container aset, serta lingkungan operasional yang unik dalam organisasi.

3. Pembahasan

Adapun pelaksanaan penilaian risiko terhadap implementasi *e-learning* yang dilakukan di Universitas Bina Insan berdasarkan 8 fase atau langkah utama dalam metode OCTAVE Allegro adalah sebagai berikut:

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini, dibangun *organizational drivers* untuk penentuan *impact area* yang paling penting serta memberikan nilai skala prioritas pada *impact area* yang telah ditentukan. Terdapat 5 area dampak dalam OCTAVE Allegro yang menentukan nilai kualitatif dengan ukuran rendah, sedang, dan tinggi. Prioritas *impact area* yang dipilih adalah reputasi dan kepercayaan pelanggan, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan penalti.

Berikut ini adalah tabel *impact area* yang berfokus pada reputasi dan kepercayaan mahasiswa.

Tabel 1. Allegro *Worksheet* 1

Impact Area	*Low*	*Medium*	*High*
Reputasi	Reputasi Universitas Bina Insan tidak terpengaruh dari perubahan *e-learning*	Reputasi Universitas Bina Insan terpengaruh sedikit dari perubahan *e-learning*	Reputasi Universitas Bina Insan terpengaruh banyak dari perubahan *e-learning*
Kepercayaan Mahasiswa	Kurang dari 2% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*	2% -10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*	Lebih dari 10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*

Berikut ini adalah tabel *impact area* yang berfokus pada keuangan.

Tabel 2. Allegro *Worksheet* 2

Impact Area	*Low*	*Medium*	*High*
Biaya Operasional	Peningkatan biaya operasional saat implementasi *e-learning* kurang dari 2,5%	Peningkatan biaya operasional saat implementasi *e-learning* sebesar 2,5% - 5%	Peningkatan biaya operasional saat implementasi *e-learning* lebih dari 5%
Kerugian	Kurang dari 10jt kerugian tahunan jika *e-learning* ada gangguan	Antara 10jt – 50jt kerugian tahunan jika *e-learning* ada gangguan	Lebih dari 50jt kerugian tahunan jika *e-learning* ada gangguan

Dari tabel-tabel di atas, diuraikan beberapa contoh *allegro worksheet* dari semua area dampak yang berfokus di area reputasi dan kepercayaan mahasiswa dan keuangan. Dari masing-masing area dampak yang diidentifikasikan, maka ditentukan estimasi tingkat prioritas risiko apakah *low, medium*, dan *high* dan tingkat kerusakan yang mungkin terjadi saat

implementasi *e-learning* Universitas Bina Insan. Berikut ini adalah tabel skala prioritas *impact area*.

Tabel 3. Skala Prioritas *Impact Area*

Priority	*Impact Area*
1	Reputasi & Kepercayaan Mahasiswa
2	Keuangan
3	Produktivitas
4	Keamanan & Kesehatan
5	Denda & Penalti

Dari tabel-tabel identifikasi masing-masing area dampak risiko tersebut, maka didapatkan urutan prioritas area dampak, yaitu bagian reputasi dan kepercayaan mahasiswa sebagai prioritas pertama, bagian keuangan sebagai prioritas kedua, bagian produktivitas sebagai prioritas ketiga, bagian denda dan penalti sebagai prioritas keempat, dan bagian keamanan dan kesehatan sebagai prioritas kelima.

Langkah 2 – Mengembangkan Profil Aset Informasi

Profil aset informasi kritis (*Critical information assets profile*) terdiri dari deskripsi aset informasi kritis, alasan pemilihan, dan pemilik (pengelola). Profil aset informasi kritis dilengkapi dengan persyaratan (*requirements*) keamanan yang harus ada untuk melindungi aset tersebut dengan menyatakan kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan persyaratan keamanan lainnya. Berikut ini adalah tabel *critical information asset*.

Tabel 4. *Critical Information Asset Profile*

Allegro Worksheet	*Critical Information Asset*	
(1) Critical Asset	***(2) Rationale for Selection***	***(3) Description***

Peningkatan proses pembelajaran mahasiswa yang yang semakin bermutu	Penerapan *e-learning* sangat penting dilakukan untuk meningkatkan kinerja mahasiswa dan mempermudah pengaksesan materi perkuliahan, mengerjakan tugas dan kuis secara efektif dan efisien, serta dapat meningkatkan hubungan yang baik antara dosen dengan mahasiswa. Hal ini berpengaruh terhadap nilai mahasiswa.	Informasi ini terdiri dari fiturfitur *e-learning*, program studi, materi dan jadwal kuliah, jumlah kelas, deskripsi tugas dan kuis, jumlah akses fitur *elearning* oleh mahasiswa dan dosen.
(4) Owner		
Bagian Pusat Pembelajaran Elektronik		
(5) Security Requirements		
Confidentiality	Informasi selama proses perkuliahan berlangsung sangat penting untuk didistribusikan bagi mahasiswa, dosen, dan program studi. Bagian program studi menggunakan informasi ini untuk mengolah nilai mahasiswa dan melakukan evaluasi terhadap minat belajar mahasiswa melalui sistem *e-learning*.	
Integrity	Informasi selama proses perkuliahan harus benar dan *up-to-date* sesuai dengan perkembangan zaman serta mahasiswa selalu mendapatkan informasi tersebut jika terdapat perubahan antara dosen dengan mahasiswa. Bagian program studi melakukan distribusi informasi tersebut kepada dosen yang nantinya akan didistribusikan ke mahasiswa secara komprehensif.	
Availability	Informasi selama proses perkuliahan harus tersedia dengan lengkap dan jelas bagi program studi, mahasiswa, dan dosen termasuk instruksi yang diberikan, deskripsi tugas dan kuis, dan proses pengerjaan pelatihan dalam *e-learning*.	
(6) Most Important Secu rity Requirement		
Confidentiality	*Integrity*	√ ***Availability***

Dari tabel tersebut, terdapat identifikasi profil aset informasi yang kritis berupa peningkatan proses pembelajaran mahasiswa yang semakin bermutu di Universitas Bina Insan sehingga dapat diketahui risiko yang dihadapi Universitas Bina Insan.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Identifikasi *information asset container* yang terbagi menjadi tiga yaitu *technical, physical,* dan *people* masing-masing memiliki sisi eksternal dan internal dengan menggunakan *worksheet information asset risk environment map.*

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi teknikal.

Tabel 5. *Information Asset Risk Environment Map (Technical)*

Container Description	*Owner(s)*
Internal	
E-mail Server, Database Server, Internal Network	Divisi TI
Appliction Server	Divisi TI, Program Studi
Personal Computer	Dosen, Program Studi
External	
Internet, External Network.E-learning Web	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi fisik.

Tabel 6. *Information Asset Risk Environment Map (Physical)*

Container Description	*Owner(s)*
Internal	
Paper copies dari banyaknya akses *e-learning* secara rutin oleh mahasiswa	Program Studi, Bagian Pembelajaran Elektronik
External	
Paper copies dari kehadiran setiap mahasiswa	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi sumber daya manusia.

Tabel 7. *Information Asset Risk Environment Map (People)*

Container Description	*Owner(s)*
Internal	
Dosen, Staf Program Studi	Program Studi
External	
Mahasiswa	Mahasiswa

Langkah 4 – Mengidentifikasi Area Masalah

Identifikasi *areas of concerns* dilakukan untuk meninjau kembali setiap *container* untuk mempertimbangkan dan menentukan *area of concern* yang potensial

dilanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. *Areas of concern* diperluas untuk mendapatkan *threat scenarios* dan didokumentasikan untuk melihat apakah memengaruhi *security requirements.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Identifikasi *threat scenario* yang memberikan gambaran mengenai *property* dari *threat,* antara lain *actor, means, motives, outcome* dan *security requirement.* Selain itu, langkah ini dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Identifikasi risiko bertujuan untuk menentukan bagaimana *threat scenario* memberikan dampak bagi organisasi serta menentukan tingkatannya apakah masuk ke kategori *high, medium* atau *low.* Selain itu, dilakukan perhitungan *relative score* untuk membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko.

Berikut ini adalah tabel penentuan nilai prioritas berdasarkan *impact area*.

Tabel 8. *Impact – Priority Score*

Impact Area	*Priority*	*Impact Score*		
		Low (1)	*Medium (2)*	*High (3)*
Reputasi & Kepercayaan Mahasiswa	1	1	2	3
Keuangan	2	2	4	6
Produktivitas	3	3	6	9
Keamanan dan Kesehatan	5	5	10	15
Denda dan Penalti	4	4	8	12

Langkah 7 – Menganalisis Risiko

Analisis risiko dilakukan pada setiap *areas of concern* terhadap *information asset* serta identifikasi konsekuensi yang terjadi berdasarkan *relative risk score.* Nilai risiko relatif diperoleh dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area* dan estimasi kemungkinan terjadi risiko tersebut.

Berikut ini adalah tabel penilaian risiko relatif.

Tabel 9. *Relative Risk Score*

Area of Concern	*Risk*

Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *elearning* secara bersamaan setiap harinya	Konsekuensi	Diperlukan waktu pemrosesan *e-learning* untuk melakukan *back-up* terlebih dahulu dan perubahan terhadap prosedur perkuliahan		
	Severity	Area Terdampak	Nilai	Skor
		Keuangan	Medium	4
		Reputasi dan Kepercayaan Mahasiswa	High	3
		Produktivitas	High	9
		Denda dan Penalti	Low	4
		Keselamatan dan Kesehatan	Low	5
	Nilai Risiko Relatif			25

Langkah 8 – Memilih Pendekatan Pengurangan

Berdasarkan pengelompokkan risiko yang diidentifikasikan, maka dilakukan pemilihan pendekatan mitigasi. Hal ini dilakukan dengan cara memprioritaskan risiko – risiko berdasarkan nilai risiko relatif, kemudian mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset dan kebutuhan keamanan, kontainer atas aset, serta lingkungan operasional yang unik dari organisasi. Berikut ini adalah tabel matriks penentuan nilai risiko.

Tabel 10. *Relative Risk Matrix*

Risk Score		
30 to 45	16 to 29	0 to 15
POOL 1	POOL 2	POOL 3

Berikut ini adalah tabel pendekatan yang menentukan tindakan dalam penanganan risiko.

Tabel 11. *Mitigation Approach*

POOL	*Mitigation Approach*
POOL 1	*Mitigate*
POOL 2	*Mitigate or Defer*
POOL 3	*Accept*

Dari nilai risiko relatif yang didapatkan sebesar 25, maka nilai risiko tersebut dapat dikategorikan ke dalam POOL 2 yang memiliki pendekatan *mitigate* atau *defer*.

Berikut ini adalah tabel strategi pengendalian risiko terhadap risiko-risiko yang dihadapi Universitas Bina Insan

Tabel 12. *Risk Mitigation*

Risk Mitigation	
Area of Concern	Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *e-learning* secara bersamaan setiap harinya
Action	Mitigasi
Container	Kontroli
Server	Melakukan filter tehadap informasi yang dihasilkan dari setiap fitur *e-learning*
Internet	Memastikan bahwa jaringan internet telah stabil untuk akses *e-learning*
Dosen	Memastikan bahwa semua instruksi sudah diditribusikan secara menyeluruh
Program Studi	Melakukan *back-up* terhadap materi perkuliahan/ informasi terbaru dari *e-learning*
Bagian Pembelajaran Elektronik	Memastikan bahwa akses fitur *e-learning* dapat dilakukan dosen dan mahasiswa sesuai dengan prosedur perkuliahan dan melakukan *report* terkait dengan akses *e-learning* dan perubahan fitur-fitur *e-learning*

4. Kesimpulan

Analisis manajemen risiko yang dapat mengidentifikasikan *area of concern* yang berdampak pada Universitas Bina Insan. Penilaian risiko dari masing-masing *area of concern* tersebut dapat dilakukan dengan metode OCTAVE Allegro. Selain itu, Universitas Bina Insan dapat melakukan penilaian risiko berdasarkan tingkat prioritas dan besarnya dampak *e-learning* terhadap proses pembelajaran mahasiswa. Setelah mengidentifikasi adanya risiko yang akan berpengaruh terhadap keberlangsungan implementasi *e-learning*, maka Universitas Bina Insanmelakukan identifikasi pendekatan strategi atau mitigasi yang berfokus dari aspek lingkungan internal dan eksternal organisasi.

Berdasarkan hasil analisis manajemen risiko yang dilakukan, maka terdapat area perhatian mengenai perubahan fitur-fitur *e-learning* untuk akses material kuliah, tugas, dan kuis serta mengetahui hasil terhadap banyaknya akses *e-learning* yang dilakukan oleh mahasiswa dan dosen. Dari area perhatian tersebut, maka didapatkan konsekuensi berupa waktu pemrosesan *e-learning* untuk melakukan *back-up* dan memantau perubahan prosedur perkuliahan dengan mempertimbangkan kelima area dampak yang sudah

diidentifikasi nilai prioritas risikonya. Dari hasil penelitian ini, Universitas Bina Insanjuga harus mempertimbangkan strategi mana yang diutamakan untuk penyimpanan aset informasi yang kritis dan fitur-fitur *e-learning* yang perlu dikembangkan secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat. Untuk penelitian berikutnya, diharapkan dapat melakukan identifikasi risiko yang mendalam dan menyeluruh. Tidak hanya melihat sisi dari penggunaan fitur-fitur *e-learning*, tetapi juga mempertimbangkan pengembangan sistem *e-learning* dengan memperhatikan lingkungan eksternal perkuliahan dalam Universitas Bina Insan.

5. Daftar Pustaka

Al-Samarraie, H., Teng, B. K., Alzahrani, A. I., & Alalwan, N. 2017. E-learning continuance satisfaction in higher education: a unified perspective from instructors and students. *Studies in Higher Education*, 1–17.

Aqlan, F., & Lam, S. S. 2015. Supply chain risk modelling and mitigation. *International Journal of Production Research*, 1–17.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

Dewi, N. A. N., & Yudana, I. G. P. H. 2016. Analisa Manajemen Risiko Pada Sistem Akademik Di STMIK STIKOM Bali. In *Seminar Nasional Teknologi Informasi dan Multimedia*, 7–12.

Ekelhart, A., Fenz, S., & Neubauer, T. 2009. AURUM: A framework for information security risk management. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*: 1–10. https://doi.org/10.1109/HICSS.2009.82

Jakaria, D. A., Dirgahayu, R. T., & Hendrik. 2013. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. In *Seminar Nasional Aplikasi Teknologi Informasi. (SNATI)* (pp. 37–42).

Keating, C. G. 2014. *Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study. NSUWorks*. Nova Southeastern University.

King, E., & Boyatt, R. 2014. Exploring factors that influence adoption of e-learning within higher education. *British Journal of Educational Technology*, 1–9.

Matondang, N., Isnainiyah, I. N., & Muliawati, A. 2018. Analisis Manajemen Risiko Keamanan Data SistemInformasi (Studi Kasus: RSUD XYZ). *Rekayasa Sistem Dan Teknologi Informasi*, *2*(1), 282–287.

Tobing, J. J. L., & Puspa, A. K. 2015. Analisis Manajemen Resiko Untuk Evaluasi Aset Menggunakan Metode Octave Allegro. *Jurnal Manajemen Sistem Informasi Dan Teknologi*, *5*(1), 28–30.

Contoso

REVOLUSI INDUSTRI 4.0 : PELUANG DAN TANTANGAN BAGI MASYARAKAT MILENIAL

Contoso

KELOMPOK 3
RAJU SEPTA WIJAYA
ABI DAUD YUSUF
EVAN APRIADI D
RIAN AMANDA
ARVIAN SAPUTRA

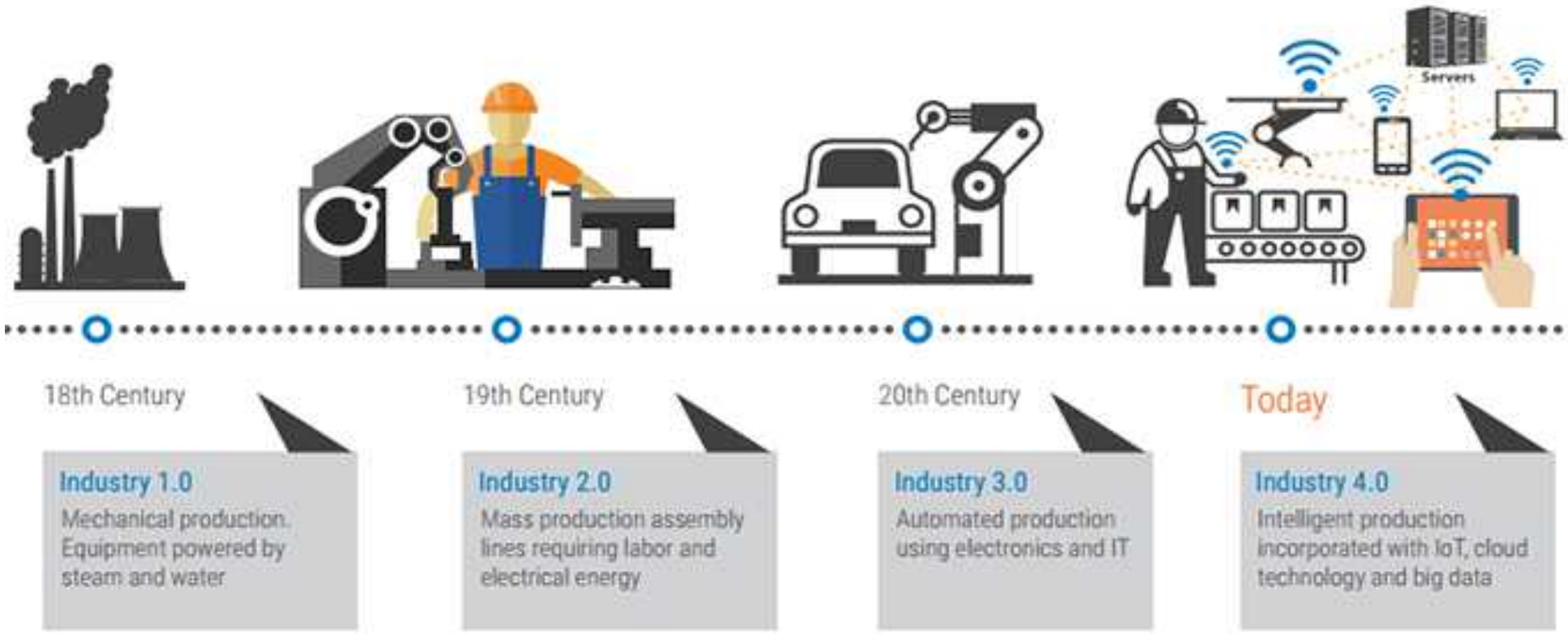
APA ITU REVOLUSI INDUSTRI 4.0?

Prof Schawab (2017) menjelaskan revolusi industri 4.0 telah mengubah hidup dan kerja manusia secara fundamental. Berbeda dengan revolusi industri sebelumnya, revolusi industri generasi ke-4 ini memiliki skala, ruang lingkup dan kompleksitas yang lebih luas. Bidang-bidang yang mengalami terobosoan berkat kemajuan teknologi baru diantaranya (1) robot kecerdasan buatan (*artificial intelligence robotic*), (2) teknologi nano, (3) bioteknologi, dan (4) teknologi komputer kuantum, (5) blockchain (seperti bitcoin), (6) teknologi berbasis internet, dan (7) printer 3D.

APA ITU REVOLUSI INDUSTRI 4.0?

Revolusi industri mengalami puncaknya saat ini dengan lahirnya teknologi digital yang berdampak masif terhadap hidup manusia di seluruh dunia. Teknologi internet yang semakin masif tidak hanya menghubungkan jutaan manusia di seluruh dunia tetapi juga telah menjadi basis bagi transaksi perdagangan dan transportasi secara online. Munculnya bisnis transportasi online seperti Gojek, Uber dan Grab menunjukkan integrasi aktivitas manusia dengan teknologi informasi dan ekonomi menjadi semakin meningkat.

Contoso



GAMBAR 1. REVOLUSI INDUSTRI 4.0 (SUMBER: WWW.KOMPASIANA.COM)

ERA DISRUPSI

Seperti yang disampaikan oleh Presiden Joko Widodo, revolusi industri 4.0 telah mendorong inovasi-inovasi teknologi yang memberikan dampak disrupsi atau perubahan fundamental terhadap kehidupan masyarakat. Kita menyaksikan pertarungan antara taksi konvensional versus taksi online atau ojek pangkalan vs ojek online. Dampaknya, publik menjadi lebih mudah untuk mendapatkan layanan transportasi dan bahkan dengan harga yang sangat terjangkau. layanan ojek online tidak sebatas sebagai alat transportasi alternatif tetapi juga merambah hingga bisnis layanan antar (*online delivery order*). Dengan kata lain, teknologi online telah membawa perubahan yang besar terhadap peradaban manusia dan ekonomi.

Contoso

PELUANG

Revolusi industri 4.0 membuka peluang yang luas bagi siapapun untuk maju. Teknologi informasi yang semakin mudah terakses hingga ke seluruh pelosok menyebabkan semua orang dapat terhubung didalam sebuah jejaring sosial. Informasi yang sangat melimpah ini menyediakan manfaat yang besar untuk pengembangan ilmu pengetahuan maupun perekonomian. *Karakteristik informasi sebagai kekayaan menunjukkan bahwa informasi yang diterima dan dikuasai seseorang dapat dimanfaatkan untuk sarana akumulasi kekayaan atau sumber komersialisasi. Dalam konteks ini, alumni atau mahasiswa dapat mempromosikan hasil kreasinya kepada publik melalui jejaring media social.*

Contoso

PELUANG

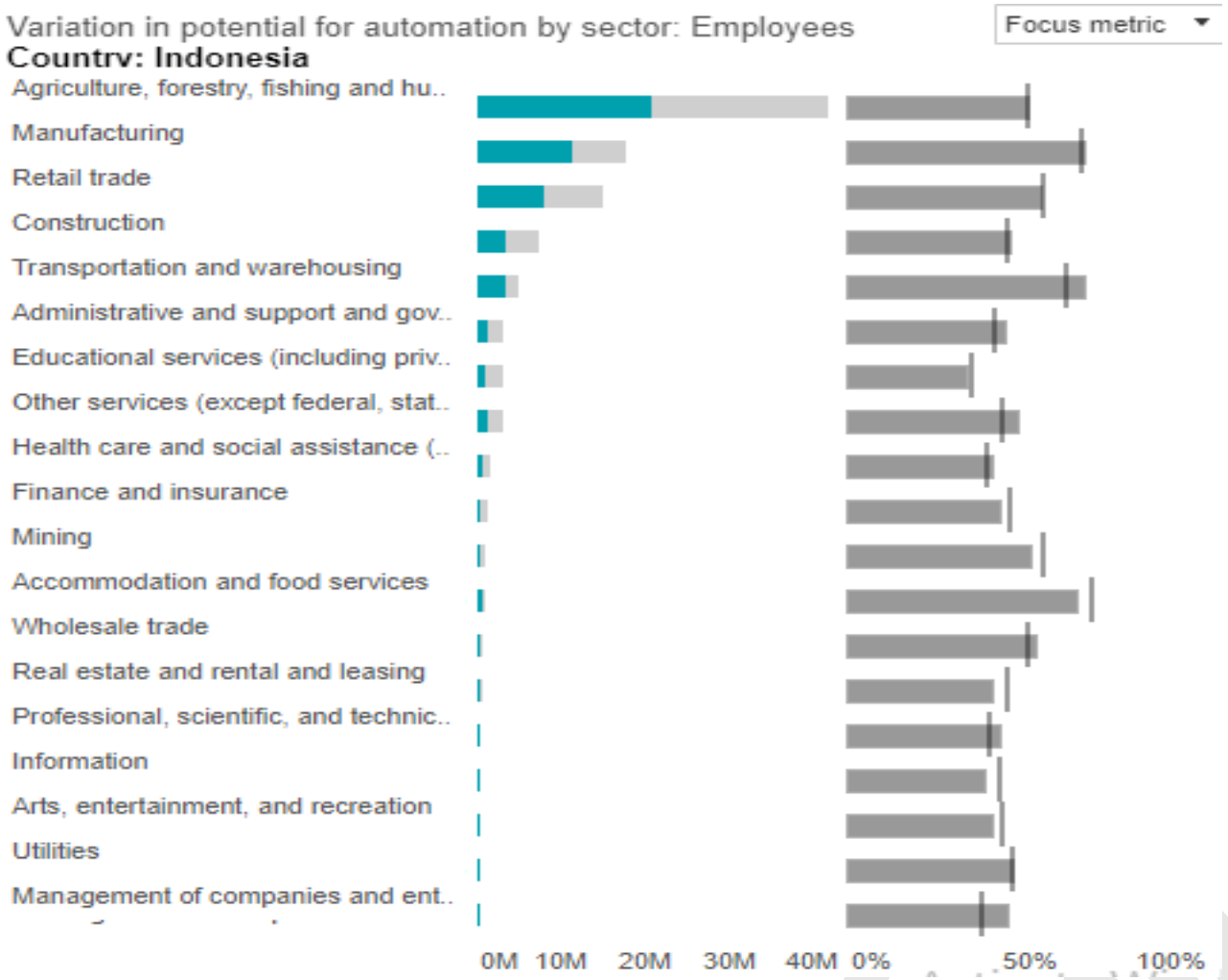
Kedua, satu dari empat orang mengakui durasi onlinenya lebih banyak daripada durasi tidurnya dalam setiap harinya. Ketiga, 1.500 responden di Inggris menghabiskan waktunya dengan bermedia sosial selama 62 juta jam per hari. Keempat, perempuan lebih sering berselancar di facebook daripada laki-laki. Kelima, tingkat kecanduan terhadap media sosial seperti twitter dan facebook lebih tinggi daripada merokok (sumber: http://www.beritasatu.com/gaya-hidup/ 232713-8-fakta-ketergantungan-pada-teknologi.html). Saat ini pasar atau toko secara fisik tidak lagi populer. Disamping ongkos pembangunan atau sewanya mahal, pasar konvensional makin sulit dijangkau.

TANTANGAN

Revolusi industri generasi empat tidak hanya menyediakan peluang, tetapi juga tantangan bagi generasi milineal. Kemajuan ilmu pengetahuan dan teknologi sebagai pemicu revolusi indutri juga diikuti dengan implikasi lain seperti pengangguran, kompetisi manusia vs mesin, dan tuntutan kompetensi yang semakin tinggi. Menurut Prof Dwikorita Karnawati (2017), revolusi industri 4.0 dalam lima tahun mendatang akan menghapus 35 persen jenis pekerjaan. Dan bahkan pada 10 tahun yang akan datang jenis pekerjaan yang akan hilang bertambah menjadi 75 persen. Hal ini disebabkan pekerjaan yang diperankan oleh manusia setahap demi setahap digantikan dengan teknologi digitalisasi program. Dampaknya, proses produksi menjadi lebih cepat dikerjakan dan lebih mudah didistribusikan secara masif dengan keterlibatan manusia yang minim,

TANTANGAN

- Gambar 2 menunjukkan bahwa lapangan pekerjaan yang potensial diotomatisasikan diantaranya usaha pengolahan (manufaturing), perdagangan ritel, transportasi dan pergudangan, tenaga administrasi, konstruksi, layanan makanan dan akomodasi, pertanian, perikanan, dan kehutanan, serta layanan kesehatan dan keuangan/asuransi. Dengan demikian, revolusi industri dapat mengancam makin tingginya pengangguran di Indonesia.



GAMBAR 2. JENIS PEKERJAAN YANG POTENSIAL DIOTOMATISASIKAN (SUMBER: HTTPS://PUBLIC.TABLEAU.COM/PROFILE/MCKINSEY.ANALYTICS#!/VIZHOME/INTERNATIONAL AUTOMATION/ WHEREMACHINESCANREPLACE HUMANS)

Contoso

TANTANGAN

Namun demikian, bidang pekerjaan yang berkaitan dengan keahlian Komputer, Matematika, Arsitektur dan Teknik akan semakin banyak dibutuhkan. Bidang-bidang keahlian ini diproyeksikan sesuai dengan tuntutan pekerjaan yang mengandalkan teknologi digital. Situasi pergeseran tenaga kerja manusia ke arah digitalisasi merupakan bentuk tantangan yang perlu direspon . terutama penguasaan teknologi komputer, keterampilan berkomunikasi, kemampuan bekerjasama secara kolaboratif, dan kemampuan untuk terus belajar dan adaptif terhadap perubahan lingkungan.

KESIMPULAN

Revolusi industri saat ini memasuki fase keempat. Perkembang ilmu pengetahuan dan teknologi yang sangat pesat memberika dampak yang besar terhadap kehidupan manusia. Banyak kemudahan dan inovasi yang diperoleh dengan adanya dukungan teknologi digital. Layanan menjadi lebih cepat dan efisien. Namun demikian, digitalisasi program juga membawa dampak negatif. Peran manusia setahap demi setahap diambil alih oleh mesin otomatis. Akibatnya, jumlah pengangguran semakin meningkat. Hal ini tentu saja akan menambah beban masalah lokal maupun nasional

Contoso

THANK YOU

IMPLEMENTASI PENILAIAN RISIKO
DALAM MENUNJANG PENCAPAIAN TUJUAN INSTANSI PENDIDIKAN

Oleh:

Kelompok 4:

1. **Ahmad Dief Aritzah**
2. **David Agustian**
3. **Ricca Verana Sari**
4. **Sahirillah**
5. **Uci Suriani**

Dosen Pengampu: M. Izman Herdiansyah, M.M., Ph.D.

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

Abstrak

Penelitian ini dilakukan dalam rangka memberikan informasi bagi kepala lembaga pendidikan untuk mengantisipasi risiko yang dihadapi oleh lembaga mereka. Lembaga pendidikan perlu melakukan penilaian risiko karena lembaga akan selalu menghadapi perubahan signifikan yang terjadi karena perubahan internal dan eksternal. Langkah penilaian risiko dimulai dari menetapkan tujuan lembaga. Penting untuk membagi tujuan lembaga menjadi lebih spesifik dengan merumuskan tujuan untuk setiap program. Langkah kedua penilaian risiko adalah identifikasi risiko. Pada langkah ini, risiko perlu diidentifikasi dan dikategorikan. Selain itu, faktor-faktor yang menyebabkan risiko juga harus dianalisis. Langkah terakhir penilaian risiko adalah menganalisis risiko. Di sini, lembaga akan mencoba menentukan status risiko dan peta risiko sehingga respons yang tepat dapat diambil untuk menangani risiko tersebut

Kata kunci : Penilaian risiko, Perumusan tujuan, Identifikasi risiko, Analisis risiko

1. Pendahuluan

Instansi pendidikan sebagaimana halnya dengan organisasi dan instansi lainnya pasti akan selalu berhadapan dengan perubahan, baik itu perubahan yang berasal dari dalam maupun dari luar instansi pendidikan. Perubahan pengelolaan pendidikan yang tidak lagi terpusat, perubahan kurikulum hingga berubahnya peraturan pemerintah kesemuanya menuntut perhatian serius dari instansi pendidikan. Perubahan dalam dunia pendidikan terjadi begitu cepat dimana semua perubahan ini diharapkan dapat meningkatkan kualitas pendidikan di Indonesia.

Kualitas pendidikan di Indonesia saat ini banyak sekali menjadi sorotan publik. Banyaknya permasalahan yang membelenggu dunia pendidikan mulai dari pengelolaan aset dan keuangan oleh instansi pendidikan hingga rendahnya mutu lulusan yang dihasilkan dari setiap jenjang sekolah kesemuanya membawa efek negatif bagi dunia pendidikan di Indonesia. Kualitas lulusan sarjana di Indonesia baik itu S1, S2 maupun S3 dipandang jauh lebih rendah kualitasnya daripada lulusan negara tetangga, seperti Malaysia. Selain itu, era globalisasi juga menuntut perhatian lebih dari instansi pendidikan karena instansi pendidikan di Indonesia harus bersaing dengan instansi pendidikan dari negara lain yang bebas membuka cabangnya di Indonesia. Kesemua perubahan ini pada akhirnya akan menjadi risiko yang harus dihadapi oleh instansi pendidikan. Jika risiko ini tidak diolah dengan baik, maka tujuan yang telah ditetapkan oleh setiap instansi pendidikan bisa jadi tidak akan bisa tercapai. Oleh karena itu, penting

kiranya bagi setiap instansi pendidikan untuk mengelola risiko sehingga keefektifan tujuan instansi pendidikan bisa diwujudkan.

Penilaian risiko merupakan salah satu unsur dalam Sistem Pengendalian Intern Pemerintah (SPIP) dimana pemerintah telah menetapkan aturan yang jelas mengenai pentingnya SPIP bagi instansi pemerintah dengan dikeluarkannya Peraturan Pemerintah No. 60 Tahun 2008. Dalam peraturan tersebut, SPIP didefinisikan sebagai proses yang integral pada tindakan dan kegiatan yang dilakukan secara terus menerus oleh pimpinan dan seluruh pegawai untuk memberikan keyakinan memadai atas tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien, keandalan pelaporan keuangan, pengamanan aset negara dan ketaatan terhadap peraturan perundang-undangan yang diselenggarakan secara menyeluruh pada lingkungan pemerintah pusat dan pemerintah daerah. Instansi pendidikan terutama yang berada dalam lingkup pemerintah hendaknya juga turut serta mematuhi peraturan tersebut dengan mengimplementasikan SPIP dalam lingkup organisasinya.

Berdasarkan definisi SPIP di atas, dapat dilihat bahwa terdapat 4 tujuan yang hendak dicapai oleh SPIP yaitu, (i) efisiensi dan keefektifan pencapaian tujuan negara, (ii) keandalan pelaporan keuangan, (iii) pengamanan aset negara dan (iv) ketaatan terhadap peraturan perundang-undangan. Tujuan tersebut diharapkan dapat dicapai dengan memperhatikan unsur-unsur pembentuk SPIP, yaitu (i) lingkungan pengendalian yang kondusif, (ii) penilaian risiko, (iii) aktivitas pengendalian, (iv) informasi dan komunikasi, dan (v) pemantauan.

Mengingat banyaknya perubahan dan tuntutan yang tinggi akan kualitas pendidikan Indonesia, instansi pendidikan-khususnya yang berada di bawah naungan pemerintah-perlu melakukan penilaian risiko. Hal ini penting untuk dilakukan dengan segera karena penilaian risiko akan membantu instansi pendidikan untuk mengelola risiko tersebut dan meminimalisir dampak yang dapat menghambat pencapaian tujuan instansi pendidikan. Dengan adanya penilaian risiko, efisiensi dan keefektifan dalam memberikan pelayanan akan meningkat sehingga instansi pendidikan dapat memberikan pelayanan yang berkesinambungan kepada *stakeholders*. Penilaian risiko juga menjadi dasar bagi instansi pendidikan dalam menyusun rencana strategis dan membantu menghindari pemborosan karena seluruh risiko yang mungkin terjadi telah diantisipasi dan dikendalikan oleh instansi pendidikan.

2. Pembahasan

A. Risiko dan Proses Penilaian Risiko

David Mc Namee & Georges Selim (1998) mendefinisikan risiko sebagai konsep yang digunakan untuk menyatakan ketidakpastian atas kejadian dan atau akibatnya yang dapat berdampak secara material bagi tujuan organisasi. Definisi yang hampir sama disampaikan oleh Bringham (1999) yang menyatakan bahwa risiko adalah bahaya, petaka; kemungkinan menderita rugi atau mengalami kerusakan. Pemerintah Indonesia melalui melalui Bank Indonesia dan Peraturan Pemerintah juga memberikan definisi risiko. Risiko adalah potensi

timbulnya suatu kerugian akibat terealisasinya suatu kejadian tertentu yang diperkirakan (Bank Indonesia, 2003). Sedangkan, pengertian risiko berdasarkan Peraturan Pemerintah No. 60 Tahun 2008 yaitu kemungkinan kejadian yang mengancam pencapaian tujuan dan sasaran instansi pemerintah.

Dari pengertian tersebut dapat ditarik kesimpulan bahwa risiko mengandung tiga unsur pembentuk risiko, yaitu (i) kemungkinan kejadian atau peristiwa, (ii) dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi, dan (iii) kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas). Ketiga unsur tersebut harus selalu dipenuhi oleh instansi pendidikan ketika akan mengidentifikasi risiko.

Risiko bisa timbul dari sumber internal dan sumber eksternal dari suatu instansi pendidikan. Risiko yang berasal dari sumber eksternal mencakup munculnya peraturan perundang-undangan baru, perkembangan teknologi, bencana alam dan gangguan keamanan. Sementara itu, sumber internal risiko terdiri atas keterbatasan dana operasional, sumber daya manusia yang tidak kompeten, peralatan yang tidak memadai, kebijakan prosedur yang tidak jelas, dan suasana kerja yang tidak kondusif. Selain kedua sumber di atas, risiko juga bisa disebabkan oleh faktor lain, misalnya pengeluaran program yang tidak tepat, pelanggaran terhadap pengendalian dana, ketidaktaatan terhadap peraturan perundang-undangan, risiko yang melekat pada sifat misinya atau pada signifikansi (BPKP, 2010). Peraturan Pemerintah No. 60 Tahun 2008 menegaskan bahwa pimpinan instansi pemerintah wajib melakukan penilaian risiko. Pihak pimpinan instansi pemerintah wajib melakukan penilaian risiko atas faktor-faktor yang mengancam tercapainya tujuan yang telah ditetapkan, baik itu tujuan instansi pendidikan secara keseluruhan maupun tujuan dari setiap kegiatan yang dilakukan oleh instansi pendidikan.

Penilaian resiko adalah metode sistematis dalam melihat aktivitas kerja, memikirkan apa yang dapat menjadi buruk, dan memutuskan kendali yang cocok untuk mencegah terjadinya kerugian, kerusakan, atau cedera di tempat kerja. Penilaian ini harus juga melibatkan pengendalian yang diperlukan untuk menghilangkan, mengurangi,atau meminimalkan resiko (NSH Health Scotland, 2010). Definisi lain tertuang dalam Peraturan Pemerintah No. 60 Tahun 2008 yang menyatakan bahwa penilaian risiko adalah proses yang dilakukan oleh suatu instansi atau organisasi dan merupakan bagian yang integral dari proses pengelolaan risiko dalam pengambilan keputusan risiko dengan melakukan tahap identifikasi rasio, analisis rasio dan evaluasi risiko. Penilaian risiko bertujuan untuk (i) mengidentifikasi dan menguraikan semua risiko-risiko potensial yang berasal baik dari faktor internal maupun faktor eksternal, (ii) memeringkat risiko-risiko yang memerlukan perhatian manajemen instansi dan yang memerlukan penanganan segera atau tidak memerlukan tindakan lebih lanjut, dan (iii) memberikan suatu masukan atau rekomendasi untuk meyakinkan bahwa terdapat risiko-risiko yang menjadi prioritas paling tinggi untuk dikelola dengan efektif (BPKP, 2010).

Penilaian risiko dilakukan terhadap faktor-faktor yang mengancam tercapainya tujuan instansi pendidikan. Oleh karena itu, penetapan tujuan baik itu tujuan instansi maupun tujuan kegiatan merupakan langkap awal dalam melakukan penilaian risiko. Setelah tujuan ditetapkan, instansi pendidikan akan melakukan identifikasi terhadap risiko-risiko yang bisa menghambat pencapaian tujuan tersebut. Identifikasi risiko bisa dilakukan baik terhadap sumber risiko internal, sumber risiko eksternal maupun sumber risiko yang lain. Terhadap setiap risiko yang berhasil diidentifikasi, instansi pendidikan kemudian menganalisis risiko tersebut untuk mengetahui pengaruhnya terhadap pencapaian tujuan. Hasil analisis risiko bisa dijadikan patokan bagi pimpinan instansi pendidikan untuk melakukan pengendalian terhadap risiko tersebut sehingga kemungkinan dan efek terjadinya risiko tersebut dapat diminimalisir.

B. Perumusan Tujuan

Langkah pertama dalam proses penilaian risiko adalah penetapan tujuan baik itu tujuan strategik dari suatu instansi maupun tujuan operasional. Dalam kaitannya dengan instansi pemerintah, Peraturan Pemerintah No. 60 Tahun 2008 mengatur bahwa tujuan strategik instansi

pemerintah harus memuat pernyataan dan arahan yang spesifik, terukur, dapat dicapai, realistis dan terikat waktu. Tujuan strategik ini harus disampaikan kepada seluruh pegawai. Untuk mencapai tujuan tersebut, pimpinan instansi pemerintah wajib menetapkan strategi operasional yang konsisten dan strategi manajemen terintegrasi serta rencana penilaian risiko. Sedangkan, tujuan pada tingkat kegiatan harus ditetapkan dengan mempertimbangkan hal-hal sebagai berikut: (i) berdasarkan pada tujuan dan rencana strategis instansi pemerintah, (ii) saling melengkapi, saling menunjang, dan tidak bertentangan satu dengan lainnya, (iii) relevan dengan seluruh kegiatan utama instansi pemerintahan, (iv) mengandung unsur kriteria pengukuran, (v) didukung sumber daya yang cukup, dan (vi) melibatkan seluruh tingkat pejabat dalam proses penetapannya.

C. Identifikasi Risiko

Identifikasi risiko adalah proses menetepkan apa, dimana, kapan, mengapa dan bagaimana sesuatu dapat terjadi sehingga dapat berdampak negatif terhadap pencapaian tujuan (PP No 60 Tahun 2008). Identifikasi risiko bisa dilakukan secara retrospektif dan prospektif (BPKP, 2010). Instansi pemerintah dapat melakukan identifikasi risiko retrospektif dengan cara mengidentifikasi risiko-risiko yang sebelumnya pernah terjadi dalam instansi tersebut. Karena risiko ini pernah terjadi, risiko tersebut lebih mudah untuk ditetapkan dan dikendalikan oleh instansi pemerintah. Identifikasi risiko secara retrospektif bisa dilakukan dengan mencari informasi dari beberapa sumber, seperti daftar risiko yang dibuat pada periode sebelumnya, dokumen dan laporan yang disimpan perusahaan, laporan audit dan hasil evaluasi lainnya, informasi dari sumber eksternal. Berkebalikan dengan risiko retrospektif, risiko prospektif lebih sulit untuk diidentifikasi karena risiko ini belum pernah dialami suatu instansi. Instansi berusaha untuk membuat prediksi tentang kemungkinan-kemungkinan buruk yang akan dihadapi oleh instansi baik apakah risiko tersebut dapat dikendalikan maupun sulit dikendalikan. Brainstorming dan analisis SWOT merupakan dua metode penting yang bisa dilakukan untuk mengidentifikasi risiko prospektif.

Salah satu tujuan dari identifikasi risiko adalah untuk menetapkan risiko (BPKP, 2010). Dalam menetapkan risiko, setiap divisi dalam instansi pemerintah harus berusaha untuk mengetahui di mana risiko bisa timbul pada divisi tersebut serta mengidentifikasi penyebab munculnya risiko dan bagaimana risiko tersebut dapat menghambat pencapaian tujuan. BPKP (2010) memberikan panduan beberapa kejadian yang bisa menghambat pencapaian tujuan, yaitu (i) tujuan menjadi lebih lama tercapainya, (ii) tujuan tercapai hanya sebagian (< 100%),

(iii) tujuan tidak tercapai sama sekali, (iv) tujuan tercapai namun dengan biaya yang lebih tinggi, dan (v) tujuan melenceng dari yang telah ditetapkan.

Tujuan kedua dari identifikasi risiko adalah mengkategorisasikan risiko (BPKP, 2010). Risiko dapat dikelompokkan atas dasar (i) jenis risiko, misalkan risiko teknologi, risiko keuangan/ekonomi, risiko sumber daya manusia, risiko kesehatan, risiko politik, risiko hukum, risiko keamanan, (ii) sumber risiko, misalkan risiko eksternal (politik, ekonomi, bencana alam) dan risiko internal (reputasi, keamanan, manajemen, informasi untuk pengambilan keputusan), (iii) penerima risiko, misalkan orang, risiko reputasi, hasil program, bangunan dan aset, lingkungan, pelayanan, (iv) dampak risiko, misalkan risiko rendah, risiko menengah, dan risiko tinggi, (v) kemampuan mengendalikan, misalnya risiko yang sangat terkendali, kurang terkendali, dan tidak/sangat sulit dikendalikan, dan (vi) hirarki risiko, misalnya risiko strategik, risiko program, risiko proyek, dan risiko operasional.

Setelah risiko ditetapkan dan dikelompokkan, identifikasi rasio ini pada akhirnya akan menghasilkan daftar risiko. Daftar risiko merupakan suatu tabel yang berisi sumber risiko dan penyebab terjadinya risiko. Daftar risiko akan menjadi dasar dalam membuat model pernyataan risiko. Ada dua pilihan model pernyataan risiko yang dikembangkan oleh BPKP

(2010), yaitu:

Gambar 1. Model Pernyataan Risiko 1

Untuk mencapai ketiga tujuan di atas, maka proses identifikasi risiko dilakukan dengan melalui tahap-tahap sebagai berikut: (i) penetapan unit risiko, yaitu penetapan organisasi atau unit mana yang akan diidentifikasi risikonya dan tingkatan risikonya, (ii) pemahaman terhadap tupoksi organisasi/unit yang bersangkutan, (iii) pemahaman terhadap aktivitas utama dari organisasi, (iv) reviu atas kriteria risiko yang ada, mencakup tingkat tolerasi risiko, kriteria dampak, kriteria kemungkinan, dan kriteria tingkat keefektifan pengendalian yang sudah ada, (v) pembuatan daftar risiko, dan (vi) pembuatan peta atau profil risiko (BPKP, 2010)

D. Analisis Risiko

Peraturan Pemerintah No. 60 Tahun 2008 mendefinisikan analisis risiko sebagai proses penilaian terhadap risiko yang telah teridentifikasi dalam rangka mengestimasi kemungkinan munculnya dan besaran dampaknya untuk menetapkan level atau status risikonya. Status risiko ditentukan berdasarkan kombinasi antara kemungkinan (probabilitas/frekuensi) terjadinya risiko dan dampak (efek) jika risiko terjadi. BPKP (2010) memberikan panduan bagaimana instansi pemerintah melakukan analisis risiko. Langkah-langkah analisis risiko tersebut adalah sebagai berikut:

1. Menetapkan kemungkinan/probabilitas/frekuensi terjadinya risiko

Tabel 1: Kerangka Pengukuran Probabilitas

Probabilitas		**Kriteria**
Rating	**%**	
1	0–10	Sangat tidak mungkin/hampir mustahil
2	10–30	Kecil kemungkinan tapi tidak mustahil
3	30–50	Kemungkinan terjadi
4	50–90	Sering terjadi
5	>90	Hampir pasti terjadi

Sumber: BPKP, 2010

Tabel 2: Ukuran Kualitatif Kemungkinan/Frekuensi

Level	**Deskriptor**	**Contoh Deskripsi Rinci**	**Frekuensi**
1	Sangat jarang	Kejadiannya muncul hanya dalam keadaan tertentu	Kurang dari sekali dalam 10 tahun
2	Jarang	Kejadiannya dapat muncul pada saat yang sama	Paling sedikit sekali dalam 10 tahun

3	Moderat	Kejadiannya seharusnya muncul pada saat yang sama	Paling sedikit sekali dalam 5 tahun
4	Sering	Kejadiannya mungkin muncul pada kebanyakan situasi	Paling sedikit sekali dalam 1 tahun
5	Hampir pasti /Sangat sering	Kejadiannya diharapkan muncul pada kebanyakan situasi	Lebih dari satu kali dalam setahun

Sumber: BPKP, 2010

2. Menentukan dampak dan besaran dari setiap risiko.
Tabel 3: Kerangka Pengukuran Dampak

Level	Rating Dampak	Keterangan
5	Sangat tinggi/ katastropik	Mengancam program dan organisasi serta *stakeholders*. Kerugian sangat besar bagi organisasi dari segi keuangan maupun politis.
4	Besar	Mengancam fungsi program yang efektif dan organisasi. Kerugian cukup besar bagi organisasi dari segi keuangan maupun politis.
3	Menengah/medium	Mengganggu administrasi program. Kerugian keuangan dan politis cukup besar.
4	Kecil	Mengancam efisiensi dan keefektifan beberapa aspek program. Kerugian kurang material dan sedikit mempengaruhi *stakeholders.*
5	Sangat rendah/tidak signifikan	Dampaknya dapat ditangani pada tahap kegiatan rutin. Kerugian kurang material dan tidak mempengaruhi *stakeholders*.

Sumber: BPKP, 2010

3. Menetapkan status risiko dan peta risiko

Formula untuk menghitung status risiko menurut BPKP (2010) adalah sebagai berikut: Status Risiko = Probabilitas x Dampak

Berikut adalah tabel untuk menentukan peta risiko. Tabel 4: Peta Risiko

Matriks Analisis Risiko	Dampak

			1	2	3	4	5
Deskripsi	**Prob.**	**Frek.**	**Tidak Signifikan**	**Kecil**	**Medium**	**Besar**	**Katas-tropik**
Hampir pasti	90%	5	Moderat	Tinggi	Ekstrim	Ekstrim	Ekstrim
Kemungkinan besar	70%	4	Rendah	Moderat	Tinggi	Ekstrim	Ekstrim
Mungkin	50%	3	Rendah	Moderat	Moderat	Tinggi	Ekstrim
Kemungkinan kecil	30%	2	Sangat rendah	Rendah	Moderat	Moderat	Tinggi
Sangat jarang	10%	1	Sangat rendah	Sangat rendah	Rendah	Rendah	Moderat

Sumber: BPKP, 2010

Tabel 5: Rating Risiko

Deskripsi	Level	Level dimulai dari status
Ekstrim	5	15
Tinggi	4	10
Moderat	3	5
Rendah	2	3
Sangat rendah	1	1

Sumber: BPKP, 2010.

4. Menentukan respon terhadap risiko
   Tabel 6: Kriteria Respon Risiko

Status Risiko	**Kriteria untuk Manajemen Risiko**		**Yang Bertanggung Jawab**
1 – 3	Dapat diterima	Dengan pengendalian yang cukup	Manajer Operasi
4 – 5	Dipantau	Dengan pengendalian yang cukup	Manajer Operasi
6 – 9	Diperlukan pengendalian manajemen	Dengan pengendalian yang cukup	Manajer Operasi
10 – 14	Harus menjadi perhatian manajemen (*urgent*)	Dapat Diterima hanya dengan Pengendalian yang sangat baik	CEO
15 – 25	Tak dapat diterima	Dapat diterima hanya dengan pengendalian yang sangat baik	Komisaris

Sumber: BPKP, 2010

5. Memberi informasi kepada pimpinan

Tabel 7: Informasi Pengelolaan Risiko

Status Risiko	Apa yang Terjadi	Apa yang Harus Dilakukan
Ekstrim	Tujuan dan hasil tidak tercapai. Mengakibatkan kerugian keuangan yang besar. Mengurangi kapabilitas instansi. Reputasi instansi sangat menurun.	Pengelolaan bersifat urgen dan aktif yang melibatkan pimpinan tingkat tinggi. Strategi risiko wajib dilaksanakan secepatnya. Pendekatan yang segera dan tepat serta pelaporan secara rutin
Tinggi	Beberapa tujuan dan hasil tidak tercapai. Mengakibatkan kerugian keuangan yang cukup besar. Mengurangi kapabilitas instansi. Cukup menurunkan reputasi	Perlu pengelolaan aktif dan reviu rutin. Strategi harus dilaksanakan terutama difokuskan pada pemeliharaan kendali yang sudah baik. Pendekatan yang tepat.
Medium	Mengganggu kualitas atau ketepatan waktu dari tujuan dan hasilnya. Mengakibatkan kerugian	Perlu pengelolaan dan reviu secara rutin. Perlu pengendalian intern yang efektif dan pemantauan.

	keuangan yang dapat diterima dengan wajar. □ Mengurangi kapabilitas instansi dalam tingkatan normal. □ Menurunkan reputasi dalam tingkat wajar.	□ Strategi risiko harus dilaksanakan.
Rendah	□ Mengganggu kualitas, kuantitas, dan ketepatan waktu dari tujuan dan hasil. □ Mengakibatkan kerugian keuangan, penurunan kapabilitas dan reputasi yang tidak besar.	□ Prosedur rutin yang cukup untuk menanggung dampak. □ Perlu pengendalian intern yang efektif dan pemantauan. □ Strategi yang fokus pada pemantauan dan reviu terhadap prosedur pengendalian yang sudah ada
Sangat Rendah	□ Dampak terhadap pencapaian tujuan adalah sangat kecil. □ Kerugian keuangan, penurunan kapabilitas, dan reputasi adalah sangat kecil.	□ Hanya perlu pemantauan singkat. □ Pengendalian normal sudah mencukupi. □ Jika sama sekali tidak diperhatikan, risiko-risiko ini dapat meningkat statusnya/prioritasnya.

Sumber: BPKP, 2010

E. Implementasi Penilaian Risiko pada Instansi Pendidikan

Penilaian risiko perlu dilakukan oleh instansi pendidikan mengingat terdapat banyak perubahan terjadi dalam dunia pendidikan dimana dampak dari perubahan perlu dikelola untuk meminimalisir kegagalan pencapaian tujuan yang telah ditetapkan. Berikut ini adalah gambaran bagaimana instansi pendidikan bisa mengimplementasikan penilaian risiko yang tahapannya dimulai dari menetapkan tujuan instansi dan tujuan tingkat kegiatan, identifikasi risiko dan analisis risiko.

1) Merumuskan Tujuan Instansi dan Tujuan Tingkat Kegiatan

Tujuan instansi pendidikan hendaknya terkait dengan visi dan misi yang telah ditetapkan karena tujuan merupakan implementasi dari visi dan misi. Visi, misi dan tujuan yang akan disajikan dalam makalah ini akan mengadopsi visi dan misi dari salah satu universitas pendidikan di Indonesia, yaitu Universitas Negeri Yogyakarta

2) Identifikasi Risiko

Identifikasi risiko dilakukan dengan melalui tiga tahap penting, yaitu menetapkan risiko, mengkategorisasikan risiko dan membuat daftar risiko.

Menetapkan Risiko

Direktorat Jenderal Pendidikan Tinggi memberikan panduan kriteria-kriteria yang harus dipenuhi dalam menerbitkan jurnal ilmiah berskala internasional. Kriteria tersebut adalah sebagai berikut:

1. Bahasa yang digunakan adalah bahasa PBB (Inggris, Perancis, Spanyol, Arab, Cina)
2. Pengelolaan naskah sedemikian rupa sehingga naskah yang diterima cepat terbit (rapid review) dan ada keteraturan terbit
3. Jurnal berkualitas (prestisius), bisa dilihat dari daftar penelaah naskahnya dan *Editorial Board*-nya yaitu pakar di bidangnya dalam dan luar negeri.
4. Dibaca oleh banyak orang di bidangnya, bisa dilihat dari distribusi/peredarannya (*circulation*).
5. Menjadi acuan bagi banyak peneliti (citation).
6. Tercantum dalam *Current Content* dan sejenisnya.
7. Artikel yang dimuat berkualitas, bisa dilihat dari kemutakhiran topik dan daftar acuannya.
8. Penyumbang artikel/naskah berasal dari banyak negara
9. Penelaah berasal dari banyak negara yang terkemuka di bidangnya.
10. Menawarkan *off-prints/reprints*.
11. Terbit teratur sesuai dengan jadwal yang ditentukan.
12. Penerbitan jurnal tidak terkendala oleh dana.
13. Bukan jurnal Jurusan, Fakultas, Universitas atau Lembaga yang mencerminkan derajat kelokalan. Seyogyanya diterbitkan oleh himpunan profesi.
14. Memberi kesempatan penulis artikel membaca contoh cetak
15. Artikel yang dominan (kalau bisa > 80%), berupa artikel orisinil (hasil penelitian), bukan sekadar review atau ulasan.
16. Kadar sumber acuan primer >80%, derajat kemutakhiran acuan >80%.
17. Tersedia Indeks di setiap volume.
18. Ketersediaan naskah tidak menjadi masalah (ITB, 2009)

Dengan melihat pada kriteria-kriteria di atas, maka beberapa kriteria tersebut bisa membawa risiko kegagalan UNY menerbitkan jurnal ilmiah berskala internasional. Tidak semua kriteria di atas menjadi risiko bagi UNY untuk mencapai tujuannya karena untuk bisa disebut sebagai risiko harus memenuhi tiga unsur pembentuk risiko, yaitu

1. Kejadian atau peristiwa
2. Kemungkinan kejadian (risiko masih berupa kemungkinan atau diukur dalam bentuk probabilitas).
3. Dampak atau konsekuensi (jika terjadi, risiko akan membawa akibat atau konsekuensi) Berikut adalah ilustrasi risiko yang bisa menghambat UNY dalam menerbitkan jurnal internasional.

Tabel 8: Ilustrasi Risiko

No.	**Uraian Risiko**	**Kejadian /Peristiwa**	**Kemungkinan Kejadian/Peristiwa**	**Dampak /Konsekuensi**
1	Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Ya	Ya Kejadian/peristiwa ini baru merupakan kemungkinan karena bisa saja pengelola di kemudian hari mendapatkan *paper* berkualitas tinggi.	Jurnal tidak bisa terbit teratur atau terlambat terbit.
2	Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Ya	Ya Ada kemungkinan pengelola akan menghadapi peristiwa tersebut karena masih terbatasnya jaringan kerja sama antara UNY dengan universitas di luar negeri.	Tidak memenuhi kriteria penerbitan jurnal internasional yang ditetapkan Dikti.

3	Kesulitan dalam mencari penulis artikel dari luar negeri.	Ya	Ya Terbatasnya ruang lingkup kerja sama dengan civitas akademika serta peneliti luar negeri	Tidak memenuhi kriteria penerbitan jurnal internasional yang ditetapkan Dikti.

			kemungkinan bisa menghambat pengelola dalam mendapatkan artikel dari penulis luar negeri	
4	Keterbatasan distribusi/pemasaran jurnal.	Ya	Ya Belum dikenalnya UNY di dunia internasional kemungkinan bisa menjadi faktor penghambat distribusi jurnal ke luar negeri.	Artikel di jurnal tidak dibaca dan tidak dikutip (disitasi) oleh peneliti lain

Dari 18 kriteria penerbitan jurnal internasional, hanya 4 faktor yang bisa ditetapkan sebagai risiko. Faktor lain bukan merupakan risiko karena tidak memenuhi salah satu unsur pembentuk risiko sebagaimana dijelaskan dalam uraian di bawah ini.

1. Bahasa yang digunakan yaitu bahasa PBB bukan merupakan risiko karena ada banyak peneliti yang memiliki potensi kemampuan berbahasa asing terutama bahasa Inggris.
2. Keteraturan dan tepat waktu dalam penerbitan merupakan akibat yang timbul karena risiko sedikitnya naskah yang diterima oleh pengelola. Dengan demikian keteraturan dan tepat waktu dalam penerbitn bukan merupakan risiko bagi pengelola melainkan dampak dari risiko keterbatasan naskah.
3. Acuan bagi banyak peneliti bukan merupakan risiko melainkan dampak dari risiko tidak dibacanya jurnal yang diterbitkan pengelola UNY karena keterbatasan distribusi jurnal.
4. Ketersediaan *current content*, *offprint/reprint* dan indeks di setiap volume penerbitan bukan merupakan risiko yang dihadapi pengelola karena pengelola memiliki kapabilitas memadai untuk memenuhi kriteria tersebut.
5. Keterbatasan dana merupakan masalah yang dihadapi oleh pengelola jurnal UNY saat ini sehingga hal ini bukan merupakan risiko. Unsur pembentuk risiko yang kedua adalah kemungkinan peristiwa/kejadian terjadi di masa mendatang dan unsur ini tidak dipenuhi sehingga keterbatasan dana tidak tepat jika diidentifikasi sebagai risiko.
6. Jurnal diterbitkan oleh himpunan profesi juga bukan merupakan risiko bagi pengelola karena UNY telah memiliki kerjasama dengan himpunan profesi.
7. Penulis artikel bisa melihat contoh cetak jurnal juga bukan merupakan risiko karena sebagian besar jurnal di UNY selama ini didistribusikan kepada penulis artikel.

Mengkategorisasikan Risiko

Pengelompokkan risiko dilakukan dengan mengidentifikasi jenis risiko, sumber risiko, penerima risiko, level risiko, pengendalian risiko dan hierarki risiko. Tabel 9 di bawah ini memuat kategorisasi risiko terhadap risiko yang berhasil diidentifikasi dari tahap penetapan risiko.

Membuat Daftar Risiko

Langkah terakhir dalam proses identifikasi risiko adalah membuat daftar risiko. Untuk keperluan penyusunan daftar risiko, faktor-faktor yang menyebabkan risiko tersebut terjadi harus ditemukan. Tabel di bawah ini memuat contoh daftar risiko dari risiko yang telah diidentifikasi dan dikelompokkan pada langkah sebelumnya:

Tabel 10: Daftar Risiko

No.	Risiko Teridentifikasi	Faktor Penyebab
1	Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Budaya penelitian masih terbatas dimana penelitian selama ini dilakukan oleh akademisi untuk memenuhi persyaratan kenaikan pangkat dan jabatan fungsional. Akibatnya, kualitas paper yang dihasilkan cenderung rendah dan belum layak untuk dipublikasikan dalam lingkup internasional.
2	Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Pengelola kurang aktif dalam mengikuti konferensi/seminar internasional sehingga jaringan kerja dengan akademisi/peneliti luar negeri menjadi terbatas. Padahal, konferensi/seminar internasional merupakan sarana untuk mendapatkan reviewer secara langsung.
3	Kesulitan dalam mencari penulis artikel dari luar negeri	Pengelola kurang aktif dalam mengikuti konferensi/seminar internasional sehingga jaringan kerja dengan akademisi/peneliti luar negeri menjadi terbatas. Padahal, konferensi/seminar internasional merupakan sarana untuk memperoleh jaringan akademisi dari luar negeri sehingga bisa terjadi saling tukar artikel untuk dipublikasikan pada jurnal masing-masing.
4	Keterbatasan distribusi/pemasaran jurnal.	Pengelola maupun akademisi UNY belum banyak yang berpartisipasi dalam acara-acara lingkup internasional sehingga hal ini

3) Analisis Risiko

Langkah terakhir dalam proses penilaian risiko adalah analisis risiko. Analisis risiko dilakukan dengan melalui beberapa tahapan yaitu menetapkan kemungkinan/frekuensi terjadinya risiko, menentukan dampak yang timbul dari setiap risiko, menetapkan status risiko dan peta risiko, menentukan respon terhadap risiko dan member informasi kepada pimpinan. Setiap tahapan dilakukan dengan menggunakan panduan yang telah diberikan oleh BPKP dimana hasil analisis risiko ditunjukkan pada tabel di bawah ini:

Tabel 11: Kemungkinan/Frekuensi Terjadinya Risiko

Risiko	Keterangan	Level
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional	Risiko ini berada dalam kategori jarang terjadi. UNY memiliki beberapa dosen yang cukup sering menerbitkan artikel/paper pada jurnal internasional yang diterbitkan universitas lain di luar negeri. Jika pengelola kesulitan mendapatkan artikel, pengelola bisa menghubungi dosen-dosen tersebut untuk bisa mengirimkan artikel ke jurnal internasional UNY.Selainitu,dosen-dosen UNY diperkirakan juga akan bersemangat dalam mengirimkan artikel ke jurnal ini karena penerbitan artikel dalam jurnal sendiri relatif lebih mudah dibandingkan pada jurnal milik penerbit lain.	2
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Risiko ini berada dalam kategori mungkin terjadi. Kendala yang dihadapi jurnal-jurnal yang diterbitkan UNY untuk mendapatkan akreditasi nasional adalah sulitnya memperoleh mitra bestari. Kendala yang sama besar kemungkinan juga terjadi dalam menerbitkan jurnal internasional. Akan tetapi, UNY telah memiliki kerjasama dengan beberapa universitas di luar negeri sehingga kerjasama ini bisa digunakan sebagai sarana untuk mendapatkan reviewer dari luar negeri.	3
Kesulitan dalam mencari penulis artikel dari luar negeri	Risiko ini berada dalam kategori mungkin terjadi. Beberapa dosen UNY ada yang menempuh studi lanjut di luar negeri dan mengikuti seminar internasional walaupun jumlahnya relatif sedikit jika dibandingkan dengan total	3

	dosen yang dimiliki UNY. Dosen-dosen tersebut sekiranya bisa mendapatkan artikel dari jaringan yang telah mereka bentuk selama	

	mengikuti kuliah/seminar di luar negeri.	
Keterbatasan distribusi/pemasaran jurnal.	Risiko ini berada dalam kategori jarang terjadi. Pengelola bisa secara kontinyu mengirimkan jurnal internasional kepada lembaga atau instansi pendidikan dan penelitian baik dalam maupun luar negeri sehingga pengelola bisa menyusun daftar pelanggan jurnal internasional UNY.	2

Tabel 12: Dampak Risiko

Risiko	Keterangan	Level
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional	Dampak risiko berada pada kategori sedang. Kualitas artikel yang masih belum memenuhi target jurnal internasional bukan menjadi hambatan serius dalam menerbitkan jurnal untuk penerbitan awal. Yang terpenting pada awal pertama penerbitan bukan terletak pada kualitas artikel melainkan pada kontinuitas penerbitan. Setelah kontinuitas terjaga, maka untuk lebih meningkatkan status akreditasi internasional, kualitas artikel ditingkatkan.	3
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Dampak risiko berada pada kategori besar. Reviewer luar negeri merupakan kriteria penting dalam menerbitkan jurnal berskala internasional sehingga dengan tidak terpenuhinya kriteria ini bisa mengakibatkan jurnal internasional gagal diterbitkan.	4
Kesulitan dalam mencari penulis artikel dari luar negeri	Dampak risiko berada pada kategori sedang. Penulis luar negeri memang merupakan kriteria penerbitan jurnal internasional yang memberatkan pengelola pada awal penerbitan. Akan tetapi, hal ini tidak menghambat Pengelola untuk menerbitkan jurnal internasional karena pengelola di awal	3

	penerbitan bisa meminta artikel dengan komposisi sebagian besar dari dalam negeri. Segera setelah kontinuitas penerbitan terjaga dan jurnal sudah mulai dikenal, komposisi penulis dari luar negeri diharapkan dapat meningkat secara bertahap.	
Keterbatasan distribusi/pemasaran jurnal.	Dampak risiko berada pada kategori kecil. Dampak dari risiko ini kurang begitu signifikan dan tidak menghambat penerbitan jurnal karena pengelola bisa mempelajari bagaimana strategi pemasaran jurnal sebaiknya dilakukan untuk mendapatkan pasar pembaca dan pelanggan jurnal.	2

Tabel 13: Status Risiko dan Respon Risiko

Risiko	**Frekuensi**	**Dampak**	**Status dan**	**Respon Risiko**

	Risiko	Risiko	Peta Risiko	
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Jarang Terjadi (2)	Sedang (3)	Moderat (6)	Dapat diterima hanya dengan pengendalian yang cukup.
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Mungkin Terjadi (3)	Besar (4)	Tinggi (12)	Dapat diterima dengan pengendalian yang sangat baik.
Kesulitan dalam mencari penulis artikel dari luar negeri	Mungkin Terjadi (3)	Sedang (3)	Moderat (9)	Dapat diterima dengan pengendalian yang cukup.
Keterbatasan distribusi/pemasaran jurnal.	Jarang Terjadi (2)	Kecil (2)	Rendah (4)	Dapat diterima dengan pengendalian yang cukup

Tabel 14: Informasi kepada Pimpinan

Risiko	Pihak yang Bertanggung Jawab	Informasi
Keterbatasan naskah yang layak untuk dipublikasikan pada jurnal berskala internasional.	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pemantauan terhadap risiko yang timbul
Kesulitan dalam mendapatkan penelaah (reviewer) luar negeri.	Pimpinan Universitas	Pimpinan universitas perlu memberi perhatian serius terhadap risiko yang terjadi.
Kesulitan dalam mencari penulis artikel dari luar negeri	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pengendalian manajemen terhadap risiko yang terjadi.

Keterbatasan distribusi/pemasaran jurnal.	Pimpinan Jurnal	Pimpinan jurnal perlu melakukan pemantauan terhadap risiko yang timbul

Keseluruhan tabel tersebut pada akhirnya akan memberikan informasi kepada pimpinan baik itu pimpinan jurnal maupun universitas mengenai risiko yang dihadapi dalam rangka menerbitkan jurnal internasional dan apa yang harus dilakukan oleh kedua pimpinan tersebut untuk mengatasi risiko yang terjadi. Pimpinan jurnal hendaknya perlu melakukan pengelolaan, pengendalian dan pemantauan terhadap operasional penerbitan jurnal. Sedangkan, pimpinan universitas perlu melakukan merumuskan strategi yang ditujukan untuk meningkatkan kualitas penelitian dan penerbitan dengan memberikan dukungan insentif yang memadai. Selain itu, pimpinan universitas juga sekiranya bisa merumuskan pendekatan yang tepat untuk memperluas jaringan kerjasama dengan lembaga/institusi pendidikan di luar negeri.

4. Kesimpulan

Instansi pendidikan sebagaimana instansi yang lain akan dihadapkan pada risiko dimana risiko ini menghambat instansi pendidikan dalam mencapai tujuan yang telah ditetapkan. Oleh karena itu, penting kiranya bagi instansi pendidikan untuk melakukan penilaian risiko. Penilaian risiko diawali dengan proses perumusan tujuan baik itu tujuan instansi maupun tujuan kegiatan. Setelah tujuan dirumuskan, mulailah dilakukan proses pengidentifikasian terhadap risiko serta analisis risiko. Keseluruhan langkah tersebut pada akhirnya akan memberi informasi kepada pimpinan baik itu pimpinan instansi maupun pimpinan kegiatan untuk melakukan pendekatan yang tepat guna meminimalisir dampak dari risiko.

5. Daftar Pustaka

Badan Pengawasan Keuangan dan Pembangunan, 2010, *Penilaian Risiko*, Pusat Pendidikan dan Pelatihan Pengawasan, Jakarta.

Bank Indonesia, 2003, Peraturan Bank Indonesia *No 5/8/PBI/2003, tentang Penerapan Manajemen Risiko Bagi Bank*, Bank Indonesia, Jakarta

Bringham, EF., & Gapenski, LC., Daves, PR., 1999, *Intermediate Financial Management*, The Dryden Press, New York

Institut Teknologi Bandung, 2009, *Panduan Bagi Pengelola Jurnal Ilmiah*, Lembaga Penelitian dan Pengabdian Kepada Masyarakat, Bandung.

Namee, David Mc, et all, *Risk Management: Changing The Internal Auditor's Paradigm*, Institute Of Internal Auditors Research Foundation, Altamore, Sping Florida, 1998, hal.186.

NSH Health Scotland. 2010. *Risk Assessment*.

http://www.healthyworkinglives.com/advice/minimising-workplace-risks/risk-assessment.aspx#what. Diakses pada tanggal 11 februari 2012.

Pemerintah Indonesia, 2008, *Peraturan Pemerintah Nomor 60 Tahun 2008 tentang Sistem Pengendalian Intern Pemerintah*, Biro Peraturan Perundang-undangan Bagian Politik dan Kesejahteraan Rakyat, Jakarta.

Analisis Resiko Pada Akademik Management System Universitas Bina Insani Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-

masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview.* Proses ini

dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden

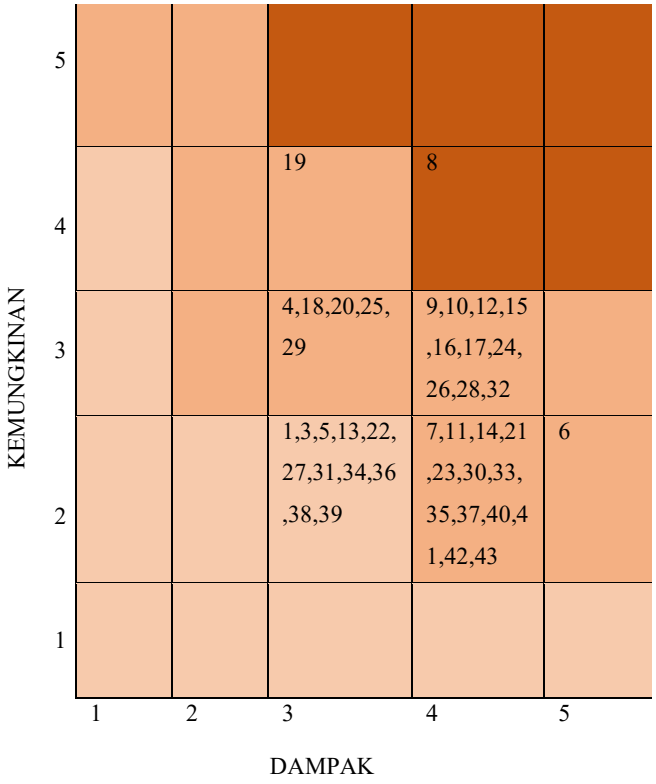
dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling

tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

1. Pendahuluan

Enterprise risk management. Secara singkat, pengertian dan definisi risiko cukup beragam. Sumber risiko pada dasarnya adalah ketidakpastian. Ketidakpastian memunculkan risiko. Proses manajemen risiko adalah tahapan yang dilakukan untuk mengelola risiko secara sistematis. *Enterprise Risk Management* (ERM) adalah manajemen risiko dalam suatu organisasi. Modul satu berikut ini membicarakan lebih lanjut ketiga konsep dasar manajemen risiko tersebut. Setelah mempelajari Modul 1 ini, secara umum Anda diharapkan dapat menjelaskan gambaran secara umum mengenai risiko dan pengelolaan risiko tersebut. Secara khusus, setelah mempelajari Modul 1 ini, Anda diharapkan bisa menjelaskan:

1. Beberapa pengertian dan definisi risiko.
2. Kondisi ketidakpastian sebagai sumber risiko.
3. Beberapa contoh kerugian yang dialami organisasi akibat kegagalan mengelola risiko.
4. Proses atau tahapan dalam pengelolaan risiko.
5. *Enterprise Risk Management* (pengelolaan risiko dalam suatu organisasi).
6. Komponen-komponen dalam *Enterprise Risk Management.*

A. RISIKO DAN KONDISI KETIDAKPASTIAN

Risiko merupakan kata yang sudah kita dengar hampir setiap hari. Biasanya kata tersebut mempunyai konotasi yang negatif, sesuatu yang tidak kita sukai, sesuatu yang ingin kita hindari. Sebagai contoh, jika kita jalan keluar dengan mobil, maka ada risiko mobil kita bertabrakan dengan mobil lainnya (kejadian yang tidak kita inginkan). Jika kita mempunyai saham, ada risiko harga saham yang kita pegang turun nilainya, sehingga kita tidak memperoleh keuntungan (kejadian yang tidak kita harapkan). Jika bank memberikan kredit kepada suatu perusahaan, maka ada kemungkinan perusahaan tersebut gagal bayar (tidak membayar bunga dan/atau cicilan pinjamannya).

Apa yang dimaksud dengan risiko? Risiko bisa didefinisikan dengan berbagai cara. Sebagai contoh, risiko bisa didefinisikan sebagai kejadian yang merugikan. Definisi lain yang sering dipakai untuk analisis investasi, adalah kemungkinan hasil yang diperoleh menyimpang dari yang diharapkan. Deviasi standar merupakan alat statistik yang bisa digunakan untuk mengukur penyimpangan, karena itu deviasi standar bisa dipakai untuk mengukur risiko. Pengukuran yang lain adalah menggunakan probabilitas. Sebagai contoh, pengemudi kendaraan orang muda lebih sering mengalami kecelakaan dibandingkan dengan orang dewasa. Probabilitas terjadinya kecelakaan untuk

orang muda lebih tinggi dibandingkan dengan untuk orang dewasa. Karena itu risiko kecelakaan untuk orang muda lebih tinggi dibandingkan untuk orang dewasa.

Kenapa muncul suatu risiko? Risiko berkaitan erat dengan kondisi ketidakpastian. Risiko muncul karena ada kondisi ketidakpastian. Praktis kita menghadapi banyak ketidakpastian di dunia ini. Sebagai contoh, hari ini bisa hujan, bisa juga tidak hujan. Investasi kita bisa mendatangkan keuntungan (harga naik), bisa juga menyebabkan kerugian (harga turun). Kepastian dalam dunia ini adalah ketidakpastian itu sendiri. Ketidakpastian tersebut menyebabkan munculnya risiko. Ketidakpastian itu sendiri ada banyak

tingkatannya. Tabel berikut ini menunjukkan tingkatan ketidakpastian dengan karakteristiknya.

Tabel 1.1.

Tingkatan Ketidakpastian

TINGKAT KETIDAKPASTIAN	KARAKTERISTIK	CONTOH
TIDAK ADA (PASTI)	HASIL BISA DIPREDIKSI DENGAN PASTI	HUKUM ALAM
KETIDAKPASTIAN OBJEKTIF	HASIL BISA DIIDENTIFIKASI DAN PROBABILITAS DIKETAHUI	PERMAINAN DADU, KARTU
KETIDAKPASTIAN SUBJEKTIF	HASIL BISA DIIDENTIFIKASI TAPI PROBABILITAS TIDAK DIKETAHUI	KEBAKARAN, KECELAKAAN MOBIL, INVESTASI
SANGAT TIDAK PASTI	HASIL TIDAK BISA DIIDENTIFIKASI DAN PROBABILITAS TIDAK DIKETAHUI	EKSPLORASI ANGKASA

Pada tingkatan pertama, kondisi kepastian sangat tinggi. Hasil bisa diprediksi dengan relatif pasti. Hukum alam merupakan contoh kepastian tersebut. Sebagai contoh, kita bisa memprediksi dengan pasti bahwa bumi mengitari matahari selama 360 hari (satu tahun). Tingkatan selanjutnya adalah ketidakpastian objektif, dengan contoh adalah dadu, jika kita melempar dadu, ada enam kemungkinan yaitu angka 1, 2, 3, 4, 5, dan 6 (ada enam kemungkinan hasil). Kita bisa menghitung probabilitas masing-masing angka untuk keluar, yaitu 1/6.

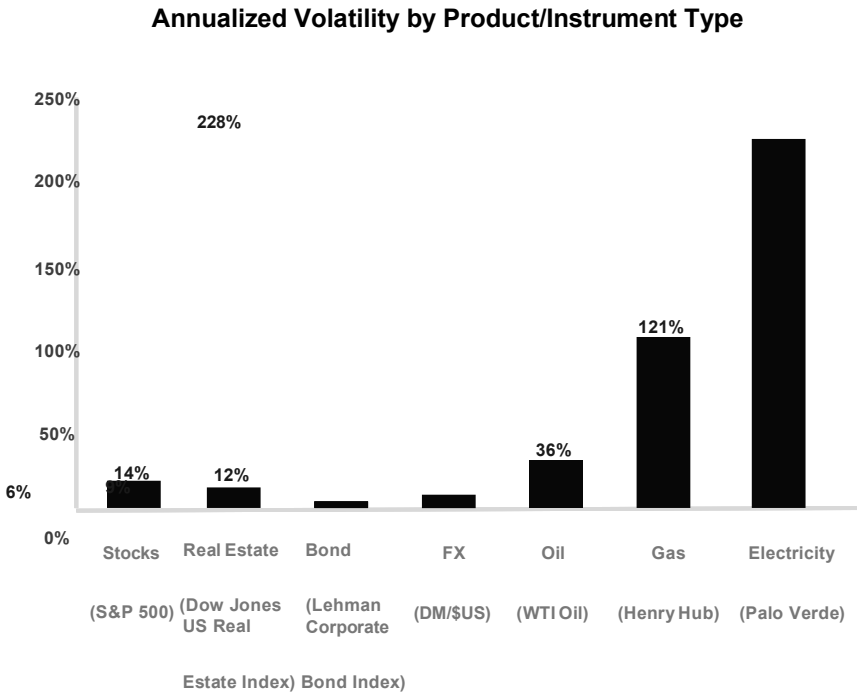
Tingkatan berikutnya adalah ketidakpastian subjektif, dengan contoh adalah kecelakaan mobil. Identifikasi hasil dan probabilitas (kemungkinan) yang berkaitan dengan kecelakaan mobil lebih sulit dilakukan. Sebagai contoh, jika kita pergi keluar dengan mobil, berapa besar probabilitas kita mengalami kecelakaan mobil? Dan jika terjadi kecelakaan, kerusakan atau kerugian yang bagaimana yang akan kita dapatkan? Tidak mudah untuk menjawab pertanyaan tersebut. Tingkatan berikutnya adalah kondisi sangat tidak pasti,

dengan contoh eksplorasi angkasa. Kita tidak tahu apa hasil yang akan diperoleh dari eksplorasi angkasa, apakah akan bertemu dengan makhluk asing (*alien*), ataukah menemukan planet yang mirip bumi, atau apa

yang akan kita temukan. Sangat sulit memprediksi atau mengidentifikasi hasil yang barangkali bisa diperoleh dari eksplorasi angkasa seperti itu. Tentu saja juga akan sangat sulit menentukan probabilitas untuk masing-masing kemungkinan hasil tersebut.

Ketidakpastian bisa tercermin dari fluktuasi pergerakan yang tinggi; Semakin tinggi fluktuasi, semakin besar tingkat ketidakpastiannya. Bagan berikut ini menunjukkan fluktuasi harga beberapa instrumen (dihitung berdasarkan deviasi standar tahunan). Terlihat bahwa semua harga instrumen berfluktuasi. Sebagai contoh, saham mempunyai fluktuasi sebesar 14%, sementara harga listrik mempunyai fluktuasi sebesar 228%.

Hasil empiris pada bagan di atas menunjukkan bahwa di dunia ini semuanya serba tidak pasti. Saham, valas (FX), harga minyak, sampai dengan harga listrik, mempunyai fluktuasi, meskipun dengan tingkat fluktuasi yang berbeda-beda. Kepastian adalah ketidakpastian itu sendiri. Dengan demikian risiko ada di mana-mana, mencakup semua instrumen.



Gambar 1.1.
Fluktuasi Tahunan Berdasarakn Tipe Instrumen

Selain itu, fluktuasi harga cenderung semakin meningkat dari tahun ke tahun. Sebagai ilustrasi, Indonesia mengalami perubahan sistem kurs dari tetap menjadi mengambang pada pertengahan tahun 1997. Sebelum krisis pada tahun 1997, Indonesia menganut sistem kurs tetap, dengan menetapkan kurs Rp/$ pada tingkat sekitar Rp2.500/$. Pada pertengahan tahun 1997, untuk mengurangi tekanan terhadap kurs karena ada krisis ekonomi, pemerintah mengambangkan kurs Rp/$. Sistem kurs mengambang tersebut masih berlaku sampai saat ini. Kurs Rp/$ tidak lagi tetap, tetapi bisa berubah tergantung mekanisme pasar. Sistem kurs mengambang tersebut mengakibatkan fluktuasi kurs Rp/$ jauh lebih tinggi dibandingkan dengan fluktuasi kurs Rp/$ pada sistem kurs tetap.

Mengapa fluktuasi cenderung meningkat? Ada beberapa faktor yang mendorong peningkatan fluktuasi tersebut, seperti:

1. Globalisasi dunia.
2. Liberalisasi dunia.
3. Proses Informasi yang semakin cepat, reaksi investor yang semakin cepat.

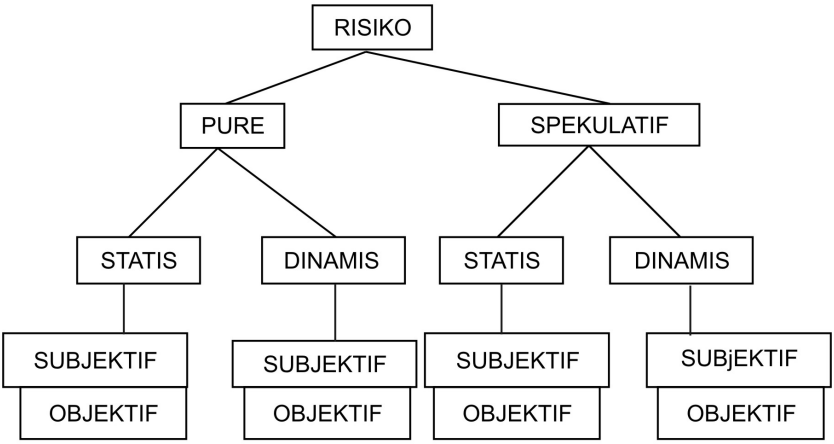
Globalisasi dunia membuat keterkaitan perekonomian dunia lebih erat. Kejadian di suatu negara akan lebih cepat mempengaruhi negara lain. Dengan kondisi seperti itu, fluktuasi akan cenderung meningkat. Liberalisasi dunia (membuka pasar domestik terhadap investor asing) mempunyai efek yang sama dengan globalisasi. Hambatan antar negara menjadi berkurang. Aliran modal menjadi lebih mudah untuk masuk atau keluar. Hal semacam ini akan meningkatkan fluktuasi dunia. Sebagai ilustrasi, krisis ekonomi di Thailand pada tahun 1997, memicu terjadinya krisis ekonomi di negara- negara sekitarnya (Indonesia, Filipina, Malaysia) dengan cepat. Investor dengan cepat memindahkan dananya dari Thailand dan negara-negara sekitarnya ke negara-negara lain yang dianggap lebih aman. Terbukanya perekonomian dunia memungkinkan pergerakan modal yang cepat semacam itu.

Teknologi yang semakin maju membuat investor atau pelaku pasar semakin canggih dalam memproses informasi. Kecanggihan tersebut akan mendorong pelaku pasar untuk lebih cepat memperoleh informasi dan bertindak lebih cepat atas informasi tersebut. Kemudahan informasi dan reaksi yang cepat dari investor akan mendorong fluktuasi harga yang semakin tinggi.

Globalisasi, liberalisasi, dan teknologi yang semakin canggih akan semakin meningkatkan fluktuasi harga, semakin meningkatkan ketidakpastian. Fluktuasi tersebut ternyata praktis dialami oleh semua atau sebagian besar instrumen keuangan atau komoditas di dunia. Dengan demikian bisa diambil kesimpulan bahwa risiko ada di mana-mana, dan risiko cenderung semakin meningkat dari tahun ke tahun.

B. TIPE-TIPE RISIKO

Risiko beragam jenisnya, mulai dari risiko kecelakaan, kebakaran, risiko kerugian, fluktuasi kurs, perubahan tingkat bunga, dan lainnya. Untuk memudahkan pemahaman dan analisis terhadap risiko, kita bisa memetakan atau mengelompokkan risiko-risiko tersebut. Salah satu cara untuk mengelompokkan risiko adalah dengan melihat tipe-tipe risiko. Bagan berikut ini menunjukkan bahwa risiko bisa dikelompokkan ke dalam dua tipe risiko: risiko murni dan risiko spekulatif, risiko subjektif dan objektif, dan dinamis dan statis.



Gambar 1.2.
Kategorisasi Risiko

Risiko bisa dikelompokkan ke dalam risiko murni dan risiko spekulatif dengan penjelasan sebagai berikut ini.

1. Risiko murni (*pure risks*) adalah risiko di mana kemungkinan kerugian ada, tetapi kemungkinan keuntungan tidak ada. Jadi kita membicarakan potensi kerugian untuk risiko tipe ini. Beberapa contoh risiko tipe ini adalah risiko kecelakaan, kebakaran, dan semacamnya. Contoh lain adalah risiko banjir menghantam rumah kita. Kejadian seperti itu akan merugikan kita. Tetapi rumah berdiri di tempat tertentu tidak secara langsung akan mendatangkan keuntungan tertentu. Jika terjadi kebakaran atau banjir, di samping individu yang terkena dampaknya, masyarakat secara keseluruhan juga akan dirugikan. Asuransi biasanya lebih banyak berurusan dengan risiko murni.
2. Risiko spekulatif adalah risiko di mana kita mengharapkan terjadinya kerugian dan juga keuntungan. Potensi kerugian dan keuntungan dibicarakan dalam jenis risiko ini. Contoh tipe risiko ini adalah usaha bisnis. Dalam kegiatan bisnis, kita mengharapkan keuntungan, meskipun ada potensi kerugian. Contoh lain adalah jika kita memegang (membeli) saham. Harga pasar bisa meningkat (kita memperoleh keuntungan), bisa juga analisis kita salah, harga saham bukannya meningkat, tetapi malah turun (kita memperoleh kerugian). Risiko spekulatif juga bisa dinamakan sebagai risiko bisnis. Kerugian akibat risiko spekulatif akan merugikan individu tertentu, tetapi akan menguntungkan individu lainnya. Misalkan suatu perusahaan mengalami kerugian karena penjualannya turun, perusahaan lain barangkali akan memperoleh keuntungan dari situasi tersebut. Secara total, masyarakat tidak dirugikan oleh risiko spekulatif tersebut.

Di samping kategorisasi murni dan spekulatif, risiko juga bisa dibedakan antara risiko yang dinamis dan yang statis.

1. Risiko statis muncul dari kondisi keseimbangan tertentu. Sebagai contoh, risiko terkena petir merupakan risiko yang muncul dari kondisi alam yang tertentu. Karakteristik risiko ini praktis tidak berubah dari waktu ke waktu.
2. Risiko dinamis muncul dari perubahan kondisi tertentu. Sebagai contoh, perubahan kondisi masyarakat, perubahan teknologi, memunculkan jenis-jenis risiko baru. Misal, jika masyarakat semakin kritis, sadar akan haknya, maka risiko hukum (*legal risk*) yang muncul karena masyarakat

lebih berani mengajukan gugatan hukum (*sue*) terhadap perusahaan, akan semakin besar.

Risiko juga bisa dikelompokkan ke dalam risiko subjektif dan objektif dengan penjelasan sebagai berikut ini.

1. Risiko objektif adalah risiko yang didasarkan pada observasi parameter yang objektif. Sebagai contoh, fluktuasi harga atau tingkat keuntungan investasi di pasar modal bisa diukur melalui standar deviasi, misal standar deviasi *return* saham adalah 25% per tahun.
2. Risiko subjektif berkaitan dengan persepsi seseorang terhadap risiko. Dengan kata lain, kondisi mental seseorang akan menentukan kesimpulan tinggi rendahnya risiko tertentu. Sebagai contoh, untuk standar deviasi *return* pasar yang sama sebesar 25%, dua orang dengan kepribadian berbeda akan mempunyai cara pandang yang berbeda. Orang yang konservatif akan menganggap risiko investasi di pasar modal terlalu tinggi. Sementara bagi orang yang agresif, risiko investasi di pasar modal dianggap tidak terlalu tinggi. Perhatikan bahwa kedua orang tersebut melihat pada risiko objektif yang sama, yaitu standar deviasi *return* sebesar 25% per tahun.

Berikut ini contoh-contoh risiko yang biasa dihadapi oleh suatu organisasi. Risiko-risiko tersebut dikelompokkan ke dalam risiko murni dan spekulatif.

Tabel 1.2.
Contoh-contoh Risiko Murni

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko Aset Fisik	Risiko yang terjadi karena kejadian tertentu berakibat buruk (kerugian) pada aset fisik organisasi.	Kebakaran yang melanda gudang atau bangunan perusahaan. Banjir mengakibatkan kerusakan pada bangunan dan peralatan
Risiko karyawan	Risiko karena karyawan organisasi mengalami peristiwa yang merugikan	Kecelakaan kerja mengakibatkan karyawan cedera, kegiatan operasional perusahaan terganggu
Risiko legal	Risiko kontrak tidak sesuai yang diharapkan, dokumentasi yang tidak benar	Terjadi perselisihan sehingga perusahaan lain menuntut ganti rugi yang signifikan

Tabel 1.3.

Contoh-Contoh Risiko Spekulatif

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko pasar	Risiko yang terjadi dari pergerakan harga atau volatilitas harga pasar	Harga pasar saham dalam portofolio perusahaan mengalami penurunan, yang mengakibatkan kerugian yang dialami perusahaan.
Risiko kredit	Risiko karena *counter party* gagal memenuhi kewajibannya kepada perusahaan	Debitur tidak bisa membayar cicilan dan bunga hutang, sehingga perusahaan mengalami kerugian. Piutang dagang tidak terbayar.
Risiko Likuiditas	Risiko tidak bisa memenuhi kebutuhan kas, risiko tidak bisa menjual dengan cepat karena ketidaklikuidan atau gangguan pasar	Perusahaan tidak mempunyai kas untuk membayar kewajibannya (misal melunasi hutang). Perusahaan terpaksa menjual tanah dengan harga murah (di bawah standar) karena sulit menjual tanah tersebut (tidak likuid), padahal perusahaan membutuhkan kas dengan cepat.
Risiko operasional	Risiko kegiatan operasional tidak berjalan lancar dan mengakibatkan kerugian: kegagalan sistem, human error, pengendalian dan prosedur yang kurang	Komputer perusahaan terkena virus sehingga operasi perusahaan terganggu. Prosedur pengendalian perusahaan tidak memadai sehingga terjadi pencurian barang-barang yang dimiliki perusahaan.

Pembagian risiko ke dalam dua tipe, yaitu risiko murni dan risiko spekulatif, barangkali tidak sepenuhnya memuaskan. Ada beberapa jenis risiko yang barangkali bisa masuk ke dalam risiko murni maupun spekulatif. Sebagai contoh, risiko tuntutan hukum bisa dimasukkan ke dalam risiko murni, tetapi jika dilihat sebagai konsekuensi kegiatan bisnis, maka risiko tersebut bisa dimasukkan ke dalam risiko spekulatif. Pembagian semacam itu bukan 'harga mati'. Pembagian semacam itu diharapkan memudahkan kita memahami jenis-jenis risiko dan karakteristiknya.

C. PROSES MANAJEMEN RISIKO

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari. Jika

risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa

mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko. Jika organisasi tersebut tidak bisa mengelola risiko dengan baik, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Karena itu risiko yang dihadapi oleh organisasi tersebut juga harus dikelola, agar organisasi bisa bertahan, atau barangkali mengoptimalkan risiko. Perusahaan sering kali secara sengaja mengambil risiko tertentu, karena melihat potensi keuntungan dibalik risiko tersebut.

Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko.
2. Evaluasi dan Pengukuran Risiko, dan
3. Pengelolaan risiko.

1. Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang dihadapi oleh suatu organisasi. Banyak risiko yang dihadapi oleh suatu organisasi, mulai dari risiko penyelewengan oleh karyawan, risiko kejatuhan meteor atau komet, dan lainnya. Ada beberapa teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh, kompor ditaruh dekat penyimpanan minyak tanah. Api merupakan sumber risiko, kompor yang ditaruh dekat minyak tanah merupakan kondisi yang meningkatkan terjadinya kecelakaan, bangunan yang bisa terbakar merupakan *eksposur* yang dihadapi perusahaan. Misalkan terjadi kebakaran, kebakaran merupakan peristiwa yang merugikan (peril). Identifikasi semacam dilakukan dengan melihat sekuen dari sumber risiko sampai ke terjadinya peristiwa yang merugikan. Pada beberapa situasi, risiko yang dihadapi oleh perusahaan cukup standar. Sebagai contoh, bank menghadapi risiko terutama adalah risiko kredit (kemungkinan debitur tidak melunasi hutangnya). Untuk bank yang juga aktif melakukan perdagangan sekuritas, maka bank tersebut akan menghadapi risiko pasar. Setiap bisnis akan menghadapi risiko yang berbeda-beda karakteristiknya.

2. Evaluasi dan Pengukuran Risiko

Langkah berikutnya adalah mengukur risiko tersebut dan mengevaluasi risiko tersebut. Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk 'mengukur' risiko tersebut.

Ada beberapa teknik untuk mengukur risiko tergantung jenis risiko tersebut. Sebagai contoh kita bisa memperkirakan probabilitas (kemungkinan) risiko atau suatu kejadian jelek terjadi. Dengan probabilitas tersebut kita berusaha 'mengukur' risiko. Sebagai contoh, ada risiko perusahaan terkena jatuhan meteor atau komet, tetapi probabilitas risiko semacam itu sangat kecil (0,000000001). Karena itu risiko tersebut tidak perlu diperhatikan. Contoh lain adalah risiko kebakaran dengan probabilitas (misal) 0,6. Karena probabilitas yang tinggi, maka risiko kebakaran perlu diberi perhatian ekstra. Contoh tersebut menunjukkan bahwa dengan menggunakan teknik probabilitas kita bisa melakukan prioritisasi risiko, sehingga kita bisa lebih memfokuskan pada risiko yang mempunyai kemungkinan yang besar untuk terjadi.

Contoh lain adalah membuat matriks dengan sumbu mendatar adalah probabilitas terjadinya risiko, dan sumbu vertikal adalah tingkat keseriusan konsekuensi risiko tersebut (*severity*, atau besarnya kerugian yang timbul akibat risiko tersebut). Setiap risiko bisa dievaluasi kemudian dimasukkan ke dalam matriks tersebut. Sebagai contoh, risiko kebakaran mempunyai probabilitas 0,6 (tinggi). Jika kebakaran terjadi, maka kerugian yang diakibatkan akan besar juga (tinggi). Dengan demikian risiko kebakaran akan ditempatkan pada kuadran probabilitas tinggi dan *severity* tinggi. Selanjutnya langkah yang lebih tepat bisa dirumuskan. Sebagai contoh, untuk risiko kebakaran seperti itu, langkah yang lebih aktif bisa ditujukan untuk menangani risiko kebakaran tersebut.

Untuk risiko lain, evaluasi dan pengukuran yang berbeda bisa dilakukan. Sebagai contoh, risiko perubahan tingkat bunga bisa diukur dengan teknik duration (durasi). Modul identifikasi dan pengukuran risiko spekulatif akan banyak membicarakan pengukuran risiko perubahan tingkat bunga. Risiko pasar bisa dievaluasi dengan menggunakan teknik VAR (*Value At Risk*). Pemahaman kita terhadap beberapa risiko sudah cukup baik sehingga teknik pengukuran risiko tersebut sudah berkembang. Sementara pemahaman kita terhadap risiko lain belum begitu baik sehingga teknik pengukuran risiko tersebut belum begitu berkembang.

Teknik lain untuk mengukur risiko adalah dengan mengevaluasi dampak risiko tersebut terhadap kinerja perusahaan.

3. Pengelolaan Risiko

Setelah analisis dan evaluasi risiko, langkah berikutnya adalah mengelola risiko. Risiko harus dikelola. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misal kerugian yang besar. Risiko bisa dikelola dengan berbagai cara, seperti penghindaran, ditahan (*retention*), diversifikasi, atau ditransfer ke pihak lainnya. Erat kaitannya dengan manajemen risiko adalah pengendalian risiko (*risk control*), dan pendanaan risiko (*risk financing*).

a. Penghindaran. Cara paling mudah dan aman untuk mengelola risiko adalah menghindar. Tetapi cara semacam ini barangkali tidak optimal. Sebagai contoh, jika kita ingin memperoleh keuntungan dari bisnis, maka mau tidak mau kita harus keluar dan menghadapi risiko tersebut. Kemudian kita akan mengelola risiko tersebut.
b. Ditahan (*Retention*). Dalam beberapa situasi, akan lebih baik jika kita menghadapi sendiri risiko tersebut (menahan risiko tersebut, atau *risk retention*). Sebagai contoh, misalkan seseorang akan keluar rumah membeli sesuatu dari supermarket terdekat, dengan menggunakan kendaraan. Kendaraan tersebut tidak diasuransikan. Orang tersebut merasa asuransi terlalu repot, mahal, sementara dia akan mengendarai kendaraan tersebut dengan hati-hati. Dalam contoh tersebut, orang tersebut memutuskan untuk menanggung sendiri (menahan, *retention*) risiko kecelakaan.
c. Diversifikasi. Diversifikasi berarti menyebar eksposur yang kita miliki sehingga tidak terkonsentrasi pada satu atau dua eksposur saja. Sebagai contoh, kita barangkali akan memegang aset tidak hanya satu, tetapi pada beberapa aset, misal saham A, saham B, obligasi C, properti, dan sebagainya. Jika terjadi kerugian pada satu aset, kerugian tersebut diharapkan bisa dikompensasi oleh keuntungan dari aset lainnya.
d. Transfer Risiko. Jika kita tidak ingin menanggung risiko tertentu, kita bisa mentransfer risiko tersebut ke pihak lain yang lebih mampu menghadapi risiko tersebut. Sebagai contoh, kita bisa membeli asuransi kecelakaan. Jika terjadi kecelakaan, perusahaan asuransi akan menanggung kerugian dari kecelakaan tersebut.

e. Pengendalian Risiko. Pengendalian risiko dilakukan untuk mencegah atau menurunkan probabilitas terjadinya risiko atau kejadian yang tidak kita inginkan. Sebagai contoh, untuk mencegah terjadinya kebakaran, kita memasang alarm asap di bangunan kita. Alarm tersebut merupakan salah satu cara kita mengendalikan risiko kebakaran.
f. Pendanaan Risiko. Pendanaan risiko mempunyai arti bagaimana 'mendanai' kerugian yang terjadi jika suatu risiko muncul. Sebagai contoh, jika terjadi kebakaran, bagaimana menanggung kerugian akibat kebakaran tersebut, apakah dari asuransi, ataukah menggunakan dana cadangan? Isu semacam itu masuk dalam wilayah pendanaan risiko.

Di samping proses manajemen risiko seperti yang disebutkan di muka, manajemen risiko suatu organisasi juga memerlukan infrastruktur baik keras maupun lunak. Sebagai contoh, manajemen risiko barangkali akan memerlukan sistem komputer untuk analisis risiko. Manajemen risiko juga memerlukan staf dan struktur organisasi yang tepat. Infrastruktur manajemen risiko tidak dibahas secara khusus dalam modul ini. Modul enam menyajikan ilustrasi bagaimana perusahaan terkemuka dunia mengembangkan manajemen risiko dalam organisasinya.

Enterprise Risk Management

Makhluk hidup secara natural akan mengantisipasi dan 'mengelola' risiko. Sebagai contoh, jika kita keluar mengendarai mobil, maka kita akan waspada dengan kondisi sekitarnya. Jika dari arah yang berlawanan ada mobil yang agak ke tengah jalannya, kita akan menghindari mobil tersebut dengan jalan mengendarainya agak ke kiri, supaya tidak terjadi tabrakan. Konon binatang mempunyai indera keenam yang bisa mendeteksi risiko lebih baik dibandingkan manusia. Pada waktu tsunami melanda wilayah Asia pada tahun 2004, binatang (gajah, dan sebagainya) yang menjadi korban tsunami jauh lebih kecil dibandingkan manusia. Binatang tersebut sepertinya mampu mendeteksi datangnya bahaya, kemudian menyingkir sebelum bahaya tersebut datang. Konon manusia dulu juga mempunyai kemampuan yang serupa, tetapi karena tidak banyak digunakan, karena manusia lebih banyak mengandalkan otak mereka, kemampuan indera keenam tersebut menghilang. Bagaimana dengan organisasi? Organisasi tidak mempunyai kemampuan mengelola risiko seperti halnya manusia atau makhluk hidup mengelola risiko, karena organisasi bukan makhluk hidup. Tugas dari manajer suatu organisasi adalah membuat agar organisasi bisa mengantisipasi dan mengelola risiko

sebagaimana halnya makhluk hidup mengelola risiko yang dihadapinya. Dengan kata lain, tugas manajer adalah membuat organisasi menjadi sadar risiko, sehingga risiko bisa diantisipasi dan dikelola dengan baik.

Tabel 1.4 berikut ini menyajikan konsekuensi merugikan jika suatu organisasi gagal mengelola risiko

Tabel 1.4.
Beberapa Contoh Kegagalan Mengelola Risiko

Tahun	Penjelasan
1997	Trader Bank Baring (Nick Leeson) membeli *instrument derivative* saham Jepang (futures Nikkei). Bank Baring adalah Bank dari Inggris. Ekonomi Jepang turun drastic karena ada bencana gempa Kobe. Akibatnya dia mengalami kerugian besar. Transaksi selanjutnya (jual opsi) tidak mengurangi kerugian, tetapi memperparah kerugian. Pada akhirnya Bank Baring mengalami kerugian sebesar $1,3 miliar. Bank Baring terpaksa bangkrut karena kerugiannya sudah melebihi modalnya.

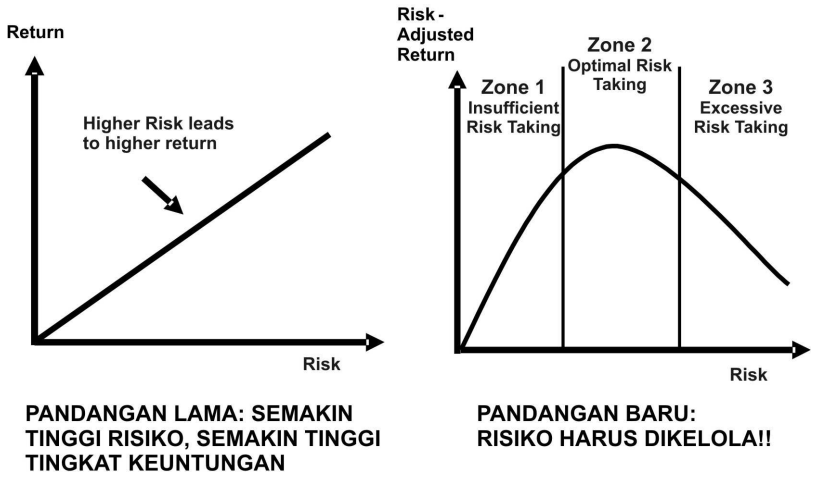
Tahun	Penjelasan
1997	Long Term Capital (LTC), perusahaan investasi di Amerika Serikat, mempunyai posisi pada mata uang Rusia Rubel yang cukup besar. Mereka memperkirakan Rusia tidak akan bangkrut. Tetapi Rusia ternyata bangkrut, mendeklarasikan tidak mampu dan tidak akan membayar hutang-hutangnya. Akibatnya *Long Term Capital* mengalami kerugian yang sangat besar, sekitar $3,5 miliar, dan pada akhirnya LTC terpaksa bangkrut.
2001	Enron merupakan perusahaan yang memperdagangkan energi (jual beli energi). Mereka juga masuk ke kontrak *derivative* energi. Usaha mereka cukup kompleks sehingga transparansi menjadi lebih sulit. Transparansi yang kompleks dimanfaatkan untuk menjalankan sistem akuntansi yang tidak wajar. Di samping itu Enron melakukan beberapa *manuever* agar laporan keuangannya kelihatan baik. Akhirnya investor mengetahui trik-trik mereka. Keuntungan mereka yang sesungguhnya ternyata tidak sebesar yang dilaporkan. Harga saham Enron jatuh dari $80 per lembar menjadi hanya $0,5. Mereka mempunyai kewajiban jangka pendek yang segera jatuh tempo. Mereka tidak bisa memperoleh bantuan dana. Tidak ada yang percaya dengan mereka. Enron akhirnya bangkrut.
1980-an	*Saving Loan* (S & L) *Association* (bank yang memberi pinjaman kredit rumah di Amerika Serikat) mempunyai struktur neraca: memberi kredit rumah dengan bunga tetap jangka panjang (misal 20 tahun), sementara memperoleh dana melalui deposito jangka pendek (misal 1 tahun). Struktur semacam itu rentan terhadap risiko perubahan tingkat bunga. Pada waktu tingkat bunga di Amerika Serikat naik signifikan pada tahun 1980-an, banyak S & L yang mengalami masalah dan puluhan S & L bangkrut karenanya.
1995	Bank Duta (Indonesia) mengalami kerugian yang sangat besar karena mereka melakukan perdagangan valas dan mengalami kerugian besar dari perdagangan valas tersebut.

Pertanyaan yang muncul adalah bisakah organisasi-organisasi di atas menghindari kerugian besar karena munculnya risiko-risiko tersebut? Manajemen risiko organisasi bertujuan menciptakan sistem atau mekanisme dalam organisasi sehingga risiko yang bisa merugikan organisasi bisa diantisipasi dan dikelola untuk tujuan meningkatkan nilai perusahaan.

Pentingnya pengelolaan risiko juga bisa dilihat melalui Bagan 1.1 berikut ini. Bagan 1.1 tersebut menggambarkan pandangan lama (sebelah kiri) dan baru (sebelah kanan) dalam kaitannya antara risiko dengan tingkat keuntungan. Pandangan lama menganggap ada hubungan positif antara risiko dengan tingkat keuntungan. Semakin tinggi risiko, akan semakin tinggi tingkat keuntungan yang diharapkan. Jika suatu organisasi ingin meningkatkan tingkat

keuntungannya, maka organisasi tersebut harus menaikkan risikonya.

Pandangan baru mengatakan bahwa hubungan antara risiko dengan tingkat keuntungan tidak bersifat linear, tetapi non-linear. Pada wilayah satu, risiko yang diambil oleh perusahaan terlalu kecil, sehingga keuntungan yang diperoleh juga kecil. Pada tahap ini, risiko masih bisa ditingkatkan untuk meningkatkan tingkat keuntungan. Contoh ekstrem situasi ini adalah jika manajer hanya tinggal di rumah, tidak pergi ke mana-mana. Dia bisa menghindari banyak risiko (risiko kecelakaan, dan sebagainya), tetapi dia juga tidak mendapatkan banyak keuntungan. Di tahap ini, pengelolaan risiko belum optimal.



Gambar 1.3.
Hubungan Risiko dan Tingkat Keuntungan (*Return*): Pandangan Lama dan Baru

Pada tahap berikutnya (zona 2), penambahan risiko tidak banyak meningkatkan tingkat keuntungan. Tahap ini merupakan tahap optimal. Tahap berikutnya (zona 3), risiko yang diambil organisasi terlalu tinggi, sehingga penambahan risiko akan berakibat negatif terhadap organisasi. Sebagai contoh, bank memberi pinjaman pada sektor-sektor yang risikonya terlalu tinggi, misal usaha burung walet, usaha perjudian. Risiko yang terlalu tinggi menjadi sulit untuk dikendalikan, sehingga bisa berakibat membahayakan dan merugikan perusahaan. Berdasarkan kerangka tersebut, pengelolaan risiko organisasi seharusnya berada pada wilayah tengah (zona 2), yang merupakan zona optimal.

Pengelolaan risiko yang digambarkan dalam bagan di atas bisa diilustrasikan melalui perjalanan dengan menggunakan kendaraan (mobil). Mobil yang berjalan terlalu lambat barangkali tidak menguntungkan, karena beberapa hal, misal terlalu lama, atau bahkan bisa membahayakan kendaraan lainnya. Mobil tersebut perlu dipacu lebih cepat. Jika mobil berjalan terlalu cepat (misal, ngebut), maka risiko bertabrakan atau kehilangan kendali menjadi semakin besar. Tentu saja hal ini tidak menguntungkan. Yang paling optimal adalah mobil berjalan dengan kecepatan optimal, yaitu cukup cepat tetapi bisa dikendalikan. Pengelolaan risiko bisa diilustrasikan sebagai kombinasi penekanan gas (mempercepat kendaraan) dan penekanan rem (memperlambat kendaraan). Kombinasi yang ideal bisa membuat mobil berjalan kencang tetapi tetap terkendali.

B. DEFINISI DAN PENGERTIAN MANAJEMEN RISIKO

Manajemen risiko organisasi adalah suatu sistem pengelolaan risiko yang dihadapi oleh organisasi secara komprehensif untuk tujuan meningkatkan nilai perusahaan. Meskipun pengertian manajemen risiko organisasi adalah seperti yang disebutkan di atas, tetapi ada banyak definisi dan pengertian manajemen risiko organisasi. Berikut ini beberapa definisi manajemen risiko organisasi.

Manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi, untuk mengelola, memonitor, dan mengendalikan eksposur organisasi terhadap risiko (SBC Warburg, *The Practice of Risk Management*, Euromoney Book, 2004)

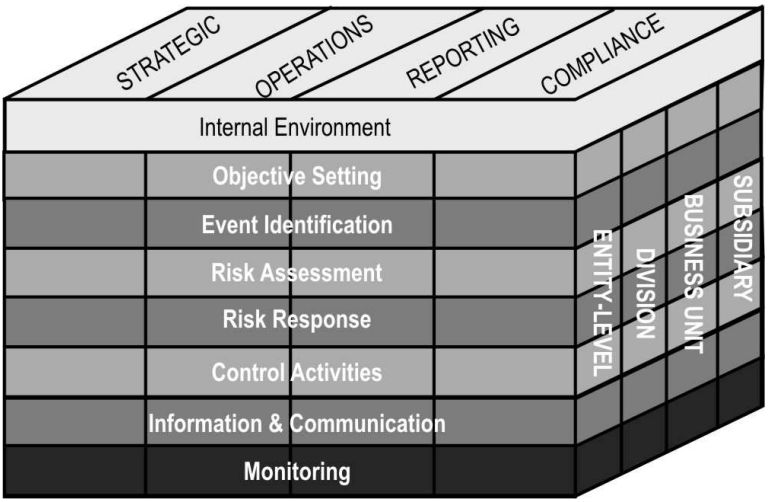
Enterprise Risk Management adalah kerangka yang komprehensif, terintegrasi, untuk mengelola risiko kredit, risiko pasar, modal ekonomis, transfer risiko, untuk memaksimumkan nilai perusahaan (Lam, James, *Enterprise Risk Management*, Wiley, 2004)

Manajemen risiko organisasi mempunyai elemen-elemen berikut ini:
Identifikasi Misi: Menetapkan Tujuan manajemen risiko.
Penilaian Risiko dan Ketidakpastian: Mengidentifikasi dan mengukur risiko.
Pengendalian Risiko: Mengendalikan risiko melalui diversifikasi, asuransi, hedging, penghindaran, dan lain-lain.

Pendanaan Risiko: Bagaimana membiayai manajemen risiko.
Administrasi program: Administrasi organisasi, seperti manual, dan sebagainya.
(Williams, Smith, Young, *Risk Management and Insurance*, McGraw Hill, 1998)

Enterprise Risk Management (ERM) adalah suatu proses, yang dipengaruhi oleh manajemen, board of directors, dan personel lain dari suatu organisasi, diterapkan dalam setting strategi, dan mencakup organisasi secara keseluruhan, didisain untuk mengidentifikasi kejadian potensial yang mempengaruhi suatu organisasi, mengelola risiko dalam toleransi suatu organisasi, untuk memberikan jaminan yang cukup pantas berkaitan dengan pencapaian tujuan organisasi. (COSO, *COSO Enterprise Risk Management – Integrated Framework.* COSO, 2004) .

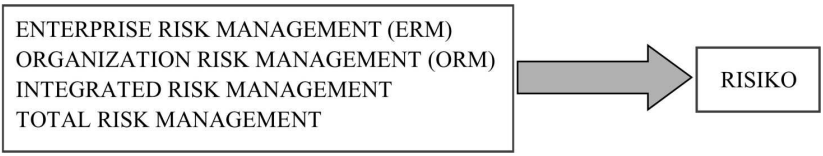
Selanjutnya COSO menampilkan format berikut ini yang menunjukkan bahwa ERM adalah manajemen risiko yang komprehensif (Lihat bagan berikut ini).



Gambar 1.4.
COSO – *Enterprise Risk Management*

Gambar 1.4 tersebut menunjukkan delapan komponen ERM yaitu (1) lingkungan internal, (2) penentuan tujuan, (3) Identifikasi kejadian, (4) Evaluasi (*assessment*) risiko, (5) Respons terhadap risiko, (6) Aktivitas pengendalian, (7) Informasi dan komunikasi, (8) Monitoring. Risiko yang dikelola mencakup risiko strategis, operasi, pelaporan, dan kepatuhan (*compliance*). Kemudian ERM mencakup keseluruhan organisasi, mulai dari level perusahaan keseluruhan (*entity level*), level divisi, level unit bisnis, dan level anak perusahaan (*subsidiary*).

Perhatikan bahwa definisi-definisi tersebut menggunakan istilah yang beragam untuk menjelaskan manajemen risiko organisasi, seperti terlihat pada bagan berikut ini.



Gambar 1.5.
Beberapa Istilah Manajemen Risiko Organisasi

Kemudian, ciri lain dari definisi tersebut adalah pengelolaan risiko yang komprehensif, dan bertujuan mencapai tujuan organisasi. Dengan menggabungkan beberapa karakteristik tersebut, bagan berikut ini menyajikan pengertian manajemen risiko suatu organisasi yang menjadi acuan modul ini.

Gambar 1.6.
Kerangka Manajemen Risiko Organisasi

Gambar 1.6 tersebut menunjukkan manajemen risiko organisasi (*enterprise risk management*) terdiri dari dua elemen besar: (1) Infrastruktur atau prasarana, yang terdiri dari prasarana lunak dan keras, dan (2) Proses Manajemen Risiko. Kemudian manajemen risiko organisasi bertujuan membantu pencapaian tujuan organisasi, dalam hal ini dirumuskan secara eksplisit menjadi memaksimumkan nilai perusahaan.

C. ELEMEN MANAJEMEN RISIKO ORGANISASI

Misalkan kita ditugaskan untuk membuat dan memimpin departemen manajemen risiko suatu perusahaan, bagaimana kita memulainya? Bagan di atas menunjukkan kerangka yang bisa digunakan untuk memulai membangun departemen manajemen risiko. Pertama, kita harus menyiapkan prasarana yang diperlukan untuk memulai pekerjaan manajemen risiko, yang meliputi prasarana lunak (non-fisik) dan prasarana keras (fisik).

1. Prasarana Manajemen Risiko

Salah satu hal yang penting dikerjakan untuk mempersiapkan manajemen risiko adalah menyiapkan prasarana yang mendukung manajemen risiko, yang meliputi prasarana lunak dan keras.

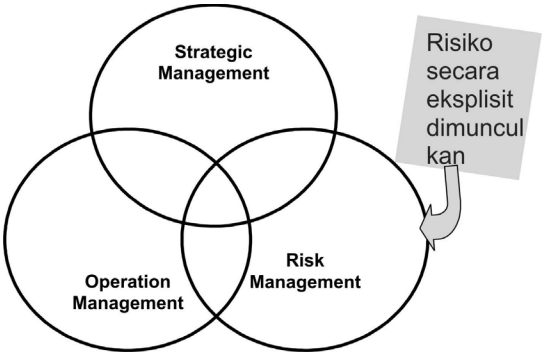
a. Prasarana lunak

Ada beberapa isu yang berkaitan dengan penyiapan prasarana lunak untuk manajemen risiko, yaitu: (1) Mengembangkan budaya sadar risiko untuk anggota organisasi, (2) Dukungan manajemen.

Mengembangkan Budaya Sadar Risiko. Tujuan dari budaya sadar risiko adalah agar setiap anggota organisasi sadar adanya risiko, dan mengambil keputusan tertentu dengan mempertimbangkan aspek risikonya. Dengan singkat, tujuan budaya sadar risiko adalah agar anggota lebih berhati-hati dalam pengambilan keputusan. Jika anggota tersebut sadar akan risiko, maka organisasi (yang terdiri dari kumpulan individu) akan menjadi lebih peka terhadap risiko.

Bagaimana mengembangkan perilaku yang sadar risiko untuk anggota organisasi? Salah satu cara yang bisa dilakukan adalah dengan memaksa mereka untuk berpikir risiko untuk setiap keputusan yang akan diambil. Pebisnis secara natural adalah orang yang optimis (karena itu mereka berani terjun ke dunia bisnis), dan cenderung melupakan aspek risiko (yang mendorong mereka untuk lebih berhati-hati). Jika dipaksa untuk berpikir mengenai risiko, maka mereka akan lebih seimbang dalam memutuskan sesuatu.

Sebagai contoh, bagan berikut ini menunjukkan tiga aspek yang harus dipikirkan oleh manajer dalam pengambilan keputusan, yaitu aspek strategis, operasi, dan risiko. Evaluasi terhadap risiko yang mungkin terjadi harus dipikirkan dan dilaporkan secara eksplisit.



Gambar 1.7.
Aspek Risiko Yang Dimunculkan Secara Eksplisit

Misalkan seorang manajer akan meluncurkan produk baru. Dia harus memikirkan tiga aspek yang disebutkan di atas, dengan pertanyaan seperti berikut ini.

1) Aspek Strategis: Apakah produk ini bisa memenuhi kebutuhan konsumen? Apakah produk ini bisa membantu pencapaian tujuan perusahaan (mencapai target keuntungan tertentu)?
2) Aspek Operasi: Bagaimana memproduksi produk ini? Apakah perusahaan mempunyai kemampuan memproduksi produk ini? Bagaimana memasarkan dan mengembangkan jaringan distribusi untuk produk ini?
3) Aspek Risiko: Risiko apa saja yang bisa muncul berkaitan dengan peluncuran produk ini? Bagaimana perusahaan bisa mengendalikan risiko-risiko tersebut?

Perhatikan pertanyaan aspek risiko secara eksplisit dimunculkan. Misalkan seorang manajer akan meluncurkan program promosi/iklan. Dia harus memikirkan tiga aspek yang disebutkan di atas, melalui pertanyaan-pertanyaan berikut ini.

1) Aspek Strategis: Bagaimana strategi promosi yang efektif? Bagaimana kontribusi promosi ini terhadap tujuan organisasi?
2) Aspek Operasi: Bagaimana menjalankan program promosi ini? Media apa yang paling efektif? Bagaimana *timing* (waktu yang tepat) untuk promosi ini? Bagaimana aspek detil lainnya dari promosi ini? Bagaimana

mengendalikan risiko-risiko yang barangkali muncul akibat peluncuran program promosi ini?

3) Aspek Risiko: Risiko apa yang potensial muncul akibat dari program promosi ini? Apakah promosi ini bisa menimbulkan gugatan hukum? Apakah promosi ini sudah etis? Pihak-pihak mana saja yang barangkali berkeberatan dengan promosi ini?

Perhatikan bahwa sama seperti sebelumnya, aspek risiko secara eksplisit perlu dipikirkan dan dimunculkan. Jika manajer terbiasa berpikir secara eksplisit mengenai risiko-risiko yang mungkin muncul, maka manajer tersebut akan semakin sadar terhadap risiko. Jika semua anggota organisasi sadar akan risiko, maka organisasi menjadi lebih sadar dan lebih peka terhadap risiko.

Mengembangkan kesadaran risiko juga bisa dilakukan melalui *workshop* atau pertemuan secara berkala antar manajer atau anggota organisasi. Agenda dalam *workshop* tersebut adalah membicarakan kejadian-kejadian yang bisa menimbulkan dampak yang negatif terhadap organisasi, alternatif-alternatif pemecahannya. *Workshop* tersebut bisa dikelola oleh manajer risiko perusahaan atau departemen risiko perusahaan. Melalui *workshop* atau pertemuan yang regular yang membicarakan risiko dengan segala aspeknya yang relevan, anggota organisasi diharapkan menjadi lebih sadar akan risiko yang dihadapi organisasi.

Teknik lain yang bisa digunakan adalah memasukkan risiko ke dalam elemen penilaian kinerja. Sebagai contoh, alokasi modal diberikan kepada usulan investasi yang memberikan *risk-adjusted return* (tingkat keuntungan setelah disesuaikan dengan risikonya) yang paling tinggi. Jika kriteria semacam itu yang akan dipakai, maka organisasi akan secara langsung 'menghukum' manajer yang berperilaku risiko tinggi. Risiko tinggi bisa dibenarkan sepanjang memberikan tingkat keuntungan yang diharapkan yang lebih tinggi juga. Dengan mekanisme evaluasi semacam itu, manajer diharapkan akan lebih sadar mengenai risiko, dan budaya risiko di organisasi akan menjadi semakin baik (semakin sadar akan risiko).

Dukungan Manajemen. Sama seperti program lainnya, dukungan manajemen khususnya manajemen puncak terhadap program manajemen risiko penting diberikan. Bentuk dukungan bisa eksplisit maupun implisit. Dukungan manajemen puncak bisa dituangkan antara lain ke dalam pernyataan tertulis, misal manajemen puncak mendukung atau ikut

merumuskan/menyetujui misi dan visi, prosedur dan kebijakan, yang berkaitan dengan manajemen risiko. Dukungan manajemen juga bisa ditunjukkan melalui partisipasi manajemen pada program-program manajemen risiko.

b. Prasarana keras

Di samping prasaran lunak, prasarana keras juga perlu disiapkan. Contoh prasarana keras yang perlu disiapkan adalah ruangan perkantoran, komputer, dan prasarana fisik lainnya. Prasarana fisik tersebut perlu dipersiapkan agar pekerjaan manajemen risiko berjalan sebagaimana mestinya.

2. Proses Manajemen Risiko

Elemen yang lebih penting lagi adalah proses manajemen risiko. Proses atau fungsi manajemen sering diterjemahkan ke dalam tiga langkah: perencanaan, pelaksanaan, dan pengendalian. Mengikuti kebiasaan tersebut, proses manajemen risiko juga bisa dibagi ke dalam tiga tahap yaitu perencanaan, pelaksanaan, dan pengendalian manajemen risiko.

a. Perencanaan

Perencanaan manajemen risiko bisa dimulai dengan menetapkan visi, misi, dan tujuan, yang berkaitan dengan manajemen risiko. Kemudian perencanaan manajemen risiko bisa diteruskan dengan penetapan target, kebijakan, dan prosedur yang berkaitan dengan manajemen risiko. Akan lebih baik lagi jika visi, misi, kebijakan, dan prosedur tersebut dituangkan secara tertulis. Dokumen tertulis semacam itu memudahkan pengarahan, sekaligus menegaskan dukungan manajemen terhadap program manajemen risiko.

Berikut ini beberapa contoh misi atau kebijakan dan prosedur yang berkaitan dengan manajemen risiko dari beberapa perusahaan/organisasi.

PERNYATAAN MISI MANAJEMEN RISIKO GOLDMAN SACH:
Misi dari departemen risiko adalah mengumpulkan, menganalisis, memonitor, dan mendistribusikan informasi yang berkaitan dengan risiko pasar dari posisi perusahaan supaya traders, manajer, dan personel lain dalam organisasi dan terutama komite risiko memahami dan membuat keputusan berdasarkan informasi (informed decisions) mengenai manajemen dan pengendalian risiko yang diambil.
(Goldman Sach adalah perusahaan sekuritas Amerika Serikat)

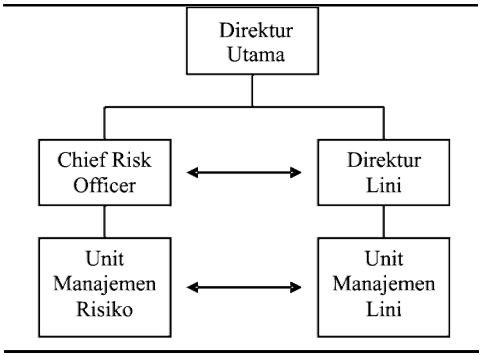
PERNYATAAN MISI SWISS BANK CORPORATION:
Pengendalian risiko Swiss Bank memfokuskan pada perlindungan terhadap modal dan memungkinkan pengambilan risiko yang sesuai. Kepentingan investor Swiss Bank adalah hal yang utama. Modal yang mereka investasikan harus dikompensasi untuk risiko yang ditanggung, baik untuk transaksi individual maupun portofolio.

Setelah misi dan kebijakan serta prosedur yang umum ditetapkan, langkah berikutnya adalah menyusun kebijakan serta prosedur yang lebih spesifik.

b. Pelaksanaan

Pelaksanaan manajemen risiko meliputi aktivitas operasional yang berkaitan dengan manajemen risiko. Proses identifikasi dan pengukuran risiko, kemudian diteruskan dengan manajemen (pengelolaan) risiko merupakan aktivitas operasional yang utama dari manajemen risiko. Identifikasi, pengukuran, dan manajemen risiko akan dibicarakan lebih detil di bagian dua, tiga, dan empat, dari modul ini. Bagian empat khusus membicarakan ilustrasi bagaimana perusahaan menerapkan manajemen risiko secara terencana dan sistematis di organisasinya.

Untuk melaksanakan pekerjaan manajemen risiko, diperlukan organisasi (struktur organisasi) dan *staffing* (personel). Struktur organisasi manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya. Berikut ini contoh struktur organisasi manajemen risiko.

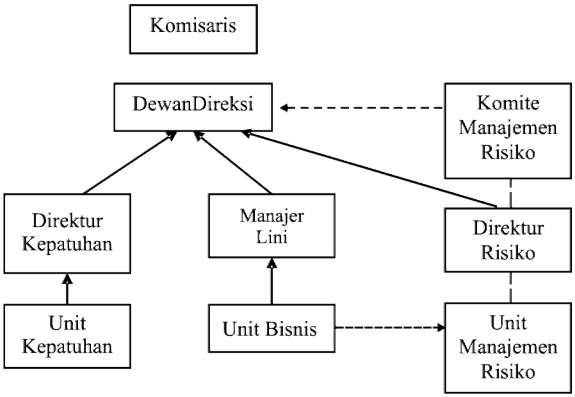


Gambar 1.8.
Struktur Organisasi Manajemen Risiko

Dalam Gambar 1.8 di atas, unit manajemen risiko bertanggung jawab ke manajer risiko yang disebut sebagai *chief risk officer* (CRO). CRO kemudian melapor (bertanggung jawab) langsung ke direktur utama. Pemisahan unit manajemen risiko menjadi bagian sendiri diharapkan mampu menjaga independensi unit manajemen risiko. Unit manajemen risiko mempunyai kedudukan yang sejajar dengan unit lini (pemasaran, keuangan, produksi). Status sebagai unit lini memungkinkan kekuatan yang cukup dalam organisasi untuk mendorong praktek manajemen risiko yang baik dalam suatu organisasi. Unit lini berkomunikasi dengan unit manajemen risiko (seperti ditunjukkan panah dua arah). Komunikasi semacam itu penting agar unit manajemen risiko memperoleh gambaran yang lengkap mengenai risiko yang dihadapi oleh perusahaan.

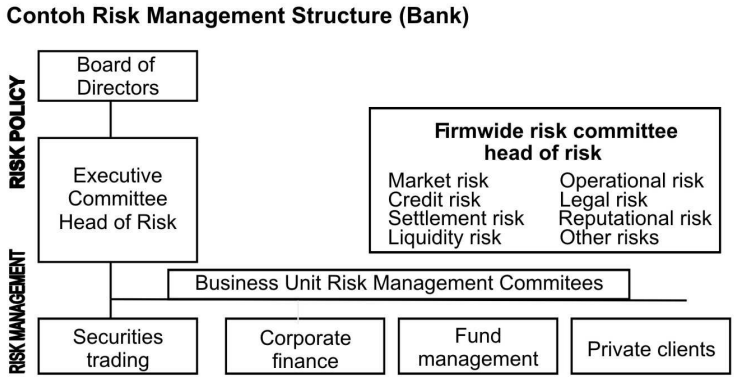
Aspek perilaku dari struktur organisasi manajemen risiko juga perlu diperhatikan. Pekerjaan manajemen risiko cenderung bertentangan dengan pekerjaan manajemen lini. Manajemen lini (misal pemasaran) ingin berjalan cepat tanpa memperhitungkan risiko. Manajemen risiko cenderung menahan keinginan semacam itu dengan mengingatkan risiko-risiko yang mungkin muncul. Struktur organisasi bisa diakomodasi untuk mengatasi potensi konflik semacam itu. Sebagai contoh, unit manajemen risiko bisa dibuat untuk melapor ke manajer risiko dan manajer lini sekaligus. Tetapi cara semacam itu barangkali tidak sempurna, karena pelaporan menjadi tidak jelas (ambigu). Contoh lain, unit manajemen risiko bertanggung jawab ke manajer lini dan memberikan laporan (hubungan garis terputus) kepada manajer risiko. Contoh lain adalah sebaliknya, unit lini bertanggung jawab ke manajer lini dan memberikan laporan ke manajer risiko. Contoh terakhir mirip seperti struktur organisasi pada bagan di atas.

Berikut ini dua contoh variasi dari struktur manajemen risiko.



Gambar 1.9.
Struktur Organisasi Manajemen Risiko Bank

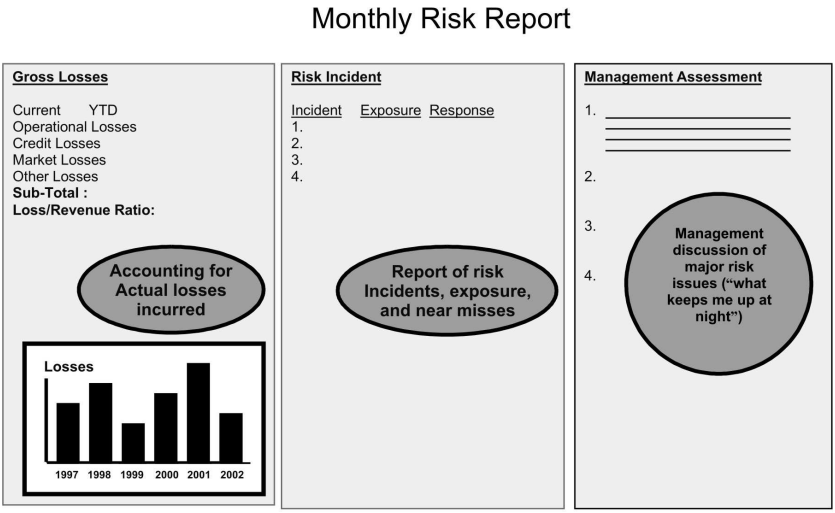
Pada struktur di atas, komite manajemen risiko mengawasi manajemen risiko organisasi. Direktur risiko mengelola kegiatan operasional manajemen risiko. Unit bisnis berkomunikasi dengan unit manajemen risiko untuk melaporkan hal-hal yang berkaitan dengan risiko organisasi. Direktur risiko mempunyai garis keanggotaan kepada komite manajemen risiko.



Gambar 1.10.
Struktur Organisasi Manajemen Risiko Bank (2)

c. Pengendalian

Tahap berikutnya dari proses manajemen risiko adalah pengendalian yang meliputi evaluasi secara periodik pelaksanaan manajemen risiko, output pelaporan yang dihasilkan oleh manajemen risiko, dan umpan balik (*feedback*). Format pelaporan manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya, dan dari satu kegiatan ke kegiatan lainnya. Sebagai contoh, bagan berikut ini menampilkan laporan profil risiko regular (misal bulanan).

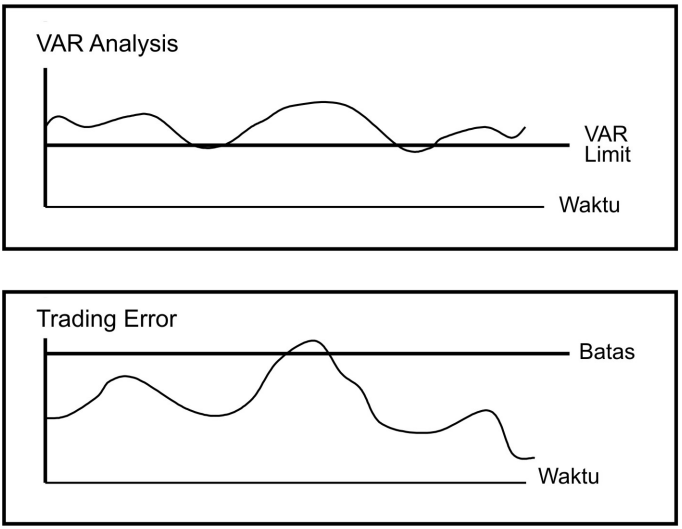


Gambar 1.11.
Contoh Laporan Risiko Bulanan

Gambar 1.11 tersebut menunjukkan laporan kerugian (keuntungan) di sebelah kiri. Gambar di tengah menunjukkan laporan mengenai kejadian-kejadian penting yang menyebabkan perusahaan mengalami kerugian, atau hampir rugi, eksposur perusahaan terhadap kejadian tersebut, dan respons yang dilakukan oleh organisasi. Sebagai contoh, perusahaan barangkali melaporkan kejadian naiknya tingkat bunga sebesar 1% (cukup tinggi). Kemudian perusahaan melaporkan eksposur yaitu posisi obligasi dengan nilai
$10 juta (sepuluh juta dolar AS). Jika tingkat bunga naik, maka nilai obligasi akan turun (yang berarti perusahaan mengalami kerugian). Kolom berikutnya menyajikan respons yang dilakukan perusahaan dalam situasi tersebut (misal

melakukan *hedging*). Bagan paling kanan menunjukkan evaluasi dan diskusi oleh manajemen terhadap risiko-risiko utama yang dihadapi oleh perusahaan.

Unit manajemen risiko bisa juga menampilkan laporan berikut ini.



Gambar 1.12.
Contoh Laporan Risiko Untuk VAR dan *Trading Error*

Kedua bagan tersebut menunjukkan perkembangan VAR (*Value At Risk*, yang merupakan indikator risiko pasar) dan kesalahan perdagangan dari waktu ke waktu. Perusahaan juga menampilkan batas untuk masing-masing variabel risiko tersebut. Jika variabel risiko tersebut masih berada di bawah batas toleransi, maka risiko tersebut belum menunjukkan tingkat keseriusan yang tinggi. Tetapi jika variabel yang diamati tersebut bergerak melewati batas toleransi perusahaan, maka perusahaan harus lebih aktif untuk mengelola risiko tersebut.

Manajer risiko bisa juga menampilkan profil risiko untuk kegiatan tertentu. Sebagai contoh tabel berikut ini menunjukkan profil risiko untuk dua proyek A dan B. Risiko dilihat berdasarkan dimensi keuangan, sosial, dan politik.

Tabel 1.4.
Profil Risiko Usulan Investasi

	Keuangan	Sosial	Politik
Proyek A	1) Tinggi	3)Tinggi 4)Tinggi	5) Tinggi
Proyek B	1)Medium 2)Rendah	3)Medium 4)Rendah	5) Rendah

Keuangan: (1) Risiko kesulitan akses dana, (2) Risiko perubahan kurs
Sosial: (3) Penerimaan masyarakat sekitar, (4) Dukungan pemerintah lokal
Politik: (5) Stabilitas politik, (6) Perubahan Peraturan

Tabel 1.4 tersebut menunjukkan beberapa item risiko untuk keuangan, sosial, dan politik yang dievaluasi. Sebagai contoh, untuk keuangan ada dua item yang dievaluasi, yaitu risiko kesulitan akses dana dan risiko perubahan kurs. Proyek A tidak mempunyai risiko perubahan kurs karena lebih banyak beroperasi di pasar domestik. Dari tabel tersebut terlihat bahwa proyek A nampaknya mempunyai risiko yang lebih besar dibandingkan dengan proyek B. Semua item risiko untuk proyek A mempunyai penilaian risiko yang tinggi. Sedangkan untuk proyek B, kebanyakan item risiko dinilai medium atau rendah. Dengan demikian bisa diambil kesimpulan bahwa proyek A mempunyai risiko yang lebih tinggi dibandingkan dengan proyek B.

Jika pelaporan tersebut belum memuaskan (misal belum cukup informatif), maka format pelaporan bisa di rubah-rubah lagi. Proses umpan balik (*feedback*) harus dijamin bisa berjalan sebagaimana mestinya. Di samping itu hasil evaluasi dari manajemen risiko harus dikomunikasikan ke pihak-pihak yang berkepentingan dan relevan (*stakeholders*). Komunikasi yang baik menjamin disclosure dan transparansi yang baik, yang merupakan elemen manajemen risiko yang baik. Kasus Enron yang bangkrut pada tahun 2001 menunjukkan bahwa organisasi tersebut gagal membangun komunikasi dan transparansi yang baik. Manajemen risiko yang baik harus menjamin terjadinya good corporate governance, diantaranya terjaminnya disclosure dan transparansi yang baik.

Daftar Pustaka

Anderson, Sweeny, and Williams. (1999). *Statistics for Business and Economics*, South-Western Publishing, Cincinnati.

Barton, Thomas, William G. Shenkir, Paul L. Walker. (2002). *Making Enterprise Risk Management Pay Off.* New Jersey: Prentice Hall.

Boodie, Zvi and Robert C. Merton. (2000). *Finance.* New Jersey: Prentice Hall.

Doherty, Neil. (2000). *Integrated Risk Management.* New York: McGraw Hill.

Hanafi, Mamduh. (2005). *Manajemen Keuangan.* Yogyakarta: BPFE.

Hanafi, Mamduh. (2004). *Manajemen Keuangan Internasional.* Yogyakarta: BPFE.

Harrington, Scott E., dan Gregory R. Niehaus. (2003). *Risk Management and Insurance.* Boston: McGraw Hill.

Lam, James. (2004). *Enterprise Risk Management.* Wiley.

Marshall, John F., dan Vipul K. Bansal. (1992). *Financial Engineering, A Complete Guide to Financial Innovation.* New York: Institute of Finance.

Pande, Pete and Larry Holpp. (2002). *What is Six Sigma.* New York.

Risk Group (ed.). (2001). *Advances in Operational Risk.* London: Risk Water Group Ltd.

Saunders and Cornett. (2003). *Financial Institutions Management, A Risk Management Approach*, McGraw Hill.

SBC Warburg. (2004). *The Practice of Risk Management*, Euromoney Book.

Stulz, Rene M. (2003). *Risk Management and Derivatives.* Thomson-South Western.

Trieschmann, dan Gustavson. (1995). *Risk Management and Insurance*, South Western College Publishing.

Williams, C. Arthur, Michael Smith, and Peter C. Young. (1998). *Risk Management and Insurance*, Boston: McGraw Hill.

http ://www. wikip edia. corn.

1. Pendahuluan

Enterprise risk management. Secara singkat, pengertian dan definisi risiko cukup beragam. Sumber risiko pada dasarnya adalah ketidakpastian. Ketidakpastian memunculkan risiko. Proses manajemen risiko adalah tahapan yang dilakukan untuk mengelola risiko secara sistematis. *Enterprise Risk Management* (ERM) adalah manajemen risiko dalam suatu organisasi. Modul satu berikut ini membicarakan lebih lanjut ketiga konsep dasar manajemen risiko tersebut. Setelah mempelajari Modul 1 ini, secara umum Anda diharapkan dapat menjelaskan gambaran secara umum mengenai risiko dan pengelolaan risiko tersebut. Secara khusus, setelah mempelajari Modul 1 ini, Anda diharapkan bisa menjelaskan:

1. Beberapa pengertian dan definisi risiko.
2. Kondisi ketidakpastian sebagai sumber risiko.
3. Beberapa contoh kerugian yang dialami organisasi akibat kegagalan mengelola risiko.
4. Proses atau tahapan dalam pengelolaan risiko.
5. *Enterprise Risk Management* (pengelolaan risiko dalam suatu organisasi).
6. Komponen-komponen dalam *Enterprise Risk Management.*

A. RISIKO DAN KONDISI KETIDAKPASTIAN

Risiko merupakan kata yang sudah kita dengar hampir setiap hari. Biasanya kata tersebut mempunyai konotasi yang negatif, sesuatu yang tidak kita sukai, sesuatu yang ingin kita hindari. Sebagai contoh, jika kita jalan keluar dengan mobil, maka ada risiko mobil kita bertabrakan dengan mobil lainnya (kejadian yang tidak kita inginkan). Jika kita mempunyai saham, ada risiko harga saham yang kita pegang turun nilainya, sehingga kita tidak memperoleh keuntungan (kejadian yang tidak kita harapkan). Jika bank memberikan kredit kepada suatu perusahaan, maka ada kemungkinan perusahaan tersebut gagal bayar (tidak membayar bunga dan/atau cicilan pinjamannya).

Apa yang dimaksud dengan risiko? Risiko bisa didefinisikan dengan berbagai cara. Sebagai contoh, risiko bisa didefinisikan sebagai kejadian yang merugikan. Definisi lain yang sering dipakai untuk analisis investasi, adalah kemungkinan hasil yang diperoleh menyimpang dari yang diharapkan. Deviasi standar merupakan alat statistik yang bisa digunakan untuk mengukur penyimpangan, karena itu deviasi standar bisa dipakai untuk mengukur risiko. Pengukuran yang lain adalah menggunakan probabilitas. Sebagai contoh, pengemudi kendaraan orang muda lebih sering mengalami kecelakaan dibandingkan dengan orang dewasa. Probabilitas terjadinya kecelakaan untuk orang muda lebih tinggi dibandingkan dengan untuk orang dewasa. Karena itu risiko kecelakaan untuk orang muda lebih tinggi dibandingkan untuk orang dewasa.

Kenapa muncul suatu risiko? Risiko berkaitan erat dengan kondisi ketidakpastian.

Risiko muncul karena ada kondisi ketidakpastian. Praktis kita menghadapi banyak ketidakpastian di dunia ini. Sebagai contoh, hari ini bisa hujan, bisa juga tidak hujan. Investasi kita bisa mendatangkan keuntungan (harga naik), bisa juga menyebabkan kerugian (harga turun). Kepastian dalam dunia ini adalah ketidakpastian itu sendiri. Ketidakpastian tersebut menyebabkan munculnya risiko. Ketidakpastian itu sendiri ada banyak

tingkatannya. Tabel berikut ini menunjukkan tingkatan ketidakpastian dengan karakteristiknya.

Tabel 1.1.

Tingkatan Ketidakpastian

TINGKAT KETIDAKPASTIAN	KARAKTERISTIK	CONTOH
TIDAK ADA (PASTI)	HASIL BISA DIPREDIKSI DENGAN PASTI	HUKUM ALAM
KETIDAKPASTIAN OBJEKTIF	HASIL BISA DIIDENTIFIKASI DAN PROBABILITAS DIKETAHUI	PERMAINAN DADU, KARTU
KETIDAKPASTIAN SUBJEKTIF	HASIL BISA DIIDENTIFIKASI TAPI PROBABILITAS TIDAK DIKETAHUI	KEBAKARAN, KECELAKAAN MOBIL, INVESTASI
SANGAT TIDAK PASTI	HASIL TIDAK BISA DIIDENTIFIKASI DAN PROBABILITAS TIDAK DIKETAHUI	EKSPLORASI ANGKASA

Pada tingkatan pertama, kondisi kepastian sangat tinggi. Hasil bisa diprediksi dengan relatif pasti. Hukum alam merupakan contoh kepastian tersebut. Sebagai contoh, kita bisa memprediksi dengan pasti bahwa bumi mengitari matahari selama 360 hari (satu tahun). Tingkatan selanjutnya adalah ketidakpastian objektif, dengan contoh adalah dadu, jika kita melempar dadu, ada enam kemungkinan yaitu angka 1, 2, 3, 4, 5, dan 6 (ada enam kemungkinan hasil). Kita bisa menghitung probabilitas masing-masing angka untuk keluar, yaitu 1/6.

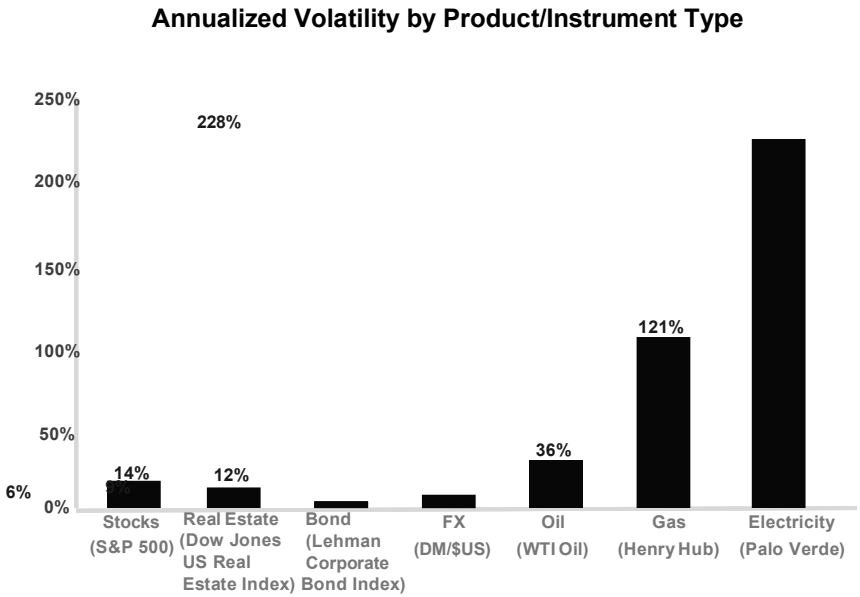
Tingkatan berikutnya adalah ketidakpastian subjektif, dengan contoh adalah kecelakaan mobil. Identifikasi hasil dan probabilitas (kemungkinan) yang berkaitan dengan kecelakaan mobil lebih sulit dilakukan. Sebagai contoh, jika kita pergi keluar dengan mobil, berapa besar probabilitas kita mengalami kecelakaan mobil? Dan jika terjadi kecelakaan, kerusakan atau kerugian yang bagaimana yang akan kita dapatkan? Tidak mudah untuk menjawab pertanyaan tersebut. Tingkatan berikutnya adalah kondisi sangat

tidak pasti, dengan contoh eksplorasi angkasa. Kita tidak tahu apa hasil yang akan diperoleh dari eksplorasi angkasa, apakah akan bertemu dengan makhluk asing (*alien*), ataukah menemukan planet yang mirip bumi, atau apa

yang akan kita temukan. Sangat sulit memprediksi atau mengidentifikasi hasil yang barangkali bisa diperoleh dari eksplorasi angkasa seperti itu. Tentu saja juga akan sangat sulit menentukan probabilitas untuk masing-masing kemungkinan hasil tersebut.

Ketidakpastian bisa tercermin dari fluktuasi pergerakan yang tinggi; Semakin tinggi fluktuasi, semakin besar tingkat ketidakpastiannya. Bagan berikut ini menunjukkan fluktuasi harga beberapa instrumen (dihitung berdasarkan deviasi standar tahunan). Terlihat bahwa semua harga instrumen berfluktuasi. Sebagai contoh, saham mempunyai fluktuasi sebesar 14%, sementara harga listrik mempunyai fluktuasi sebesar 228%.

Hasil empiris pada bagan di atas menunjukkan bahwa di dunia ini semuanya serba tidak pasti. Saham, valas (FX), harga minyak, sampai dengan harga listrik, mempunyai fluktuasi, meskipun dengan tingkat fluktuasi yang berbeda-beda. Kepastian adalah ketidakpastian itu sendiri. Dengan demikian risiko ada di mana-mana, mencakup semua instrumen.



Gambar 1.1.
Fluktuasi Tahunan Berdasarakn Tipe Instrumen

Selain itu, fluktuasi harga cenderung semakin meningkat dari tahun ke tahun. Sebagai ilustrasi, Indonesia mengalami perubahan sistem kurs dari tetap menjadi mengambang pada pertengahan tahun 1997. Sebelum krisis pada tahun 1997, Indonesia menganut sistem kurs tetap, dengan menetapkan kurs Rp/$ pada tingkat sekitar Rp2.500/$. Pada pertengahan tahun 1997, untuk mengurangi tekanan terhadap kurs karena ada krisis ekonomi, pemerintah mengambangkan kurs Rp/$. Sistem kurs mengambang tersebut masih berlaku sampai saat ini. Kurs Rp/$ tidak lagi tetap, tetapi bisa berubah tergantung mekanisme pasar. Sistem kurs mengambang tersebut mengakibatkan fluktuasi kurs Rp/$ jauh lebih tinggi dibandingkan dengan fluktuasi kurs Rp/$ pada sistem kurs tetap.

Mengapa fluktuasi cenderung meningkat? Ada beberapa faktor yang mendorong peningkatan fluktuasi tersebut, seperti:

1. Globalisasi dunia.
2. Liberalisasi dunia.
3. Proses Informasi yang semakin cepat, reaksi investor yang semakin cepat.

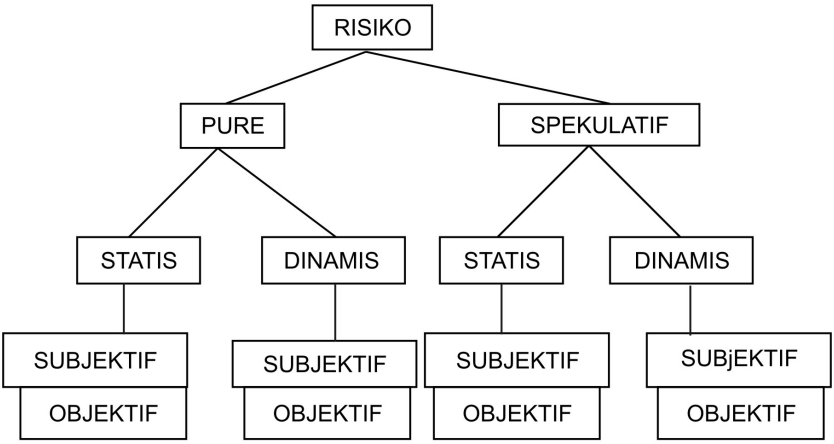
Globalisasi dunia membuat keterkaitan perekonomian dunia lebih erat. Kejadian di suatu negara akan lebih cepat mempengaruhi negara lain. Dengan kondisi seperti itu, fluktuasi akan cenderung meningkat. Liberalisasi dunia (membuka pasar domestik terhadap investor asing) mempunyai efek yang sama dengan globalisasi. Hambatan antar negara menjadi berkurang. Aliran modal menjadi lebih mudah untuk masuk atau keluar. Hal semacam ini akan meningkatkan fluktuasi dunia. Sebagai ilustrasi, krisis ekonomi di Thailand pada tahun 1997, memicu terjadinya krisis ekonomi di negara-negara sekitarnya (Indonesia, Filipina, Malaysia) dengan cepat. Investor dengan cepat memindahkan dananya dari Thailand dan negara-negara sekitarnya ke negara-negara lain yang dianggap lebih aman. Terbukanya perekonomian dunia memungkinkan pergerakan modal yang cepat semacam itu.

Teknologi yang semakin maju membuat investor atau pelaku pasar semakin canggih dalam memproses informasi. Kecanggihan tersebut akan mendorong pelaku pasar untuk lebih cepat memperoleh informasi dan bertindak lebih cepat atas informasi tersebut. Kemudahan informasi dan reaksi yang cepat dari investor akan mendorong fluktuasi harga yang semakin tinggi.

Globalisasi, liberalisasi, dan teknologi yang semakin canggih akan semakin meningkatkan fluktuasi harga, semakin meningkatkan ketidakpastian. Fluktuasi tersebut ternyata praktis dialami oleh semua atau sebagian besar instrumen keuangan atau komoditas di dunia. Dengan demikian bisa diambil kesimpulan bahwa risiko ada di mana-mana, dan risiko cenderung semakin meningkat dari tahun ke tahun.

B. TIPE-TIPE RISIKO

Risiko beragam jenisnya, mulai dari risiko kecelakaan, kebakaran, risiko kerugian, fluktuasi kurs, perubahan tingkat bunga, dan lainnya. Untuk memudahkan pemahaman dan analisis terhadap risiko, kita bisa memetakan atau mengelompokkan risiko-risiko tersebut. Salah satu cara untuk mengelompokkan risiko adalah dengan melihat tipe-tipe risiko. Bagan berikut ini menunjukkan bahwa risiko bisa dikelompokkan ke dalam dua tipe risiko: risiko murni dan risiko spekulatif, risiko subjektif dan objektif, dan dinamis dan statis.



Gambar 1.2.
Kategorisasi Risiko

Risiko bisa dikelompokkan ke dalam risiko murni dan risiko spekulatif dengan penjelasan sebagai berikut ini.

1. Risiko murni (*pure risks*) adalah risiko di mana kemungkinan kerugian ada, tetapi kemungkinan keuntungan tidak ada. Jadi kita membicarakan potensi kerugian untuk risiko tipe ini. Beberapa contoh risiko tipe ini adalah risiko kecelakaan, kebakaran, dan semacamnya. Contoh lain adalah risiko banjir menghantam rumah kita. Kejadian seperti itu akan merugikan kita. Tetapi rumah berdiri di tempat tertentu tidak secara langsung akan mendatangkan keuntungan tertentu. Jika terjadi kebakaran atau banjir, di samping individu yang terkena dampaknya, masyarakat secara keseluruhan juga akan dirugikan. Asuransi biasanya lebih banyak berurusan dengan risiko murni.
2. Risiko spekulatif adalah risiko di mana kita mengharapkan terjadinya kerugian dan juga keuntungan. Potensi kerugian dan keuntungan dibicarakan dalam jenis risiko ini. Contoh tipe risiko ini adalah usaha bisnis. Dalam kegiatan bisnis, kita mengharapkan keuntungan, meskipun ada potensi kerugian. Contoh lain adalah jika kita memegang (membeli) saham. Harga pasar bisa meningkat (kita memperoleh keuntungan), bisa juga analisis kita salah, harga saham bukannya meningkat, tetapi malah turun (kita memperoleh kerugian). Risiko spekulatif juga bisa dinamakan sebagai risiko bisnis. Kerugian akibat risiko spekulatif akan merugikan individu tertentu, tetapi akan menguntungkan individu lainnya. Misalkan suatu perusahaan mengalami kerugian karena penjualannya turun, perusahaan lain barangkali akan memperoleh keuntungan dari situasi tersebut. Secara total, masyarakat tidak dirugikan oleh risiko spekulatif tersebut.

Di samping kategorisasi murni dan spekulatif, risiko juga bisa dibedakan antara risiko yang dinamis dan yang statis.

1. Risiko statis muncul dari kondisi keseimbangan tertentu. Sebagai contoh, risiko terkena petir merupakan risiko yang muncul dari kondisi alam yang tertentu. Karakteristik risiko ini praktis tidak berubah dari waktu ke waktu.
2. Risiko dinamis muncul dari perubahan kondisi tertentu. Sebagai contoh, perubahan kondisi masyarakat, perubahan teknologi, memunculkan jenis-jenis risiko baru. Misal, jika masyarakat semakin kritis, sadar akan haknya, maka risiko hukum (*legal risk*) yang muncul karena masyarakat

lebih berani mengajukan gugatan hukum (*sue*) terhadap perusahaan, akan semakin besar.

Risiko juga bisa dikelompokkan ke dalam risiko subjektif dan objektif dengan penjelasan sebagai berikut ini.

1. Risiko objektif adalah risiko yang didasarkan pada observasi parameter yang objektif. Sebagai contoh, fluktuasi harga atau tingkat keuntungan investasi di pasar modal bisa diukur melalui standar deviasi, misal standar deviasi *return* saham adalah 25% per tahun.
2. Risiko subjektif berkaitan dengan persepsi seseorang terhadap risiko. Dengan kata lain, kondisi mental seseorang akan menentukan kesimpulan tinggi rendahnya risiko tertentu. Sebagai contoh, untuk standar deviasi *return* pasar yang sama sebesar 25%, dua orang dengan kepribadian berbeda akan mempunyai cara pandang yang berbeda. Orang yang konservatif akan menganggap risiko investasi di pasar modal terlalu tinggi. Sementara bagi orang yang agresif, risiko investasi di pasar modal dianggap tidak terlalu tinggi. Perhatikan bahwa kedua orang tersebut melihat pada risiko objektif yang sama, yaitu standar deviasi *return* sebesar 25% per tahun.

Berikut ini contoh-contoh risiko yang biasa dihadapi oleh suatu organisasi. Risiko-risiko tersebut dikelompokkan ke dalam risiko murni dan spekulatif.

Tabel 1.2.
Contoh-contoh Risiko Murni

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko Aset Fisik	Risiko yang terjadi karena kejadian tertentu berakibat buruk (kerugian) pada aset fisik organisasi.	Kebakaran yang melanda gudang atau bangunan perusahaan. Banjir mengakibatkan kerusakan pada bangunan dan peralatan
Risiko karyawan	Risiko karena karyawan organisasi mengalami peristiwa yang merugikan	Kecelakaan kerja mengakibatkan karyawan cedera, kegiatan operasional perusahaan terganggu
Risiko legal	Risiko kontrak tidak sesuai yang diharapkan, dokumentasi yang	Terjadi perselisihan sehingga perusahaan lain menuntut ganti rugi yang signifikan

	tidak benar	

Tabel 1.3.

Contoh-Contoh Risiko Spekulatif

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko pasar	Risiko yang terjadi dari pergerakan harga atau volatilitas harga pasar	Harga pasar saham dalam portofolio perusahaan mengalami penurunan, yang mengakibatkan kerugian yang dialami perusahaan.
Risiko kredit	Risiko karena *counter party* gagal memenuhi kewajibannya kepada perusahaan	Debitur tidak bisa membayar cicilan dan bunga hutang, sehingga perusahaan mengalami kerugian. Piutang dagang tidak terbayar.
Risiko Likuiditas	Risiko tidak bisa memenuhi kebutuhan kas, risiko tidak bisa menjual dengan cepat karena ketidaklikuidan atau gangguan pasar	Perusahaan tidak mempunyai kas untuk membayar kewajibannya (misal melunasi hutang). Perusahaan terpaksa menjual tanah dengan harga murah (di bawah standar) karena sulit menjual tanah tersebut (tidak likuid), padahal perusahaan membutuhkan kas dengan cepat.
Risiko operasional	Risiko kegiatan operasional tidak berjalan lancar dan mengakibatkan kerugian: kegagalan sistem, human error, pengendalian dan prosedur yang kurang	Komputer perusahaan terkena virus sehingga operasi perusahaan terganggu. Prosedur pengendalian perusahaan tidak memadai sehingga terjadi pencurian barang-barang yang dimiliki perusahaan.

Pembagian risiko ke dalam dua tipe, yaitu risiko murni dan risiko spekulatif, barangkali tidak sepenuhnya memuaskan. Ada beberapa jenis risiko yang barangkali bisa masuk ke dalam risiko murni maupun spekulatif. Sebagai contoh, risiko tuntutan hukum bisa dimasukkan ke dalam risiko murni, tetapi jika dilihat sebagai konsekuensi kegiatan bisnis, maka risiko tersebut bisa dimasukkan ke dalam risiko spekulatif. Pembagian semacam itu bukan 'harga mati'. Pembagian semacam itu diharapkan memudahkan kita memahami jenis-jenis risiko dan karakteristiknya.

C. PROSES MANAJEMEN RISIKO

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari.

Jika risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa

mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko. Jika organisasi tersebut tidak bisa mengelola risiko dengan baik, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Karena itu risiko yang dihadapi oleh organisasi tersebut juga harus dikelola, agar organisasi bisa bertahan, atau barangkali mengoptimalkan risiko. Perusahaan sering kali secara sengaja mengambil risiko tertentu, karena melihat potensi keuntungan dibalik risiko tersebut.

Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko.
2. Evaluasi dan Pengukuran Risiko, dan
3. Pengelolaan risiko.

1. Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang dihadapi oleh suatu organisasi. Banyak risiko yang dihadapi oleh suatu organisasi, mulai dari risiko penyelewengan oleh karyawan, risiko kejatuhan meteor atau komet, dan lainnya. Ada beberapa teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh, kompor ditaruh dekat penyimpanan minyak tanah. Api merupakan sumber risiko, kompor yang ditaruh dekat minyak tanah merupakan kondisi yang meningkatkan terjadinya kecelakaan, bangunan yang bisa terbakar merupakan *eksposur* yang dihadapi perusahaan. Misalkan terjadi kebakaran, kebakaran merupakan peristiwa yang merugikan (peril). Identifikasi semacam dilakukan dengan melihat sekuen dari sumber risiko sampai ke terjadinya peristiwa yang merugikan. Pada beberapa situasi, risiko yang dihadapi oleh perusahaan cukup standar. Sebagai contoh, bank menghadapi risiko terutama adalah risiko kredit (kemungkinan debitur tidak melunasi hutangnya). Untuk bank yang juga aktif melakukan perdagangan sekuritas, maka bank tersebut akan menghadapi risiko pasar. Setiap bisnis akan menghadapi risiko yang berbeda-beda karakteristiknya.

2. Evaluasi dan Pengukuran Risiko

Langkah berikutnya adalah mengukur risiko tersebut dan mengevaluasi risiko tersebut. Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk 'mengukur' risiko tersebut.

Ada beberapa teknik untuk mengukur risiko tergantung jenis risiko tersebut. Sebagai contoh kita bisa memperkirakan probabilitas (kemungkinan) risiko atau suatu kejadian jelek terjadi. Dengan probabilitas tersebut kita berusaha 'mengukur' risiko. Sebagai contoh, ada risiko perusahaan terkena jatuhan meteor atau komet, tetapi probabilitas risiko semacam itu sangat kecil (0,000000001). Karena itu risiko tersebut tidak perlu diperhatikan. Contoh lain adalah risiko kebakaran dengan probabilitas (misal) 0,6. Karena probabilitas yang tinggi, maka risiko kebakaran perlu diberi perhatian ekstra. Contoh tersebut menunjukkan bahwa dengan menggunakan teknik probabilitas kita bisa melakukan prioritisasi risiko, sehingga kita bisa lebih memfokuskan pada risiko yang mempunyai kemungkinan yang besar untuk terjadi.

Contoh lain adalah membuat matriks dengan sumbu mendatar adalah probabilitas terjadinya risiko, dan sumbu vertikal adalah tingkat keseriusan konsekuensi risiko tersebut (*severity*, atau besarnya kerugian yang timbul akibat risiko tersebut). Setiap risiko bisa dievaluasi kemudian dimasukkan ke dalam matriks tersebut. Sebagai contoh, risiko kebakaran mempunyai probabilitas 0,6 (tinggi). Jika kebakaran terjadi, maka kerugian yang diakibatkan akan besar juga (tinggi). Dengan demikian risiko kebakaran akan ditempatkan pada kuadran probabilitas tinggi dan *severity* tinggi. Selanjutnya langkah yang lebih tepat bisa dirumuskan. Sebagai contoh, untuk risiko kebakaran seperti itu, langkah yang lebih aktif bisa ditujukan untuk menangani risiko kebakaran tersebut.

Untuk risiko lain, evaluasi dan pengukuran yang berbeda bisa dilakukan. Sebagai contoh, risiko perubahan tingkat bunga bisa diukur dengan teknik duration (durasi). Modul identifikasi dan pengukuran risiko spekulatif akan banyak membicarakan pengukuran risiko perubahan tingkat bunga. Risiko pasar bisa dievaluasi dengan menggunakan teknik VAR (*Value At Risk*). Pemahaman kita terhadap beberapa risiko sudah cukup baik sehingga teknik pengukuran risiko tersebut sudah berkembang. Sementara pemahaman kita terhadap risiko lain belum begitu baik sehingga teknik pengukuran risiko tersebut belum begitu berkembang.

Teknik lain untuk mengukur risiko adalah dengan mengevaluasi dampak risiko tersebut terhadap kinerja perusahaan.

3. Pengelolaan Risiko

Setelah analisis dan evaluasi risiko, langkah berikutnya adalah mengelola risiko. Risiko harus dikelola. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misal kerugian yang besar. Risiko bisa dikelola dengan berbagai cara, seperti penghindaran, ditahan (*retention*), diversifikasi, atau ditransfer ke pihak lainnya. Erat kaitannya dengan manajemen risiko adalah pengendalian risiko (*risk control*), dan pendanaan risiko (*risk financing*).

a. Penghindaran. Cara paling mudah dan aman untuk mengelola risiko adalah menghindar. Tetapi cara semacam ini barangkali tidak optimal. Sebagai contoh, jika kita ingin memperoleh keuntungan dari bisnis, maka mau tidak mau kita harus keluar dan menghadapi risiko tersebut. Kemudian kita akan mengelola risiko tersebut.
b. Ditahan (*Retention*). Dalam beberapa situasi, akan lebih baik jika kita menghadapi sendiri risiko tersebut (menahan risiko tersebut, atau *risk retention*). Sebagai contoh, misalkan seseorang akan keluar rumah membeli sesuatu dari supermarket terdekat, dengan menggunakan kendaraan. Kendaraan tersebut tidak diasuransikan. Orang tersebut merasa asuransi terlalu repot, mahal, sementara dia akan mengendarai kendaraan tersebut dengan hati-hati. Dalam contoh tersebut, orang tersebut memutuskan untuk menanggung sendiri (menahan, *retention*) risiko kecelakaan.
c. Diversifikasi. Diversifikasi berarti menyebar eksposur yang kita miliki sehingga tidak terkonsentrasi pada satu atau dua eksposur saja. Sebagai contoh, kita barangkali akan memegang aset tidak hanya satu, tetapi pada beberapa aset, misal saham A, saham B, obligasi C, properti, dan sebagainya. Jika terjadi kerugian pada satu aset, kerugian tersebut diharapkan bisa dikompensasi oleh keuntungan dari aset lainnya.
d. Transfer Risiko. Jika kita tidak ingin menanggung risiko tertentu, kita bisa mentransfer risiko tersebut ke pihak lain yang lebih mampu menghadapi risiko tersebut. Sebagai contoh, kita bisa membeli asuransi kecelakaan. Jika terjadi kecelakaan, perusahaan asuransi akan menanggung kerugian dari kecelakaan tersebut.

e. Pengendalian Risiko. Pengendalian risiko dilakukan untuk mencegah atau menurunkan probabilitas terjadinya risiko atau kejadian yang tidak kita inginkan. Sebagai contoh, untuk mencegah terjadinya kebakaran, kita memasang alarm asap di bangunan kita. Alarm tersebut merupakan salah satu cara kita mengendalikan risiko kebakaran.
f. Pendanaan Risiko. Pendanaan risiko mempunyai arti bagaimana 'mendanai' kerugian yang terjadi jika suatu risiko muncul. Sebagai contoh, jika terjadi kebakaran, bagaimana menanggung kerugian akibat kebakaran tersebut, apakah dari asuransi, ataukah menggunakan dana cadangan? Isu semacam itu masuk dalam wilayah pendanaan risiko.

Di samping proses manajemen risiko seperti yang disebutkan di muka, manajemen risiko suatu organisasi juga memerlukan infrastruktur baik keras maupun lunak. Sebagai contoh, manajemen risiko barangkali akan memerlukan sistem komputer untuk analisis risiko. Manajemen risiko juga memerlukan staf dan struktur organisasi yang tepat. Infrastruktur manajemen risiko tidak dibahas secara khusus dalam modul ini. Modul enam menyajikan ilustrasi bagaimana perusahaan terkemuka dunia mengembangkan manajemen risiko dalam organisasinya.

Enterprise Risk Management

Makhluk hidup secara natural akan mengantisipasi dan 'mengelola' risiko. Sebagai contoh, jika kita keluar mengendarai mobil, maka kita akan waspada dengan kondisi sekitarnya. Jika dari arah yang berlawanan ada mobil yang agak ke tengah jalannya, kita akan menghindari mobil tersebut dengan jalan mengendarainya agak ke kiri, supaya tidak terjadi tabrakan. Konon binatang mempunyai indera keenam yang bisa mendeteksi risiko lebih baik dibandingkan manusia. Pada waktu tsunami melanda wilayah Asia pada tahun 2004, binatang (gajah, dan sebagainya) yang menjadi korban tsunami jauh lebih kecil dibandingkan manusia. Binatang tersebut sepertinya mampu mendeteksi datangnya bahaya, kemudian menyingkir sebelum bahaya tersebut datang. Konon manusia dulu juga mempunyai kemampuan yang serupa, tetapi karena tidak banyak digunakan, karena manusia lebih banyak mengandalkan otak mereka, kemampuan indera keenam tersebut menghilang. Bagaimana dengan organisasi? Organisasi tidak mempunyai kemampuan mengelola risiko seperti halnya manusia atau makhluk hidup mengelola risiko, karena organisasi bukan makhluk hidup. Tugas dari manajer suatu organisasi adalah membuat agar organisasi bisa mengantisipasi dan

mengelola risiko sebagaimana halnya makhluk hidup mengelola risiko yang dihadapinya. Dengan kata lain, tugas manajer adalah membuat organisasi menjadi sadar risiko, sehingga risiko bisa diantisipasi dan dikelola dengan baik.

Tabel 1.4 berikut ini menyajikan konsekuensi merugikan jika suatu organisasi gagal mengelola risiko

Tabel 1.4.
Beberapa Contoh Kegagalan Mengelola Risiko

Tahun	Penjelasan
1997	Trader Bank Baring (Nick Leeson) membeli *instrument derivative* saham Jepang (futures Nikkei). Bank Baring adalah Bank dari Inggris. Ekonomi Jepang turun drastic karena ada bencana gempa Kobe. Akibatnya dia mengalami kerugian besar. Transaksi selanjutnya (jual opsi) tidak mengurangi kerugian, tetapi memperparah kerugian. Pada akhirnya Bank Baring mengalami kerugian sebesar $1,3 miliar. Bank Baring terpaksa bangkrut karena kerugiannya sudah melebihi modalnya.

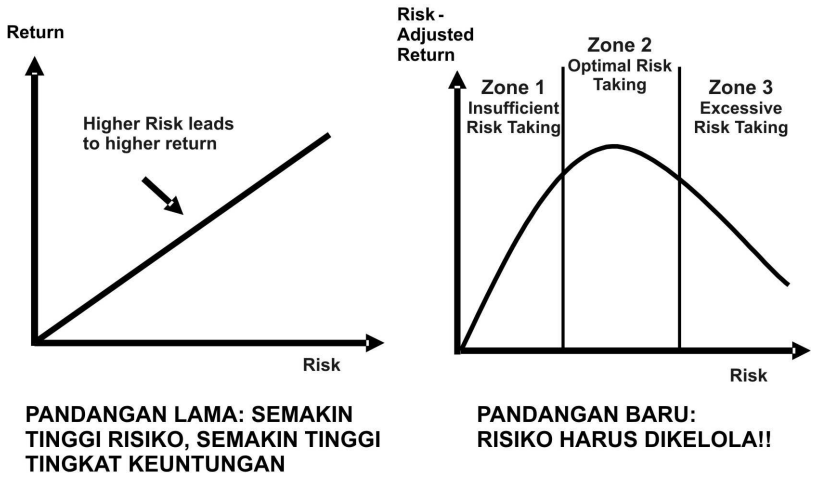
Tahun	Penjelasan
1997	Long Term Capital (LTC), perusahaan investasi di Amerika Serikat, mempunyai posisi pada mata uang Rusia Rubel yang cukup besar. Mereka memperkirakan Rusia tidak akan bangkrut. Tetapi Rusia ternyata bangkrut, mendeklarasikan tidak mampu dan tidak akan membayar hutang-hutangnya. Akibatnya *Long Term Capital* mengalami kerugian yang sangat besar, sekitar $3,5 miliar, dan pada akhirnya LTC terpaksa bangkrut.
2001	Enron merupakan perusahaan yang memperdagangkan energi (jual beli energi). Mereka juga masuk ke kontrak *derivative* energi. Usaha mereka cukup kompleks sehingga transparansi menjadi lebih sulit. Transparansi yang kompleks dimanfaatkan untuk menjalankan sistem akuntansi yang tidak wajar. Di samping itu Enron melakukan beberapa *manuever* agar laporan keuangannya kelihatan baik. Akhirnya investor mengetahui trik-trik mereka. Keuntungan mereka yang sesungguhnya ternyata tidak sebesar yang dilaporkan. Harga saham Enron jatuh dari $80 per lembar menjadi hanya $0,5. Mereka mempunyai kewajiban jangka pendek yang segera jatuh tempo. Mereka tidak bisa memperoleh bantuan dana. Tidak ada yang percaya dengan mereka. Enron akhirnya bangkrut.
1980-an	*Saving Loan* (S & L) *Association* (bank yang memberi pinjaman kredit rumah di Amerika Serikat) mempunyai struktur neraca: memberi kredit rumah dengan bunga tetap jangka panjang (misal 20 tahun), sementara memperoleh dana melalui deposito jangka pendek (misal 1 tahun). Struktur semacam itu rentan terhadap risiko perubahan tingkat bunga. Pada waktu tingkat bunga di Amerika Serikat naik signifikan pada tahun 1980-an, banyak S & L yang mengalami masalah dan puluhan S & L bangkrut karenanya.
1995	Bank Duta (Indonesia) mengalami kerugian yang sangat besar karena mereka melakukan perdagangan valas dan mengalami kerugian besar dari perdagangan valas tersebut.

Pertanyaan yang muncul adalah bisakah organisasi-organisasi di atas menghindari kerugian besar karena munculnya risiko-risiko tersebut? Manajemen risiko organisasi bertujuan menciptakan sistem atau mekanisme dalam organisasi sehingga risiko yang bisa merugikan organisasi bisa diantisipasi dan dikelola untuk tujuan meningkatkan nilai perusahaan.

Pentingnya pengelolaan risiko juga bisa dilihat melalui Bagan 1.1 berikut ini. Bagan 1.1 tersebut menggambarkan pandangan lama (sebelah kiri) dan baru (sebelah kanan) dalam kaitannya antara risiko dengan tingkat keuntungan. Pandangan lama menganggap ada hubungan positif antara risiko dengan tingkat keuntungan. Semakin tinggi risiko, akan semakin tinggi tingkat keuntungan yang diharapkan. Jika suatu organisasi ingin

meningkatkan tingkat keuntungannya, maka organisasi tersebut harus menaikkan risikonya.

Pandangan baru mengatakan bahwa hubungan antara risiko dengan tingkat keuntungan tidak bersifat linear, tetapi non-linear. Pada wilayah satu, risiko yang diambil oleh perusahaan terlalu kecil, sehingga keuntungan yang diperoleh juga kecil. Pada tahap ini, risiko masih bisa ditingkatkan untuk meningkatkan tingkat keuntungan. Contoh ekstrem situasi ini adalah jika manajer hanya tinggal di rumah, tidak pergi ke mana-mana. Dia bisa menghindari banyak risiko (risiko kecelakaan, dan sebagainya), tetapi dia juga tidak mendapatkan banyak keuntungan. Di tahap ini, pengelolaan risiko belum optimal.



Gambar 1.3.
Hubungan Risiko dan Tingkat Keuntungan (*Return*): Pandangan Lama dan Baru

Pada tahap berikutnya (zona 2), penambahan risiko tidak banyak meningkatkan tingkat keuntungan. Tahap ini merupakan tahap optimal. Tahap berikutnya (zona 3), risiko yang diambil organisasi terlalu tinggi, sehingga penambahan risiko akan berakibat negatif terhadap organisasi. Sebagai contoh, bank memberi pinjaman pada sektor-sektor yang risikonya terlalu tinggi, misal usaha burung walet, usaha perjudian. Risiko yang terlalu tinggi menjadi sulit untuk dikendalikan, sehingga bisa berakibat membahayakan dan merugikan perusahaan. Berdasarkan kerangka tersebut, pengelolaan risiko organisasi seharusnya berada pada wilayah tengah (zona 2), yang merupakan zona optimal.

Pengelolaan risiko yang digambarkan dalam bagan di atas bisa diilustrasikan melalui perjalanan dengan menggunakan kendaraan (mobil). Mobil yang berjalan terlalu lambat barangkali tidak menguntungkan, karena beberapa hal, misal terlalu lama, atau bahkan bisa membahayakan kendaraan lainnya. Mobil tersebut perlu dipacu lebih cepat. Jika mobil berjalan terlalu cepat (misal, ngebut), maka risiko bertabrakan atau kehilangan kendali menjadi semakin besar. Tentu saja hal ini tidak menguntungkan. Yang paling optimal adalah mobil berjalan dengan kecepatan optimal, yaitu cukup cepat tetapi bisa dikendalikan. Pengelolaan risiko bisa diilustrasikan sebagai kombinasi penekanan gas (mempercepat kendaraan) dan penekanan rem (memperlambat kendaraan). Kombinasi yang ideal bisa membuat mobil berjalan kencang tetapi tetap terkendali.

B. DEFINISI DAN PENGERTIAN MANAJEMEN RISIKO

Manajemen risiko organisasi adalah suatu sistem pengelolaan risiko yang dihadapi oleh organisasi secara komprehensif untuk tujuan meningkatkan nilai perusahaan. Meskipun pengertian manajemen risiko organisasi adalah seperti yang disebutkan di atas, tetapi ada banyak definisi dan pengertian manajemen risiko organisasi. Berikut ini beberapa definisi manajemen risiko organisasi.

Manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi, untuk mengelola, memonitor, dan mengendalikan eksposur organisasi terhadap risiko (SBC Warburg, *The Practice of Risk Management*, Euromoney Book, 2004)

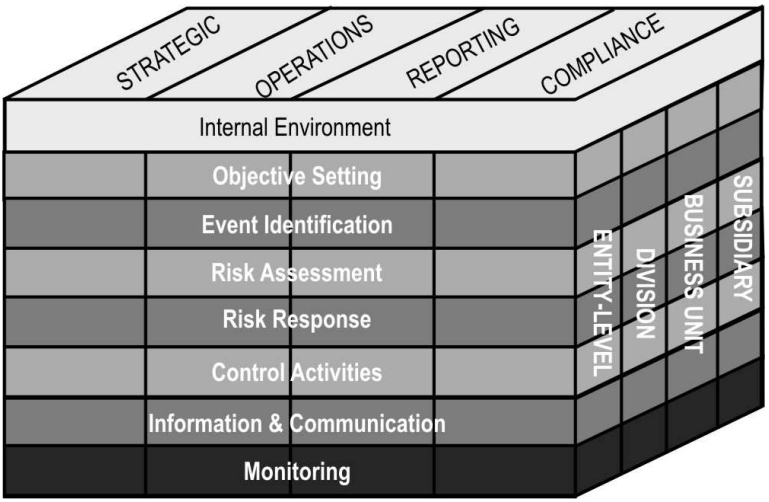
Enterprise Risk Management adalah kerangka yang komprehensif, terintegrasi, untuk mengelola risiko kredit, risiko pasar, modal ekonomis, transfer risiko, untuk memaksimumkan nilai perusahaan (Lam, James, *Enterprise Risk Management*, Wiley, 2004)

Manajemen risiko organisasi mempunyai elemen-elemen berikut ini:
Identifikasi Misi: Menetapkan Tujuan manajemen risiko.
Penilaian Risiko dan Ketidakpastian: Mengidentifikasi dan mengukur risiko.
Pengendalian Risiko: Mengendalikan risiko melalui diversifikasi, asuransi, hedging, penghindaran, dan lain-lain.

Pendanaan Risiko: Bagaimana membiayai manajemen risiko.
Administrasi program: Administrasi organisasi, seperti manual, dan sebagainya.
(Williams, Smith, Young, *Risk Management and Insurance*, McGraw Hill, 1998)

Enterprise Risk Management (ERM) adalah suatu proses, yang dipengaruhi oleh manajemen, board of directors, dan personel lain dari suatu organisasi, diterapkan dalam setting strategi, dan mencakup organisasi secara keseluruhan, didisain untuk mengidentifikasi kejadian potensial yang mempengaruhi suatu organisasi, mengelola risiko dalam toleransi suatu organisasi, untuk memberikan jaminan yang cukup pantas berkaitan dengan pencapaian tujuan organisasi. (COSO, *COSO Enterprise Risk Management – Integrated Framework.* COSO, 2004) .

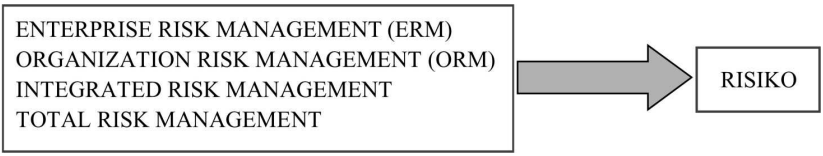
Selanjutnya COSO menampilkan format berikut ini yang menunjukkan bahwa ERM adalah manajemen risiko yang komprehensif (Lihat bagan berikut ini).



Gambar 1.4.
COSO – *Enterprise Risk Management*

Gambar 1.4 tersebut menunjukkan delapan komponen ERM yaitu (1) lingkungan internal, (2) penentuan tujuan, (3) Identifikasi kejadian, (4) Evaluasi (*assessment*) risiko, (5) Respons terhadap risiko, (6) Aktivitas pengendalian, (7) Informasi dan komunikasi, (8) Monitoring. Risiko yang dikelola mencakup risiko strategis, operasi, pelaporan, dan kepatuhan (*compliance*). Kemudian ERM mencakup keseluruhan organisasi, mulai dari level perusahaan keseluruhan (*entity level*), level divisi, level unit bisnis, dan level anak perusahaan (*subsidiary*).

Perhatikan bahwa definisi-definisi tersebut menggunakan istilah yang beragam untuk menjelaskan manajemen risiko organisasi, seperti terlihat pada bagan berikut ini.



Gambar 1.5.
Beberapa Istilah Manajemen Risiko Organisasi

Kemudian, ciri lain dari definisi tersebut adalah pengelolaan risiko yang komprehensif, dan bertujuan mencapai tujuan organisasi. Dengan menggabungkan beberapa karakteristik tersebut, bagan berikut ini menyajikan pengertian manajemen risiko suatu organisasi yang menjadi acuan modul ini.

Gambar 1.6.
Kerangka Manajemen Risiko Organisasi

Gambar 1.6 tersebut menunjukkan manajemen risiko organisasi (*enterprise risk management*) terdiri dari dua elemen besar: (1) Infrastruktur atau prasarana, yang terdiri dari prasarana lunak dan keras, dan (2) Proses Manajemen Risiko. Kemudian manajemen risiko organisasi bertujuan membantu pencapaian tujuan organisasi, dalam hal ini dirumuskan secara eksplisit menjadi memaksimumkan nilai perusahaan.

C. ELEMEN MANAJEMEN RISIKO ORGANISASI

Misalkan kita ditugaskan untuk membuat dan memimpin departemen manajemen risiko suatu perusahaan, bagaimana kita memulainya? Bagan di atas menunjukkan kerangka yang bisa digunakan untuk memulai membangun departemen manajemen risiko. Pertama, kita harus menyiapkan prasarana yang diperlukan untuk memulai pekerjaan manajemen risiko, yang meliputi prasarana lunak (non-fisik) dan prasarana keras (fisik).

1. Prasarana Manajemen Risiko

Salah satu hal yang penting dikerjakan untuk mempersiapkan manajemen risiko adalah menyiapkan prasarana yang mendukung manajemen risiko, yang meliputi prasarana lunak dan keras.

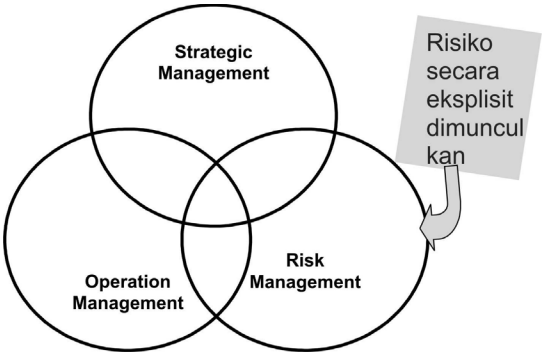
a. Prasarana lunak

Ada beberapa isu yang berkaitan dengan penyiapan prasarana lunak untuk manajemen risiko, yaitu: (1) Mengembangkan budaya sadar risiko untuk anggota organisasi, (2) Dukungan manajemen.

Mengembangkan Budaya Sadar Risiko. Tujuan dari budaya sadar risiko adalah agar setiap anggota organisasi sadar adanya risiko, dan mengambil keputusan tertentu dengan mempertimbangkan aspek risikonya. Dengan singkat, tujuan budaya sadar risiko adalah agar anggota lebih berhati-hati dalam pengambilan keputusan. Jika anggota tersebut sadar akan risiko, maka organisasi (yang terdiri dari kumpulan individu) akan menjadi lebih peka terhadap risiko.

Bagaimana mengembangkan perilaku yang sadar risiko untuk anggota organisasi? Salah satu cara yang bisa dilakukan adalah dengan memaksa mereka untuk berpikir risiko untuk setiap keputusan yang akan diambil. Pebisnis secara natural adalah orang yang optimis (karena itu mereka berani terjun ke dunia bisnis), dan cenderung melupakan aspek risiko (yang mendorong mereka untuk lebih berhati-hati). Jika dipaksa untuk berpikir mengenai risiko, maka mereka akan lebih seimbang dalam memutuskan sesuatu.

Sebagai contoh, bagan berikut ini menunjukkan tiga aspek yang harus dipikirkan oleh manajer dalam pengambilan keputusan, yaitu aspek strategis, operasi, dan risiko. Evaluasi terhadap risiko yang mungkin terjadi harus dipikirkan dan dilaporkan secara eksplisit.



Gambar 1.7.
Aspek Risiko Yang Dimunculkan Secara Eksplisit

Misalkan seorang manajer akan meluncurkan produk baru. Dia harus memikirkan tiga aspek yang disebutkan di atas, dengan pertanyaan seperti berikut ini.

1) Aspek Strategis: Apakah produk ini bisa memenuhi kebutuhan konsumen? Apakah produk ini bisa membantu pencapaian tujuan perusahaan (mencapai target keuntungan tertentu)?
2) Aspek Operasi: Bagaimana memproduksi produk ini? Apakah perusahaan mempunyai kemampuan memproduksi produk ini? Bagaimana memasarkan dan mengembangkan jaringan distribusi untuk produk ini?
3) Aspek Risiko: Risiko apa saja yang bisa muncul berkaitan dengan peluncuran produk ini? Bagaimana perusahaan bisa mengendalikan risiko-risiko tersebut?

Perhatikan pertanyaan aspek risiko secara eksplisit dimunculkan. Misalkan seorang manajer akan meluncurkan program promosi/iklan. Dia harus memikirkan tiga aspek yang disebutkan di atas, melalui pertanyaan-pertanyaan berikut ini.

1) Aspek Strategis: Bagaimana strategi promosi yang efektif? Bagaimana kontribusi promosi ini terhadap tujuan organisasi?
2) Aspek Operasi: Bagaimana menjalankan program promosi ini? Media apa yang paling efektif? Bagaimana *timing* (waktu yang tepat) untuk promosi ini? Bagaimana aspek detil lainnya dari promosi ini? Bagaimana

mengendalikan risiko-risiko yang barangkali muncul akibat peluncuran program promosi ini?

3) Aspek Risiko: Risiko apa yang potensial muncul akibat dari program promosi ini? Apakah promosi ini bisa menimbulkan gugatan hukum? Apakah promosi ini sudah etis? Pihak-pihak mana saja yang barangkali berkeberatan dengan promosi ini?

Perhatikan bahwa sama seperti sebelumnya, aspek risiko secara eksplisit perlu dipikirkan dan dimunculkan. Jika manajer terbiasa berpikir secara eksplisit mengenai risiko-risiko yang mungkin muncul, maka manajer tersebut akan semakin sadar terhadap risiko. Jika semua anggota organisasi sadar akan risiko, maka organisasi menjadi lebih sadar dan lebih peka terhadap risiko.

Mengembangkan kesadaran risiko juga bisa dilakukan melalui *workshop* atau pertemuan secara berkala antar manajer atau anggota organisasi. Agenda dalam *workshop* tersebut adalah membicarakan kejadian-kejadian yang bisa menimbulkan dampak yang negatif terhadap organisasi, alternatif-alternatif pemecahannya. *Workshop* tersebut bisa dikelola oleh manajer risiko perusahaan atau departemen risiko perusahaan. Melalui *workshop* atau pertemuan yang regular yang membicarakan risiko dengan segala aspeknya yang relevan, anggota organisasi diharapkan menjadi lebih sadar akan risiko yang dihadapi organisasi.

Teknik lain yang bisa digunakan adalah memasukkan risiko ke dalam elemen penilaian kinerja. Sebagai contoh, alokasi modal diberikan kepada usulan investasi yang memberikan *risk-adjusted return* (tingkat keuntungan setelah disesuaikan dengan risikonya) yang paling tinggi. Jika kriteria semacam itu yang akan dipakai, maka organisasi akan secara langsung 'menghukum' manajer yang berperilaku risiko tinggi. Risiko tinggi bisa dibenarkan sepanjang memberikan tingkat keuntungan yang diharapkan yang lebih tinggi juga. Dengan mekanisme evaluasi semacam itu, manajer diharapkan akan lebih sadar mengenai risiko, dan budaya risiko di organisasi akan menjadi semakin baik (semakin sadar akan risiko).

Dukungan Manajemen. Sama seperti program lainnya, dukungan manajemen khususnya manajemen puncak terhadap program manajemen risiko penting diberikan. Bentuk dukungan bisa eksplisit maupun implisit. Dukungan manajemen puncak bisa dituangkan antara lain ke dalam pernyataan tertulis, misal manajemen puncak mendukung atau ikut

merumuskan/menyetujui misi dan visi, prosedur dan kebijakan, yang berkaitan dengan manajemen risiko. Dukungan manajemen juga bisa ditunjukkan melalui partisipasi manajemen pada program-program manajemen risiko.

b. Prasarana keras

Di samping prasaran lunak, prasarana keras juga perlu disiapkan. Contoh prasarana keras yang perlu disiapkan adalah ruangan perkantoran, komputer, dan prasarana fisik lainnya. Prasarana fisik tersebut perlu dipersiapkan agar pekerjaan manajemen risiko berjalan sebagaimana mestinya.

2. Proses Manajemen Risiko

Elemen yang lebih penting lagi adalah proses manajemen risiko. Proses atau fungsi manajemen sering diterjemahkan ke dalam tiga langkah: perencanaan, pelaksanaan, dan pengendalian. Mengikuti kebiasaan tersebut, proses manajemen risiko juga bisa dibagi ke dalam tiga tahap yaitu perencanaan, pelaksanaan, dan pengendalian manajemen risiko.

a. Perencanaan

Perencanaan manajemen risiko bisa dimulai dengan menetapkan visi, misi, dan tujuan, yang berkaitan dengan manajemen risiko. Kemudian perencanaan manajemen risiko bisa diteruskan dengan penetapan target, kebijakan, dan prosedur yang berkaitan dengan manajemen risiko. Akan lebih baik lagi jika visi, misi, kebijakan, dan prosedur tersebut dituangkan secara tertulis. Dokumen tertulis semacam itu memudahkan pengarahan, sekaligus menegaskan dukungan manajemen terhadap program manajemen risiko.

Berikut ini beberapa contoh misi atau kebijakan dan prosedur yang berkaitan dengan manajemen risiko dari beberapa perusahaan/organisasi.

PERNYATAAN MISI MANAJEMEN RISIKO GOLDMAN SACH:
Misi dari departemen risiko adalah mengumpulkan, menganalisis, memonitor, dan mendistribusikan informasi yang berkaitan dengan risiko pasar dari posisi perusahaan supaya traders, manajer, dan personel lain dalam organisasi dan terutama komite risiko memahami dan membuat keputusan berdasarkan informasi (informed decisions) mengenai manajemen dan pengendalian risiko yang diambil.
(Goldman Sach adalah perusahaan sekuritas Amerika Serikat)

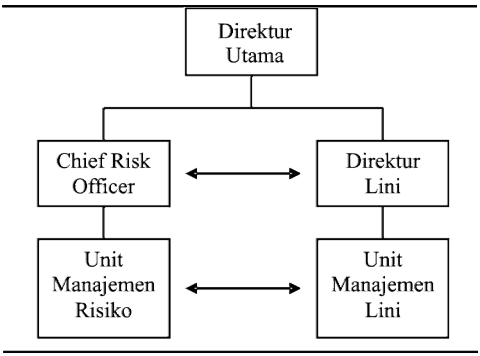
PERNYATAAN MISI SWISS BANK CORPORATION:
Pengendalian risiko Swiss Bank memfokuskan pada perlindungan terhadap modal dan memungkinkan pengambilan risiko yang sesuai. Kepentingan investor Swiss Bank adalah hal yang utama. Modal yang mereka investasikan harus dikompensasi untuk risiko yang ditanggung, baik untuk transaksi individual maupun portofolio.

Setelah misi dan kebijakan serta prosedur yang umum ditetapkan, langkah berikutnya adalah menyusun kebijakan serta prosedur yang lebih spesifik.

b. Pelaksanaan

Pelaksanaan manajemen risiko meliputi aktivitas operasional yang berkaitan dengan manajemen risiko. Proses identifikasi dan pengukuran risiko, kemudian diteruskan dengan manajemen (pengelolaan) risiko merupakan aktivitas operasional yang utama dari manajemen risiko. Identifikasi, pengukuran, dan manajemen risiko akan dibicarakan lebih detil di bagian dua, tiga, dan empat, dari modul ini. Bagian empat khusus membicarakan ilustrasi bagaimana perusahaan menerapkan manajemen risiko secara terencana dan sistematis di organisasinya.

Untuk melaksanakan pekerjaan manajemen risiko, diperlukan organisasi (struktur organisasi) dan *staffing* (personel). Struktur organisasi manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya. Berikut ini contoh struktur organisasi manajemen risiko.

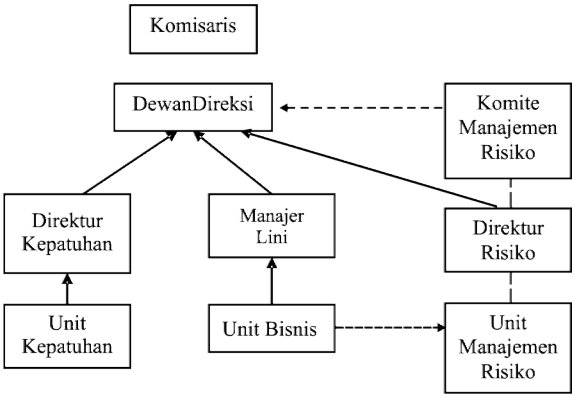


Gambar 1.8.
Struktur Organisasi Manajemen Risiko

Dalam Gambar 1.8 di atas, unit manajemen risiko bertanggung jawab ke manajer risiko yang disebut sebagai *chief risk officer* (CRO). CRO kemudian melapor (bertanggung jawab) langsung ke direktur utama. Pemisahan unit manajemen risiko menjadi bagian sendiri diharapkan mampu menjaga independensi unit manajemen risiko. Unit manajemen risiko mempunyai kedudukan yang sejajar dengan unit lini (pemasaran, keuangan, produksi). Status sebagai unit lini memungkinkan kekuatan yang cukup dalam organisasi untuk mendorong praktek manajemen risiko yang baik dalam suatu organisasi. Unit lini berkomunikasi dengan unit manajemen risiko (seperti ditunjukkan panah dua arah). Komunikasi semacam itu penting agar unit manajemen risiko memperoleh gambaran yang lengkap mengenai risiko yang dihadapi oleh perusahaan.

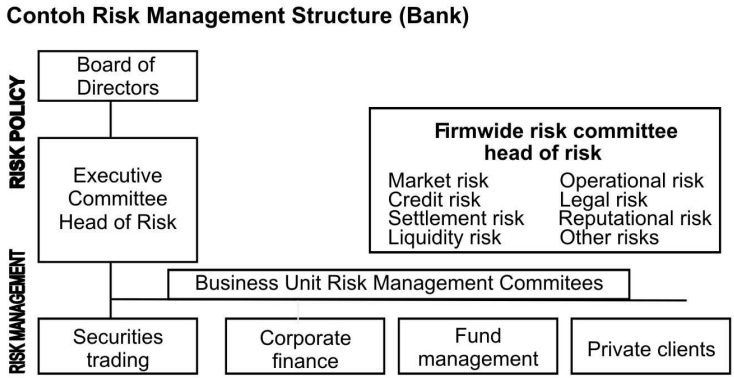
Aspek perilaku dari struktur organisasi manajemen risiko juga perlu diperhatikan. Pekerjaan manajemen risiko cenderung bertentangan dengan pekerjaan manajemen lini. Manajemen lini (misal pemasaran) ingin berjalan cepat tanpa memperhitungkan risiko. Manajemen risiko cenderung menahan keinginan semacam itu dengan mengingatkan risiko-risiko yang mungkin muncul. Struktur organisasi bisa diakomodasi untuk mengatasi potensi konflik semacam itu. Sebagai contoh, unit manajemen risiko bisa dibuat untuk melapor ke manajer risiko dan manajer lini sekaligus. Tetapi cara semacam itu barangkali tidak sempurna, karena pelaporan menjadi tidak jelas (ambigu). Contoh lain, unit manajemen risiko bertanggung jawab ke manajer lini dan memberikan laporan (hubungan garis terputus) kepada manajer risiko. Contoh lain adalah sebaliknya, unit lini bertanggung jawab ke manajer lini dan memberikan laporan ke manajer risiko. Contoh terakhir mirip seperti struktur organisasi pada bagan di atas.

Berikut ini dua contoh variasi dari struktur manajemen risiko.



Gambar 1.9.
Struktur Organisasi Manajemen Risiko Bank

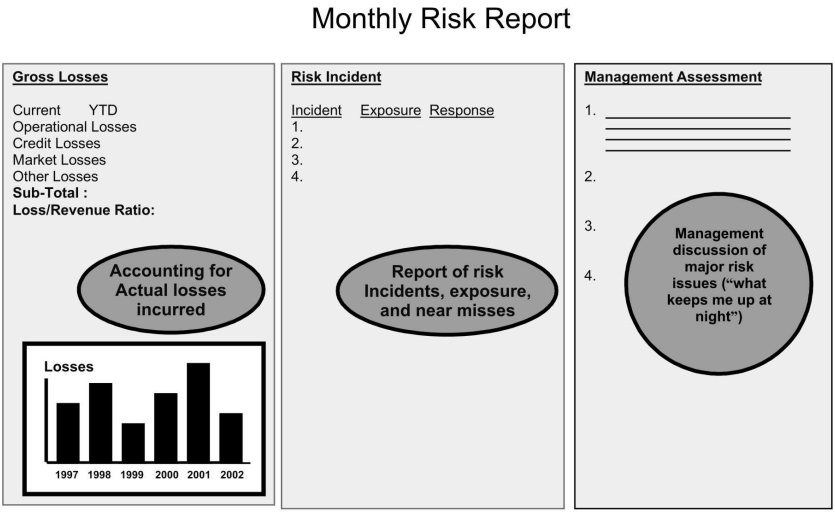
Pada struktur di atas, komite manajemen risiko mengawasi manajemen risiko organisasi. Direktur risiko mengelola kegiatan operasional manajemen risiko. Unit bisnis berkomunikasi dengan unit manajemen risiko untuk melaporkan hal-hal yang berkaitan dengan risiko organisasi. Direktur risiko mempunyai garis keanggotaan kepada komite manajemen risiko.



Gambar 1.10.
Struktur Organisasi Manajemen Risiko Bank (2)

c. Pengendalian

Tahap berikutnya dari proses manajemen risiko adalah pengendalian yang meliputi evaluasi secara periodik pelaksanaan manajemen risiko, output pelaporan yang dihasilkan oleh manajemen risiko, dan umpan balik (*feedback*). Format pelaporan manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya, dan dari satu kegiatan ke kegiatan lainnya. Sebagai contoh, bagan berikut ini menampilkan laporan profil risiko regular (misal bulanan).

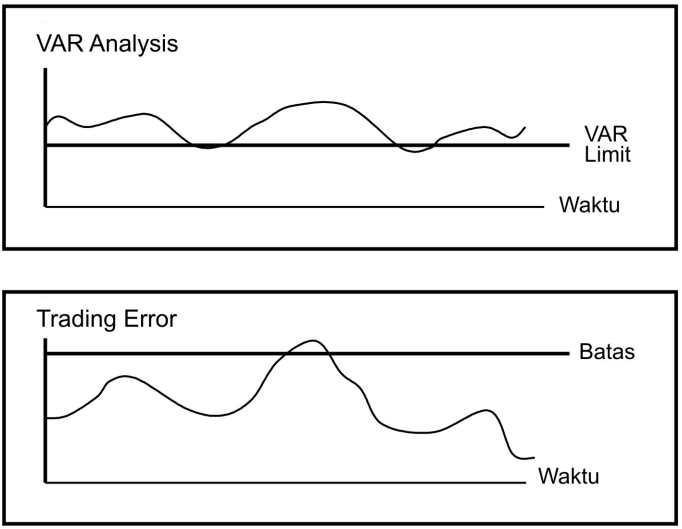


Gambar 1.11.
Contoh Laporan Risiko Bulanan

Gambar 1.11 tersebut menunjukkan laporan kerugian (keuntungan) di sebelah kiri. Gambar di tengah menunjukkan laporan mengenai kejadian-kejadian penting yang menyebabkan perusahaan mengalami kerugian, atau hampir rugi, eksposur perusahaan terhadap kejadian tersebut, dan respons yang dilakukan oleh organisasi. Sebagai contoh, perusahaan barangkali melaporkan kejadian naiknya tingkat bunga sebesar 1% (cukup tinggi). Kemudian perusahaan melaporkan eksposur yaitu posisi obligasi dengan nilai $10 juta (sepuluh juta dolar AS). Jika tingkat bunga naik, maka nilai obligasi akan turun (yang berarti perusahaan mengalami kerugian). Kolom berikutnya menyajikan respons yang dilakukan perusahaan dalam situasi tersebut (misal

melakukan *hedging*). Bagan paling kanan menunjukkan evaluasi dan diskusi oleh manajemen terhadap risiko-risiko utama yang dihadapi oleh perusahaan.

Unit manajemen risiko bisa juga menampilkan laporan berikut ini.



Gambar 1.12.
Contoh Laporan Risiko Untuk VAR dan *Trading Error*

Kedua bagan tersebut menunjukkan perkembangan VAR (*Value At Risk*, yang merupakan indikator risiko pasar) dan kesalahan perdagangan dari waktu ke waktu. Perusahaan juga menampilkan batas untuk masing-masing variabel risiko tersebut. Jika variabel risiko tersebut masih berada di bawah batas toleransi, maka risiko tersebut belum menunjukkan tingkat keseriusan yang tinggi. Tetapi jika variabel yang diamati tersebut bergerak melewati batas toleransi perusahaan, maka perusahaan harus lebih aktif untuk mengelola risiko tersebut.

Manajer risiko bisa juga menampilkan profil risiko untuk kegiatan tertentu. Sebagai contoh tabel berikut ini menunjukkan profil risiko untuk dua proyek A dan B. Risiko dilihat berdasarkan dimensi keuangan, sosial, dan politik.

Tabel 1.4.
Profil Risiko Usulan Investasi

	Keuangan	Sosial	Politik
Proyek A	1) Tinggi	3)Tinggi 4)Tinggi	5) Tinggi
Proyek B	1)Medium 2)Rendah	3)Medium 4)Rendah	5) Rendah

Keuangan: (1) Risiko kesulitan akses dana, (2) Risiko perubahan kurs
Sosial: (3) Penerimaan masyarakat sekitar, (4) Dukungan pemerintah lokal
Politik: (5) Stabilitas politik, (6) Perubahan Peraturan

Tabel 1.4 tersebut menunjukkan beberapa item risiko untuk keuangan, sosial, dan politik yang dievaluasi. Sebagai contoh, untuk keuangan ada dua item yang dievaluasi, yaitu risiko kesulitan akses dana dan risiko perubahan kurs. Proyek A tidak mempunyai risiko perubahan kurs karena lebih banyak beroperasi di pasar domestik. Dari tabel tersebut terlihat bahwa proyek A nampaknya mempunyai risiko yang lebih besar dibandingkan dengan proyek B. Semua item risiko untuk proyek A mempunyai penilaian risiko yang tinggi. Sedangkan untuk proyek B, kebanyakan item risiko dinilai medium atau rendah. Dengan demikian bisa diambil kesimpulan bahwa proyek A mempunyai risiko yang lebih tinggi dibandingkan dengan proyek B.

Jika pelaporan tersebut belum memuaskan (misal belum cukup informatif), maka format pelaporan bisa di rubah-rubah lagi. Proses umpan balik (*feedback*) harus dijamin bisa berjalan sebagaimana mestinya. Di samping itu hasil evaluasi dari manajemen risiko harus dikomunikasikan ke pihak-pihak yang berkepentingan dan relevan (*stakeholders*). Komunikasi yang baik menjamin disclosure dan transparansi yang baik, yang merupakan elemen manajemen risiko yang baik. Kasus Enron yang bangkrut pada tahun 2001 menunjukkan bahwa organisasi tersebut gagal membangun komunikasi dan transparansi yang baik. Manajemen risiko yang baik harus menjamin terjadinya good corporate governance, diantaranya terjaminnya disclosure dan transparansi yang baik.

Daftar Pustaka

Anderson, Sweeny, and Williams. (1999). *Statistics for Business and Economics*, South-Western Publishing, Cincinnati.

Barton, Thomas, William G. Shenkir, Paul L. Walker. (2002). *Making Enterprise Risk Management Pay Off.* New Jersey: Prentice Hall.

Boodie, Zvi and Robert C. Merton. (2000). *Finance.* New Jersey: Prentice Hall.

Doherty, Neil. (2000). *Integrated Risk Management.* New York: McGraw Hill.

Hanafi, Mamduh. (2005). *Manajemen Keuangan.* Yogyakarta: BPFE.

Hanafi, Mamduh. (2004). *Manajemen Keuangan Internasional.* Yogyakarta: BPFE.

Harrington, Scott E., dan Gregory R. Niehaus. (2003). *Risk Management and Insurance.* Boston: McGraw Hill.

Lam, James. (2004). *Enterprise Risk Management.* Wiley.

Marshall, John F., dan Vipul K. Bansal. (1992). *Financial Engineering, A Complete Guide to Financial Innovation.* New York: Institute of Finance.

Pande, Pete and Larry Holpp. (2002). *What is Six Sigma.* New York.

Risk Group (ed.). (2001). *Advances in Operational Risk.* London: Risk Water Group Ltd.

Saunders and Cornett. (2003). *Financial Institutions Management, A Risk Management Approach*, McGraw Hill.

SBC Warburg. (2004). *The Practice of Risk Management*, Euromoney Book.

Stulz, Rene M. (2003). *Risk Management and Derivatives.* Thomson-South Western.

Trieschmann, dan Gustavson. (1995). *Risk Management and Insurance*, South Western College Publishing.

Williams, C. Arthur, Michael Smith, and Peter C. Young. (1998). *Risk Management and Insurance*, Boston: McGraw Hill.

http ://www. wikip edia. corn.

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **DITA RAHMAWATI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa orang untuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci : *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak

sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada website Hyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang

memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

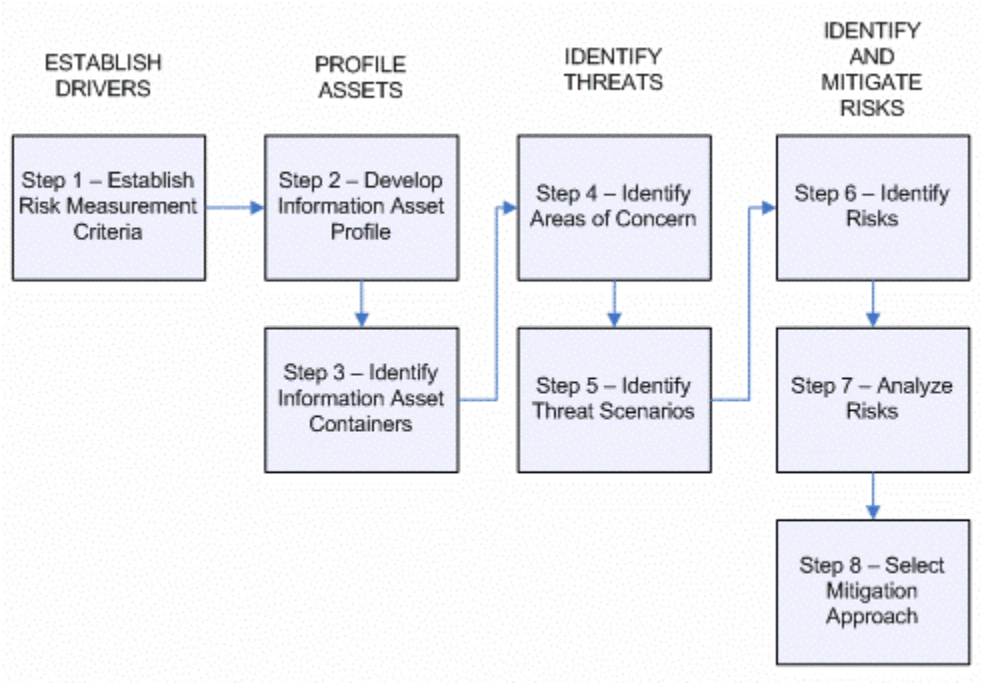
C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi. (Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset

informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang

mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	**Low**	**Medium**	**High**
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	**Impact Areas**
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting

dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang	

	mengkontak calon pelamar perusahaan tersebut dan data harus diamankan

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	Area of Concern
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user

	perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	Priority	Low (1)	Medium (2)	High (3)
Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	*Risk*			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**

POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1), 43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8 November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

PENILAIAN RISIKO KEAMANAN INFORMASI PADA PT XYZ DENGAN MENGGUNAKAN ISO 27001:2005

OLEH :

1. **DWI SEPTYA PUTRI**
2. **RIDUAN SYAHRI**
3. **RUMONDANG MARTHA A**
4. **TRI SUSANTI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Aset informasi memilki nilai tertentu bagi perusahaan sehingga harus dilindungi dari ancaman dan kerentanan keamanan informasi. Untuk pencegahan ancaman dan kerentanan keamanan informasi. Untuk itu, diperlukan penilaian risiko keamanan informasi terhadap aset informasi yang bertujuan untuk mengidentifikasi dan menilai risiko terkait keamanan aset informasi, serta memberikan rekomendasi perbaikan mengenai keamanan informasi yang harus diterapkan. PT XYZ memiliki aset informasi yang dikelola dan dilindungi terhadap ancaman dari pihak luar. Penilaian risiko dengan metode kuantitatif FMEA (*Failure Mode Effect Analysis*) untuk mengetahui nilai risiko berdasarkan tingkat kerentanan aset informasi pada PT XYZ, dan dengan pendekatan ISO 27001:2005 untuk menyesuaikan usulan kendali pengendalian dari risiko yang ditemukan berdasarkan aspek keamanan kerahasiaan, integritas, dan ketersediaan. Dengan begitu PT. XYZ mampu mengetahui nilai risiko dan risiko apa saja guna mencegah atau mengantisipasi risiko di masa yang akan datang.

Kata Kunci: aset informasi, penilaian risiko keamanan informasi, metode penilaian risiko FMEA (*Failure Mode Effect Analysis*), ISO 27001:2005

PENDAHULUAN

Data mempunyai peran yang sangat penting dalam sebuah sistem informasi karena merupakan salah satu komponen sistem informasi selain *software*, *hardware, people, procedures*, dan *networks* (Whitman dan Mattord, 2012). Oleh karena itu data yang disimpan dan diproses, kemudian disebarkan di dalam sistem komputer harus dilindungi keamanannya karena merupakan aset informasi yang paling berharga dalam sebuah perusahaan.

Pentingnya informasi membuat perusahaan perlu mengidentifikasi, mengukur, mengevaluasi, dan mengatur kegiatannya agar berfungsi dengan efektif. Sehingga tujuan dari penulisan paper ini adalah untuk mengidentifikasi dan menilai risiko pada aset informasi, agar dapat mengantisipasi, mencegah, dan membantu memperkirakan risiko apa saja yang berkemungkinan muncul terhadap kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya (Talabis & Martin, 2012).

Penilaian risiko keamanan informasi dilakukan dengan menggunakan pendekatan standar ISO 27001:2005. Karena ISO 27001:2005 merupakan standar yang sering digunakan untuk mengetahui kebutuhan untuk menerapkan keamanan sistem informasi (*IT Governance*, 2013). ISO 27001:2005 juga merupakan standar yang sangat fleksibel yang dikembangkan tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan jumlah pegawai dari struktur organisasi serta menyediakan sertifikat Sistem Manajemen Keamanan Informasi (SMKI) yang diakui internasional, disebut dengan Information Security Management System Certification (ISMSC) (Sarno & Iffano, 2009).

Selain itu penilaian risiko didukung juga dengan Metode FMEA (*Failure Mode & Effect Analysis*). Metode FMEA adalah suatu metodologi yang digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan nilai risiko dari kegagalan, dan skala prioritas untuk mengambil tindakan yang diperlukan. Di dalam FMEA juga terdapat pengendalian risiko menggunakan ISO terhadap keamanan informasi (Robin, Raymond , & Michael, 1996). Dengan demikian, penentuan level nilai risiko tersebut akan mempermudah dalam mendefinisikan aksi-aksi penanganan

risiko dengan tepat pada PT. XYZ. Metode FMEA juga dapat digunakan untuk menelusuri sumber-sumber penyebab dari suatu masalah (Lipol, 2011).

Berdasarkan dari permasalahan yang telah diuraikan di atas, maka tujuan dari penulisan paper adalah untuk melakukan analisis lebih lanjut di mana fokus utama dari penelitian yang akan dilakukan adalah mengidentifikasi dan memberikan penilaian risiko tiap-tiap aset informasi pada proses bisnis perkreditan mobil bekas di PT. XYZ.

PEMBAHASAN

A. PT. XYZ

PT. XYZ merupakan perusahaan yang bergerak di bidang pembiayaan sewa guna usaha, pembiayaan konsumen dan anjak piutang, yang memiilki beberapa cabang di Indonesia salah satunya di Palembang, dan memiliki kantor pusat yang berlokasi di Jakarta.

B. Penilaian risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, juga dikenal sebagai analisis risiko keamanan informasi, yaitu melibatkan identifikasi dan penilaian risiko terhadap kerahasiaan, integritas, dan ketersediaan sistem informasi dan sumber daya (Talabis & Martin, 2012). Hasil dari penilaian risiko adalah penentuan risiko, yaitu menentukan tingkat ancaman dan besar/kecilnya kemungkinan ancaman yang akan terjadi. Untuk mendukung komponen risiko, organisasi mengidentifikasi hal-hal sebagai berikut:

1. Ancaman terhadap organisasi (seperti operasi, aset, individu, atau ancaman yang langsung diarahkan organisasi terhadap organisasi lain.
2. Kerentanan internal atau eksternal organisasi.
3. Ancaman (yaitu, konsekuensi atau dampak) yang didapat dari ekspolitasi kelemahan sistem dalam organisasi.
4. Kemungkinan ancaman yang mungkin terjadi.
5. Bagaiaman penilaian risiko dilakukan dalam organisasi.
6. Frekuensi penilaian risiko.
7. Bagaimana ancaman diperoleh dari sumber atau metode. (National Institute of Standards and

Technology, 2011).

C. Identifikasi Risiko

Baik identifikasi maupun penilaian risiko merupakan rangkaian tahap dari manajemen risiko. Identifikasi risiko penting karena merupakan tahap pertama yang harus dilakukan karena dalam tahap ini dilakukan penentuan risiko – risiko beserta karakteristiknya yang mungkin akan mempengaruhi proyek.

D. Penilaian Risiko dengan FMEA

FMEA (*Failure Mode And Effects Analysis*) adalah metode yang akan digunakan untuk menilai dan menganalisis risiko secara kuantitatif. FMEA secara sistematis membantu untuk mengidentifikasi dan menilai pemicu (*modes*), probabilitas kejadian, dampak (*effects*) dari kegagalan dalam suatu sistem. Hasil analisis dan penilaian tersebut akan memberi peringkat dari setiap kegagalan sesuai dengan ketiga nilai tersebut.

a. Tingkat *severity*, yaitu suatu penilaian tingkat keparahan dari keseriusan *effect* yang ditimbulkan dari mode-mode kegagalan (*failure mode*), menghitung seberapa besar dampak/intensitas kejadian mempengaruhi output proses, maupun proses-proses selanjutnya.

b. Tingkat *occurrence*, yaitu suatu penilaian mengenai peluang (probabilitas) frekuensi penyebab mekanisme kegagalan yang akan terjadi, sehingga dapat menghasilkan bentuk/mode kegagalan yang memberikan akibat tertentu selama masa penggunaan produk.

c. Tingkat *detection*, yaitu pengukuran terhadap kemampuan mengendalikan/ mengontrol kegagalan yang dapat terjadi. (Robin, Raymond , & Michael, 1996.)

Langkah-langkah dalam metode FMEA dapat dilihat pada gambar 2.2 di bawah ini:

Gambar 1 FMEA *Cycle* (Steven C. Legget, 2001)

Secara keseluruhan prosesnya, metode FMEA terdiri dari 6 langkah berikut ini (Steven C. Legget, 2001):

Yang pertama kali dilakukan pada langkah pertama adalah mengidentifikasi potensial pemicu kegagalan teknologi informasi (Steven, 2001). Pada langkah kedua yaitu menentukan tingkat nilai keparahan (*severity number*) sesuai dengan rentang skala. Pada langkah ketiga yang dilakukkan adalah menentukan tingkat nilai probabilitas (*ocurrance number*) sesuai dengan rentang skala. Dan pada langkah keempat menentukan tingkat nilai kontrol risiko (*detection number*) sesuai dengan rentang skala. *Level* tingkat risiko dijelaskan pada tabel 1 di bawah ini:

Tabel 1. *Level* tingkat risiko FMEA

Level	Severity	Occurance	Detection
1	*None* (Tidak ada efek)	*Remote* (Lebih dari 5 tahun)	*Almost Certain* (Kontrol pasti dapat dan berhasil mencegah kegagalan)
2	*Very Minor*	*Very Low*	*Very High*

	(Sumber daya tersedia/ efek yang kecil terhadap proses)	(Setiap 3-5 tahun)	(Kemampuan kontrol dalam mencegah kegagalan adalah tinggi)
3	*Minor* (Sumber daya tersedia/ efek yang kecil terhadap prosedur)	*Low* (Setiap 1-3 tahun)	*High* (Kemampuan kontrol dalam mencegah kegagalan adalah tinggi)
4	*Very Low* (Sumber daya tersedia/ efek yng kecil terhadap kebijakan)	*Moderately Low* (Setiap Tahun)	*Moderately High* (Kemampuan kontrol dalam mencegah kegagalan cukup tinggi)
5	*Low* (Sumber daya tersedia/ efek yang besar terhadap proses)	*Moderate* (Setiap 6 bulan)	*Moderate* (Kemampuan kontrol dalam mencegah kegagalan adalah rendah)
6	*Moderate* (Sumber daya tersedia/ efek yang besar terhadap prosedur)	*Moderately High* (Setiap 3 bulan)	*Low* (Kemampuan Kontrol dalam mencegah kegagalan adalah rendah)
7	*High* (Sumber daya tersedia/ efek yang besar terhadap kebijakan)	*High* (Setiap bulan)	*Very Low* (Kemampuan kontrol dalam mencegah kegagalan adalah sangat rendah)
8	*Very High* (Sumber daya tidak tersedia/ kegagalan diketahui dan dapat dikontrol)	*High* (Setiap bulan)	*Remote* (Kecil kemungkinan kontrol dapat mencegah kegagalan)
9	*Extremly High* (Sumber daya tidak tersedia/ kegagalan diketahui namun tidak dapat dikontrol)	*Very High* (Setiap 3-4 hari)	*Very Remote* (Sangat kecil kemungkinan dapat mencegah kegagalan)
10	*Catastrophic* (Sumber daya tidak	*Extremely High*	*Absolute Uncertainly* (Kontrol tidak dapat

	tersedia/ kegagalan tidak diketahui)	(Setiap Hari)	mencegah kegagalan)

Setelah mengetahui *level* tingkat risiko, langkah selanjutnya adalah menentukan nilai RPN (*Risk Priority Number*). RPN merupakan nilai batasan yang menunjukkan risiko-risiko dengan nilai tertinggi. Nilai RPN diperoleh dengan mengalikan nilai tingkat keparahan efek (*severity*), nilai tingkat probabilitas (*occurrence*), dan nilai tingkat deteksi kontrol risiko (*detection*).

Menurut ISO 27001, maka nilai RPN dapat diperoleh dengan rumus :

RPN = S x O x D

Dimana:

S : *Severity Number* (Angka Tingkat Keparahan)

O : *Occurance Number* (Angka Tingkat Probabilitas Kejadian)

D : *Detection Number* (Angka Tingkat Deteksi Kontrol Risiko)

Setelah mengetahui nilai dari RPN, langkah terakhir adalah menentukan *Level* dari hasil RPN yang diperoleh, selanjutnya akan dilakukan penentuan *level* risiko, apakah risiko termasuk ke dalam golongan risiko dengan *level* tinggi, sedang, atau rendah. Penentuan *level* risiko didasarkan pada standar skala FMEA yang dapat dilihat pada tabel 2 berikut ini:

Tabel 2. Skala Nilai RPN FMEA

Skala Nilai RPN FMEA	
Skala Nilai RPN	**Level Risiko**
0-19	*Very Low*
20-79	*Low*
80-119	*Medium*
120-199	*High*
>200	*Very High*

E. ISO 27001:2005

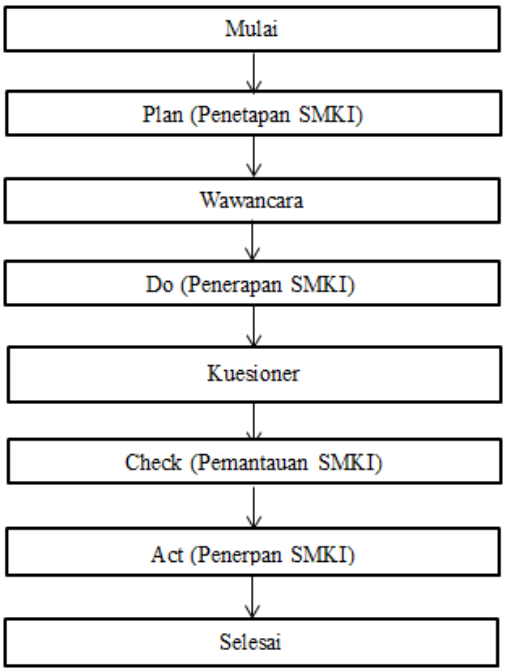
Standar ISO 27001:2005 ini sudah teruji dan direkomendasi oleh badan standar nasional Indonesia dan sudah diadopsi menjadi standar SNI ISO/IEC 27001:2009 "Teknologi informasi - Teknik keamanan - Sistem manajemen keamanan informasi - Persyaratan" disusun secara adopsi identik terhadap standar ISO/IEC 27001:2005, *Information technology - Security techniques - Information security management system - Requiretments*, dengan metode terjemahan oleh Panitia Teknis PK 03-02 Sistem Manajemen Mutu yang dibentuk BSN (SNI ISO/IEC, 2009).

Standar ISO 27001:2005 ini mengadopsi model "*Plan-Do_Check_Act*" (PDCA), yang diterapkan untuk membentuk seluruh proses SMKI. Konsep siklus PDAC ini pertama kali diperkenalkan oleh seorang ahli manajemen kualitas dari Amerika Serikat yang bernama Dr. William Edwards Deming.

a. *Plan* (penetapan SMKI) Menetapkan kebijakan prosedur SMKI yang sesuai untuk pengelolaan risiko dan perbaikan keamanan informasi agar menghasilkan hasil yang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.
b. *Do* (penerapan dan pengoperasian SMKI) Menerapkan dan mengoperasikan kebijakan, pengendalian, proses dan prosedur SMKI.
c. *Check* (pemantauan dan pengkajian SMKI) Mengases risiko (penilaian) dan, apabila berlaku, mengukur kinerja proses terhadap kebijakan, sasaran SMKI dan pengalaman praktis dan melaporkan hasilnya kepada manajemen untuk pengkajian.
d. *Act* (peningkatan dan pemeliharaan SMKI) Mengambil tindakan korektif dan pencegahan berdasarkan hasil SMKI dan tinjauan manajemen atau informasi terkait lainnya, untuk mencapai perbaikan berkesinambungan dalam SMKI.

F. Tahapan Penilaian Risiko

Tahapan-tahapan penilaian risiko diuraikan pada **Gambar 3** di bawah ini.



Gambar 3 Tahapan Penilaian Risiko

1. **Penetapan SMKI :**
   - Keamanan informasi di lakukan pada PT.XYZ. SMKI dilakukan terkait penilaian risiko pada proses perkreditan mobil bekas terhadap aset informasi.
2. **Penerapan SMKI:**
   - Pendekatan penilaian risiko menggunakan FMEA. FMEA digunakan untuk mengidentifikasi dan mengevaluasi kegagalan potensial, menentukan tingkatan nilai

risiko dari kegagalan, dan skala prioritas untuk mengambil tindakan yang diperlukan.

3. **Pemantauan SMKI** :

- Identifikasi Status Aset Pada Kelompok Aset Informasi

  Identifikasi status aset informasi terhadap kelompok aset informasi. Apakah Aset informasi yang terdapat pada PT. Clipan Finance Cabang Palembang pada proses perkreditan mobil bekas berstatus Utama atau Pusat.

- Analisis Aset Data Dan Informasi Kritis

  Pada tahap ini, penulis menganalisis dan membuat penetapan aset yang dinilai berdasarkan tingkat kritis terhadap kerentanan dan kekritisan data. Penulis meganalisis data yang paling kritis yang harus dilindungi keamananannya.

- Identifikasi Aspek Keamanan Aset Kritis

  Pada tahap ini, penulis akan mengidentifikasi kebutuhan aspek keamanan aset informasi terhadap CIA. Dimana C adalah *Confidentiality*, I adalah *Integrity*, A adalah *availability.* CIA merupakan prinsip-prinsip dasar yang digunakan dalam keamanan informasi.

- Identifikasi Potensial *Causes*

  Pada tahap ini, penulis melakukan identifikasi potensial causes, dimana penyebab dari timbulnya risiko yang terjadi dan didapatkan identifikasi kerentanan dan ancaman dari aset informasi perkreditan mobil bekas.

- Penilaian Risiko setiap aset informasi dengan metode FMEA

  Pada tahap ini, penulis melakukan penilaian risiko terhadap aset informasi dengan menggunakan FMEA. Identifikasi penilaian berdasarkan hasil RPN. Dimana RPN didapat dari hasil perkalian SxOxD.

- Hasil Analisis Penilaian Risiko

  Hasil analisis penilaian risiko didapat berdasarkan identifikasi aset yang terlibat, hasil kuesioner, status aset informasi, aspek keamanan informasi, identifikasi potensial *causes,* serta penilaian risiko dengan FMEA.

4. **Penerapan SMKI :**

- Rekomendasi Perbaikan Kendali Usulan Berdasarkan Klausul 27001:2005

  Rekomendasi perbaikan berisikan rekomendasi terhadap kondisi hasil penilaian risiko tiap-tiap aset informasi mengenai perkreditan mobil bekas didasari usulan kendali Standar ISO 27001:2005. Usulan kendali klausul dari klausul A5 sampai dengan A15 disesuaikan dengan kebutuhan dan hasil penilaian risiko terhadap rekomendasi perbaikan.

KESIMPULAN

Failure Mode and Effect Analysis (FMEA) merupakan salah satu teknik analisis kegagalan yang memiliki tujuan untuk mencermati proses maupun produk untuk mengetahui kemungkinan kegagalan yang terjadi dengan mengidentifikasi potensi kegagalan, akibat serta kemungkinan munculnya (Firdaus & Widianti, 2015). Dalam melakukan evaluasi kegagalan, FMEA menggunakan tiga indikator yaitu severity (S), occurence (O), dan detection (D). Setelah menentukan nilai ketiga indikator, selanjutnya yaitu menentukan nilai prioritas mode kegagalan berdasarkan nilai Risk Priority Number (RPN).

ISO 27001:2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan Sistem Manajemen Keamanan Informasi (SMKI). ISO 27001:2005 merupakan dokumen standar SMKI yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh suatu organisasi untuk bisa mengimplementasikan konsep-konsep keamanan informasi pada organisasi.

DAFTAR PUSTAKA

Badan Standardisasi Nasional Indonesia. SNI ISO/IEC 27001:2005.

Whitman, ME, Mattord, HJ. 2012. *Principes of Information Security*. Boston (US): Course Technology, Thomson.

Talabis, M., & Martin, J. (2012). *Information Security Risk Assessment: Risk Assessment. In Information Security Risk Assessment Toolkit* (pp. 147–175).http://doi.org/http://dx.doi.org/10.1016/B978-1-59-749735-0.00005-1

Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.

IT Governance. 2013. *Information Security & ISO 27001*. IT Governance Green Paper. United Kingdom.

Mcdermott, Robin E., Mikulak, Raymond J., Beauregard, Michael R. 1996. The Basic of FMEA. New York: 444 Park Avenue South, 7th floor.

L. S. Lipol. 2011. Risk Analysis Method: FMEA in the Organizations. International Journal of Basic & Applied Sciences IJBAS, vol XI, no 5, pp. 49-57.

IDENTIFIKASI DAN ANALISIS RESIKO KESELAMATAN DAN KESEHATAN KERJA PADA AREA PRODUKSI PT. PELITA CENGKARENG PAPER

Oleh :

Edi Supriyadi (182420058)

Dosen Pengampu : M. Izman Herdiansyah, M.M., Ph.D.

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

PT. Pelita Cengkareng Paper merupakan salah satu perusahaan industri daur ulang kertas di Cengkareng, Banten. Berdasarkan hasil observasi dan wawancara dengan bagian HSE mengenai kecelakaan kerja yang ada di PT. Pelita Cengkareng Paper, sebagian besar kecelakaan kerja terjadi di area produksi. Berdasarkan tingkat keparahan, kecelakaan tersebut dapat di kategorikan ke dalam kasus kecelakaan ringan, sedang, kritis dan fatal seperti pekerja jari terluka oleh benda tajam, lebam atau bengkak di kaki, tangan patah, dan kaki terpotong. Dari hasi observasi juga sangat memungkinkan pekerja mengalami gangguan pernafasan karena menghirup debu material. Berdasarkan kasus
– kasus tersebut, perlu adanya upaya identifikasi dan analisis risiko keselamatan dan kesehatan kerja yang terintegrasi ke dalam manajemen risiko yang dimulai dengan identifikasi risiko pada proses kerja operator sampai dengan menentukan tingkat risiko kecelakaan kerja dan menghubungkannya dengan fakta kecelakaan kerja dan penyakit akibat kerja yang pernah terjadi di PT. Pelita Cengkareng Paper. Sehingga secara mudah risiko dapat diminimalkan dengan menentukan pengendalian yang tepat. Identifikasi risiko menggunakan metode JHA(Job Hazard Analysis). Metode ini bertujuan mengetahui risiko yang ditimbulkan agar kemudian potensi kecelakaan dan penyakit akibat kerja dapat dikendalikan dengan menguraikan langkah-langkah pekerjaan. Penilaian risiko dilakukan dengan menggunakan standar manajemen risiko AS/NZS 4360:2004 metode semi kuantitatif W.T. Fine J dengan menganalisa nilai kemungkinan, pemajanan dan konsekuensi dari setiap potensi bahaya untuk mendapatkan tingkat risiko yang kemudian dibandingkan standar level risiko. Hasil penelitian menyatakan bahwa level risiko yang dimiliki pada aktivitas kerja di area produksi meliputi very high, substantial, priority 3, dan acceptable.

Kata kunci : Keselamatan dan Kesehatan Kerja, Semi Kuantitatif W.T. *Fine* J, *Job Hazard Analysis.*

ABSTRACT

PT. Pelita Cengkareng Paper is one of the paper recycling industry in Cengkareng, Banten. Based on observations and interviews with HSE about work accident in PT. Pelita Cengkareng Paper, the majority of work accidents occurred in the production area. Based on the severity, the crash can be categorized into the case of minor accidents, moderate, critical and fatal like the fingers of workers injured by sharp objects, bruising or swelling in the legs, broken hands, and feet cut off. From the observation is also very possible the workers suffered respiratory problems from inhaling dust material. Based on the cases, the need for measures for the identification and analysis of risks to safety and health are integrated into risk management starts with the identification of risks in the work process operator to determine the level of risk of occupational accidents and connect it to the facts of occupational accidents and occupational diseases that happened in PT. Pelita Cengkareng Paper. So easily risk can be minimized by determining the appropriate controls. Risk identification using JHA (Job Hazard Analysis). This method aims to determine the risks posed so that then the potential for accidents and occupational diseases can be controlled by outlining the steps work. The risk assessment carried out by using a risk management standard AS / NZS 4360: 2004 semi-quantitative method WT Fine J by analyzing possible value, exposure and consequences of any potential hazards to get the level of risk which is then compared to a standard level of risk. The study states that the level of risk of the activity of work in the production area includes very high, substantial, priority 3, and acceptable.

Keywords :
Occupational Health and Safety, Semi Quantitative WT Fine J, Job Hazard Analysis

I. PENDAHULUAN

Dalam menjalankan kegiatan produksi kearah yang lebih baik sebuah perusahaan tidak hanya dituntut untuk memfokuskan dirinya pada faktor mesin dan bahan baku saja, namun sumber daya manusia dalam hal ini keselamatan karyawan juga menjadi hal utama yang harus diperhatikan.

Selama bekerja para pekerja dihadapi oleh berbagai risiko yang memungkinkan terjadinya kecelakaan kerja. Faktor penyebab suatu kecelakaan dapat dikelompokkan menjadi dua kelompok menurut Santoso (2004). Pertama, kondisi berbahaya *(unsafe condition)*, yaitu yang tidak aman dari mesin, peralatan, bahan, dari lingkungan kerja, proses kerja, sifat pengerjaan dan cara kerja. Kedua, perbuatan berbahaya (*unsafe action)* yaitu perbuatan berbahaya dari manusia yang dapat terjadi karena kurangnya pengetahuan dan keterampilan, cacat tubuh yang tidak terlihat *(bodily defect)*, ketelitian dan kelemahan daya tahan tubuh, serta sikap dan perilaku kerja yang tidak baik.

Penerapan manajemen risiko yang terdiri dari identifikasi risiko lingkungan kerja dan pengukuran bahaya merupakan salah satu cara yang dapat dilakukan manajemen untuk memperkecil terjadinya risiko di tempat kerja. Jika seluruh risiko telah diidentifikasi, maka pengendalian untuk menghilangkan atau mengurangi bahaya-bahaya tersebut dapat diterapkan seperti diungkapkan oleh Landquist (2010) penilaian risiko diperlukan untuk memberikan dukungan keputusan dan remediasi tindakan sehingga memungkinkan penggunaan efisiensi sumber daya yang tersedia.

PT. Pelita Cengkareng Paper merupakan salah satu perusahaan manufaktur yang bergerak di bidang industri kertas yakni memanfaatkan proses daur ulang kertas sebagai bahan baku utama, terdiri dari dua bagian utama wilayah proses mesin kertas otomatis yaitu *Stock Preparation* (SP) dan *Paper Machine* (PM) yang menggunakan alat alat mesin silinder berputar dan mesin dengan ruang terbatas yang dapat menimbulkan adanya potensi bahaya yang tinggi. Kasus kecelakaan kerja selama tahun 2013 - 2014 yang pernah terjadi pada area produksi seperti Kejatuhan benda berat atau peralatan, menghirup debu, terkena atau tergores benda tajam, tertabrak alat transportasi, terciprat bahan cair keras dan *chemical,* terbentur peralatan atau mesin, terpeleset oleh lantai licin, dan terjepit peralatan atau mesin.

Dari beberapa kejadian kecelakaan tersebut, perlu upaya analisis risiko keselamatan dan kesehatan kerja yang terintegrasi kedalam manajemen risiko dimulai dengan tahap pertama identifikasi risiko menggunakan metode JHA *(Job Hazard Analysis*) dengan tujuan mendapatkan *risk event*. Menurut

Rausand (2005), *Job Hazard Analysis* digunakan pada tahap identifikasi risiko dengan menguraikan pekerjaan untuk mengetahui potensi bahaya apa saja yang terdapat pada pekerjaan sehingga dapat diketahui *risk event*. Tahap kedua, melakukan analisis risiko untuk menentukan besarnya suatu risiko menggunakan analisis Semi Kuantitatif, yakni metode *Fine*. Metode Wiliam T. Fine adalah salah satu metode analisis semi kuantitatif yaitu mengkalkulasikan risiko berdasarkan formula matematika. Metode ini terdiri dari tiga faktor utama yaitu *consequences, exposure*, dan *probability* yang telah ditentukan rating atau nilainya. Nilai dari ketiga faktor tersebut dikalikan untuk mengetahui tingkat risiko (Dickson, 2001). Tahap ketiga, evaluasi risiko dengan membandingan tingkat risiko yang telah dihitung dengan kriteria standar yang digunakan. Tahap terakhir adalah, pengendalian risiko menggunakan Hierarki pengendalian Bahaya dengan memberikan rekomendasi pengendalian untuk mencegah atau meminimasi bahaya yang terjadi berdasarkan tingkatan risiko yang sudah dianalisa dari evaluasi risiko.

II. METODOLOGI PENELITIAN

Tahapan awal dari penelitian ini adalah persiapan penelitian yang terdiri dari studi lapangan dan studi pustaka, perumusan masalah, penentuan tujuan penelitian, penetapan batasan masalah.

Untuk penelitian utama, tahapan yang peneliti lakukan adalah:

1. Objek Penelitian

Objek yang diteliti adalah bahaya dan risiko yang terdapat dalam proses produksi dari
bahan baku kertas sampai barang jadi yakni di area gudang bahan baku kertas dan bahan kimia, area mesin *stock preparations*, area mesin *paper machine* dan gudang *finished good*.

2. Mengumpulkan Data

Data yang dikumpulkan terdiri dari data primer (observasi terhadap peralatan yang digunakan, kondisi tempat kerja, tahapan proses yang dilakukan terkait dengan proses produksi dan wawancara kepada pihak-pihak terkait seperti, pihak SHE, kepala setiap departemen , pekerja pada area produksi) dan data sekunder (profil perusahaan, data kecelakaan, dan data pendukung lainnya).

3. Mengolah data

Data diolah menggunakan Risk Management AS/NZS 4360:2004 terdiri dari tahapan identifikasi risiko menggunakan *Job Hazard Analysis)*, analisis risiko Semi Kuantitatif metode *Fine,* ealuasi risiko, dan pengendalian risiko dengan *Hierarki Control*

4. Menganalisis Data

Penulis menganalisis hasil pengolahan data dari hasil identifikasi risiko, penilaian risiko dan pengendalian risiko.

5. Membuat kesimpulan dan Saran

Membuat kesimpulan berdasarkan tujuan penelitian dan memberikan saran untuk perbaikan sistem keselamatan dan kesehatan kerja di PT. Pelita Cengkareng Paper.

III. PEMBAHASAN

Identifikasi Risiko

Tahap ini bertujuan untuk mendapatkan *risk event*. Identifikasi risiko dilakukan dengan melakukan observasi pada pekerjaan yang dilakukan dalam setiap tahapan proses kerja dan melakukan wawancara terbuka terhadap pekerja yang melakukan pekerjaan, pengawas tiap area kerja, penanggung jawab area, staff HSE serta melihat dokumen perusahaan berupa catatan kecelakaan kerja. Dalam melakukan identifikasi risiko, penulis menggunakan metode *Job Hazard Analysis.*

Dalam penulisan jurnal ini, penulis hanya mengevaluasi dan mengidentifikasi area yaitu Area Gudang Bahan Baku Kertas dan Kimia. Aktivitas Pada Area Gudang Bahan Baku Kertas dan Kimia :

- **Memindahkan material dari truk ke gudang**

Langkah-langkah kerja pada aktivitas memindahkan material dari truk ke gudang :

1. Pekerja naik ke truk ke atas tumpukan material
2. Pekerja A mengangkat material dan diberikan kepada rekan kerja B yang ada di bawah
3. Pekerja A mengangkat material secara manual
4. Pekerja meletakkan material ke *material storage.*

Tabel 3.1 Tabel Identifikasi risiko memindahkan material dari truk ke gudang

No	Tahap Kegiatan	Identifikasi Bahaya	Risiko	Aktual	Pengendalia yang ada
1	Pekerja naik ke truk	Kejatuhan Material kertas karton	Cedera punggung		Tidak ada
		Menghirup debu material	Gangguan saluran pernafasan	Tidak menggun akan masker,	Tidak menyediaka n masker
2	Pekerja A mengangk at material dan	Kejatuhan material	Cedera punggung		Tidak ada
		Kejatuhan bahan kimia	Kulit melepuh	Tidak memakai baju kerja	Menyediaka n baju kerja

	diberikan kepada rekan kerja B yang ada di bawah	Menghirup debu material	Gangguan saluran pernafasan	Tidak menggun akan masker	Menyediaka n masker

Tabel 3. 1 Tabel Identifikasi risiko memindahkan material dari truk ke gudang (Lanjutan)

		Tergores sampah material yang tajam	Jari tangan terluka ringan	Tidak menggunakan sarung tangan	Menyediakan Sarung tangan
		Terjatuh dari atas tumpukan material	Kaki patah	Tidak menggunakan sepatu	Menyediakan sepatu
3	Pekerja mengangkat material secara manual	Kejatuhan Material kertas karton	Cedera punggung		Tidak ada
		Menghirup debu material	Gangguan saluran pernafasan	Tidak menggunakan masker	Menyediakan masker
4	Pekerja meletakkan *material* ke *storage*	Menghirup debu	Gangguan saluran pernafasan	Tidak menggunakan masker	Menyediakan masker
		Posisi membungkuk terjatuh material	Kaki cedera	Memakai sepatu	• Menyediakan sepatu

 Memindahkan material dari gudang ke *pulper*

Berikut langkah-langkah kerja pada aktivitas memindahkan material dari gudang ke *pulper*

1. Mengisi air radiator untuk *forklift*
2. Pekerja menaiki *forklift* (tidak terjadi kecelakaan kerja)
3. Pekerja mengangkut dan membawa material menuju *pulper* dengan bantuan *conveyor*.

Tabel 3.2 Tabel Identifikasi risiko memindahkan material dari gudang ke area *pulping*

No	Tahap Kegiatan	Identifikasi Bahaya	Risiko	Aktual	Pengendalian yang ada
1	Mengisi air radiator untuk *forklift*	Air radiator muncrat	Pundak depan dan dada melepuh	Memakai baju kerja	Menyediakan baju kerja
2	Pekerja mengangkut dan membawa material menuju *pulper* dengan bantuan *conveyor*	Tertabrak oleh forklift	Kaki patah	Menggunakan sepatu	Memiliki jasa sopir memiliki sertifikasi mengendarai *forklift*
		Terjatuh ketika membawa penumpang	Luka dalam bagian dada dan cidera kaki	Memakai sepatu dan baju kerja	• Menyediakan sepatu dan baju kerja • Larangan membawa penumpang

Analisis Risiko

Setelah mengidentifikasi risiko maka didapat *risk event* dari keadaan aktual di lapangan. Maka, selanjutnya dilakukan penilaian risiko dengan mengacu kepada analisis semi kuantitatif untuk mendapatkan nilai *probability, exposure* dan *consequences,* dimana nilai ketiga faktor sudah ditentukan menggunakan standar penilaian diadobsi dari AS/NZS 4360:2004.

Ketiga faktor akan dikalikan mendapatkan tingkat risiko. Untuk memastikan nilai *probability, exposure* dan *consequences* dapat diterima atau tidak, maka nilai ketiga faktor ditentukan berdasarkan wawacara dengan petugas HSE di PT. PCP.

Tabel 3.3 Tabel Analisis Risiko di Area Gudang Bahan Baku Kertas dan Bahan kimia

No	Identifikasi Bahaya	*P*	*E*	*C*	*Risk Rating* (R=PxExC)
1	Kejatuhan Material kertas karton	3	2	5	30
2	Menghirup debu material	3	10	15	450
3	Kejatuhan bahan kimia	3	0.5	15	22.5
4	Menghirup debu material	3	10	15	450
5	Tergores sampah material yang tajam	10	10	1	100
6	Terjatuh dari atas tumpukan material	3	2	5	30
7	Air radiator muncrat	3	2	5	30
8	Tertabrak oleh forklift	1	0.5	25	12.5
9	Terjatuh ketika membawa penumpang	3	0.5	15	22.5

Evaluasi Risiko

Evaluasi risiko adalah untuk menilai apakah risiko tersebut dapat diterima atau tidak dengan membandingkan terhadap stadar level risiko yang berlaku. Evaluasi risiko diperlukan sebagai landasan untuk melakukan pengendalian bahaya dan mengambil keputusan untuk sistem pengaman yang digunakan. Pada tahap ini, nilai risiko akan dibandingan dengan standar level risiko sesuai dengan standar manajemen AS/NZS 4360: 2004.

Dari identifikasi risiko yang dilakukan, potensi bahaya di area gudang dapat dikelompokkan menjadi 5 kategori potensi bahaya yaitu :

1) Kejatuhan material

Potensi bahaya kejatuhan material yang berisiko cedera punggung saat bongkar material, hal ini terjadi karena adanya faktor penyebab kondisi berbahaya (*unsafe condition*) yaitu keadaan tidak aman dari lingkungan kerja dimana tempat kerja kotor atau licin sehingga memungkinkan pekerja terpeleset. Sedangkan pada faktor penyebab tindakan bahaya (*unsafe action*) adalah suatu tindakan tidak aman dari manusia itu sendiri yaitu material yang diangkat terlalu berat, pekerja tidak menggunakan APD yang selayaknya dan sengaja melanggar peraturan keselamatan yang diwajibkan karena tidak mau repot dalam bekerja. Selain itu, pekerja kurang berhati- hati dan bermain-main saat bekerja.

Untuk itu dilakukan langkah pengendalian potensi bahaya, dimaksudkan supaya pekerja terhindar dari gangguan kesehatan atau penyakit dan kecelakaan akibat kerja. Berbagai cara yang dapat dilakukan dalam pengendalian potensi bahaya kejatuhan benda berat adalah :

- **Pengendalian Eliminasi** adalah teknik pengendalian menghilangkan peralatan yang dapat menimbulkan bahaya. Pengendalian ini dapat dilakukan dengan mengurangi berat beban material yang diangkat.

- **Pengendalian Subsitusi** merupakan usaha menurunkan tingkat risiko dengan menggantikan beberapa *hazard* dengan sumber lain yang memiliki potensi *hazard* yang lebih kecil. Pengendalian ini tidak dapat dilakukan, jikapun diganti dengan *forklift* tentu akan menghabiskan biaya yang banyak.
- **Pengendalian *Engineering*** tidak dapat dilakukan dengan mengubah desain tempat kerja, peralatan, atau proses kerja untuk mengurangi tingkat risiko.
- **Pengendalian Administrasi**, tahap ini menggunakan prosedur, standar operasi kerja atau panduan sebagai langkah mengurangi risiko. Pengendalian ini dapat dilakukan memberikan tabel JHA, SOP cara pengangkatan yang benar, SOP yang ada harus ditegaskan bagi setiap pekerja jika tidak maka diberikan sanksi secara lisan oleh manajemen atas, serta training peningkatan pengetahuan pekerja tentang K3, *Ergonomic dan manual lifting*.
- **Alat Pelindung Diri.** Diwajibkan untuk memakai baju kerja yang sudah disediakan.

2) Menghirup Debu Material

Potensi bahaya menghirup debu material terjadi karena bahan baku kertas bekas yang sudah tidak dipakai lagi (sampah) yang kotor diangkut dari supplier. Debu berbentuk butiran halus yang sagat mudah diterbangkan oleh angin. Risiko menghirup debu material ini terjadi karena adanya faktor penyebab kondisi berbahaya (*unsafe condition*) yaitu keadaan tidak aman dari lingkungan kerja dimana terdapat tempat kerja yang prosesnya mengeluarkan debu. Sedangkan pada faktor penyebab tindakan bahaya (*unsafe action*) adalah suatu tindakan tidak aman dari manusia itu sendiri yaitu pekerja tidak menggunakan masker dikarenakan tidak mau memakai alat pelindung diri yang disediakan dan sengaja melanggar peraturan keselamatan yang diwajibkan karena tidak mau repot dalam bekerja, orang terkadang tidak melakukan hal-hal yang mencerminkan tindakan yang selamat.

Maka, pengendalian bahaya untuk potensi bahaya menghirup debu di tempat kerja adalah sebagai berikut:

- **Pengendalian Eliminasi** tidak dapat dilakukan karena material yang digunakan adalah bahan baku dari kertas bekas dan mesin yang digunakan dirancang untuk mengolah kertas dalam proses produksi. Maka sangat kecil kemungkinan mengeliminasi proses tanpa mengganggu kelangsungan produksi secara keseluruhan.
- **Pengendalian Subsitusi**. Pengendalian ini tidak dapat dilakukan seperti pengendalian eliminasi dikarenakan dapat mengganggu kelangsungan produksi secara keseluruhan.

- **Pengendalian *Engineering*** tidak dapat dilakukan dengan memberikan *exhaust fan* karena area *material storage* berada di luar.
- **Pengendalian Administrasi** dapat dilakukan dengan mengusulkan tabel JHA (*Job Hazard analysis*) oleh penulis sebagai alat/ cara untuk mengidentifikasi bahaya kejadian yang tidak diinginkan terjadi. Pemeriksaan kesehatan secara berkala sangat bermanfaat untuk pekerja untuk mencegah penyakit yang lebih serius yang tentu saja jika hal itu terjadi dapat mengganggu kesehatan yang berakibat pada kurangnya kinerja pekerja dan bahkan dapat mempengengaruhi lingkungan menjadi tidak nyaman. Pengawasan APD sangat direkomedasikan karena pekerja sering lalai dalam penggunaan APD, beberapa pekerja merasa tidak membutuhkan APD atau merasa repot menggunakannya. Pengawasan ini harus bersifat tegas, jika memakai maka diberikan sanksi secara lisan. Oleh karena itu, supaya hal demikian tidak terjadi maka penngkatan pengetahuan pekerja tentang K3 juga sagat dibutuhkan, supaya pekerja benar-benar mengerti tentang K3, bagaimana mencegah dan menanggulangi bahaya.
- **Alat Pelindung Diri.** PT PCP seharusnya menyediakan dan menambah APD masker yang tepat

3) Terkena sampah material yang tajam

Risiko luka karena benda tajam ini terjadi dikarenakan adanya faktor penyebab kondisi bahaya (*unsafe condition)* keadaan tidak aman dari lingkungan kerja dikarenakan material merupakan sampah mentah yang belum dibersihkan dan terikut oleh benda-benda lain di dalamnya. Pada faktor penyebab tindakan bahaya (*unsafe action*) adalah suatu tindakan tidak aman dari manusia itu sendiri adalah seperti terburu- buru atau tergesa-gesa dalam melakukan pekerjaan dan tidak menggunakan APD sarung tangan karena tidak mau repot dalam bekerja.

Maka untuk mencegah adanya bahaya tergores oleh benda tajam dilakukan pengendalian risiko sebagai berikut :

- **Pengendalian Eliminasi** dapat dilakukan karena jika dihilangkan dapat mengganggu aktivitas yang terdapat di area itu dan berkemungkinan mengganggu proses produksi
- **Pengendalian Subsitusi** tidak dapat dilakukan karena akan merubah fungsi benda tersebut
- **Pengendalian *Engineering*** tidak dapat dilakukan dengan mengubah peralatan.
- **Pengendalian Administrasi** dapat dilakukan dengan cara inspeksi material sebelum material

diangkut ke perusahaan, setidaknya mengurangi benda-benda lain selain kertas.

- **Alat Pelindung Diri**. Disarankan menggunakan sarung tangan yang tepat.

4) **Tertabrak alat tranportasi *(Forklift)***

Potensi bahaya yang terjadi tabrakan baik dengan orang, objek, ataupun benda maupun kendaraan ketika sedang mengoperasikan kendaraan transportasi *forklift*. Risiko penyebab kecelakaan ini terjadi karena faktor penyebab kondisi berbahaya (*unsafe condition*) yaitu keadaan tidak aman dari lingkungan kerja, jika tempat kerja tidak memenuhi persyaratan yang telah ditentukan maka kecelakaan kerja sangat mungkin terjadi. Sebagai contoh, jalur yang kurang baik antara pengguna jalan kaki dengan jalur pengguna kendaraan dan kurangnya tanda-tanda peringatan yang terdapat di lingkungan kerja. Sedangkan faktor penyebab tindakan bahaya (*unsafe act)* yaitu tindakan tidak aman dari manusia itu sendiri sebagai contoh pekerja terburu- buru maupun tergesa-gesa dalam melakukan pekerjaan, kecepatan *forklift* dan suka bermain-main dalam bekerja menjadi salah satu penyebab terjadinya angka kecelakaan. Maka untuk mencegah adanya bahaya tergores oleh benda tajam dilakukan pengendalian risiko sebagai berikut :

- **Pengendalian Eliminasi** tidak dapat dilakukan karena jika *forklift* dihilangkan akan mengganggu aktivitas *material handling*.
- **Pengendalian *Engineering*** tidak dapat dilakukan dengan mengubah desain tempat kerja karena sudah memberikan desain jalan antara pengguna kendaraan *forklift* dan pengguna jalan kaki yaitu dengan memberikan pembatas warna kuning pada pejalan kaki dengan pengguna transportasi *forklift* hanya pembatas tersebut harus lebih diperjelas lagi agar dapat diperhatikan.
- **Pengendalian Adminitrasi** dapat dilakukan dengan menyediakan pengemudi *forklift* yang bersertifikasi artinya pengemudi tersebut sudah terampil dan memahami mengoperasikan *forklift.* Dalam pengendalian ini juga dapat dilakukan dengan menggunakan prosedur atau panduan sebagai langkah mengurangi risiko.
- **Alat Pelindung Diri** disarankan dengan menggunakan helm, sarung tangan dan sepatu untuk mengurangi risiko cidera ketika pengemudi mengoperasikan *forklift*.

5) Terciprat Air Radiator

Potensi bahaya terciprat air radiator yang berisiko bagian tubuh melepuh, hal ini terjadi karena adanya faktor penyebab tindakan bahaya (*unsafe action*) adalah suatu tindakan tidak aman dari manusia itu sendiri sebagai contohnya pekerja tidak menggunakan

APD yang selayaknya seperti baju kerja hanya memakai baju biasa dikarenakan tidak mau memakai alat pelindung diri yang disediakan dan sengaja melanggar peraturan keselamatan yang diwajibkan karena tidak mau repot dalam bekerja. Selain itu, pekerja kurang berhati- hati dan bermain-main saat bekerja.

Maka, cara yang dapat dilakukan dalam pengendalian potensi terciprat air radiator adalah :

- **Pengendalian Eliminasi** adalah tidak dapat dilakukan karena tidak mungkin menghilangkan air radiator pada *forklift* tentu saja akan mengganggu proses produksi.
- **Pengendalian Subsitusi** tidak dapat dilakukan karena air radiator pada *forklift* sebagai energi supaya *forklift* dapat beroperasi.
- **Pengendalian *Engineering*** tidak dapat dilakukan dengan mengubah peralatan atau proses kerja karena dapat mengganggu proses produksi.
- **Pengendalian Administrasi**, dapat dilakukan dengan pengawasan pemakaian APD dan pengawasan kerja supaya pekerja tidak bermain-main dan menggunakan APD demi keselamatan.
- **Alat Pelindung Diri** dilakukan dengan wajib menggunakan baju kerja yang tepat, sarung tangan, kacamata.

Pada umumnya kecelakaan kerja pada PT. Pelita Cengkareng Paper terjadi karena pekerja tidak memiliki sikap yang mencerminkan peduli akan keselamatan dan kesehatan kerja. Pekerja cenderung tidak mematuhi aturan, tidak berhati-hati dan bermain- main saat bekerja. Maka sebagai solusi, pekerja harus benar-benar sadar akan pentingnya keselamatan dan kesehatan kerja, memiliki sikap mental kepedulian akan keselamatan dan sikap mengindahkan peraturan yang ada. Jika tidak dilaksanakan, maka dapat mengambil langkah memberikan sanksi secara bertahap kepada pekerja yang tidak mematuhi aturan. PT.PCP memiliki semua alat pelindung diri kecuali kacamata. Maka sangat disarankan perusahaan dapat menyediakan kacamata untuk menghindari kecelakaan di bagian mata dan wajah. Akan tetapi, alat pelindung diri yang ada seperti baju kerja dan masker belum memenuhi kriteria alat pelindung diri yang baik apalagi dengan lantai produksi yang sangat panas. Maka, disarankan PT.PCP menyediakan masker dan baju kerja yang tepat yang dapat mengurangi dan bahkan mencegah adanya risiko kerja.

IV. KESIMPULAN DAN SARAN

Kesimpulan

Berdasarkan analisis penelitian yang telah dilakukan, didapatkan kesimpulan sebagai berikut :

1. Berdasarkan aktivitas-aktivitas kerja yang berpotensi menimbulkan bahaya pada area gudang yakni gudang bahan baku kertas dan bahan baku kimia dilakukan penjabaran proses kerja didalam area tersebut menjadi langkah-langkah yang kemudian akan diketahui *risk event* atau kejadian yang berisiko pada keselamatan dan kesehatan kerja. *Risk event* yang diketahui dapat dikelompokkan menjadi 5 kategori potensi bahaya, potensi bahaya tersebut yaitu : Kejatuhan materal, menghirup debu, terkena atau tergores benda tajam, tertabrak alat transportasi, dan air radiator.
2. Pada area gudang bahan baku kertas dan bahan kimia *risk rating* tertinggi adalah menghirup debu yang dapat menyebabkan gangguan saluran pernafasan yaitu bernilai 450 begitu juga dengan gudang bahan kimia.

   Level risiko tertinggi adalah termasuk kedalam kategori *priority 3*, artinya risiko yang ada perlu dilakukan pengawasan dan diperhatikan secara berkesinambungan. Di posisi kedua adalah *substantial* artinya bahwa risiko yang ada diharuskan perbaikan secara teknis. Ketiga, level risiko *Acceptable* artinya risiko yang terjadi dikurangi seminimal mungkin dan terakhir adalah *Very High* artinya mengharuskan penghentian aktivitas atau risiko dikurangi hingga mencapai batas yang dapat diterima.
3. Setelah dilakukan penilaian risiko, tahap terakhir yang harus dilakukan adalah pengendalian risiko sebagai rekomendasi pengendalian bahaya oleh penulis. Pengendalian risiko berdasarkan kategori potensi bahaya:

- Kejatuhan material dapat dilakukan dengan pengendalian eliminasi yakni mengurangi beban material yang diangkat. Pengendalian administrasi dengan memberikan tabel JHA, SOP cara pengangkatan yang benar dan peningkatan pengetahuan pekerja tentang K3, *Ergonomic dan manual lifting*. Untuk alat pelindung diri dapat menambah APD helm, sepatu dan baju kerja.
- Menghirup debu, dapat dilakukan dengan pengendalian administrasi dengan memberikan tabel JHA, pemeriksaan kesehatan pekerja secara berkala, pengawasan APD, training pengetahuan pekerja tentang K3. Untuk alat pelindung diri dapat menambah APD masker yang tepat.
- Terkena atau tergores benda tajam, dapat dilakukan dengan pengendalian administrasi dengan inspeksi material dari supplier sebelum sampai ke

perusahaan. Untuk APD dengan menambah sarung tangan.

- Tertabrak alat transportasi *forklift* dapat dilakukan dengan pengendalian administrasi yaitu dengan menyediakan pengemudi *forklift* yang bersertifikasi Untuk APD diwajibkan memakai sepatu yang disediakan.
- Terciprat air radiator dapat dilakukan dengan pengendalian administrasi yaitu dengan pengawasan pemakaian APD dan pengawasan kerja. Untuk APD dengan menambah baju kerja, sarung tangan, kacamata dan sepatu.

Saran

Saran berikut ini dibuat berdasarkan penelitian dan pengamatan yang dilakukan selama kegiatan penelitian dan berdasarkan teori atau pemahaman yang diketahui oleh penulis, antara lain :

1. Lanjutkan *follow up* penelitian mengenai penilaian risiko yang penulis lakukan dan terapkan kegiatan penilaian risiko secara berkala
2. Lakukan pemasangan *safety sign* di berbagai tempat strategis yang mudah terlihat dan terbaca pada masing-masing area. *Safety sign* sebaiknya dibuat dengan ukuran besar dan dapat memantulkan cahaya sehingga dapat terbaca pada malam hari.
3. Pemberian pelatihan kepada pekerja untuk mengenali potensi bahaya dan risiko di tempat kerja serta bagaimana cara untuk mencegah dan menanggulangi bahaya tersebut.
4. Melakukan sosialisasi secara rutin mengenai K3 terutama mengenai potensi bahaya dan risiko yang ada di tempat kerja. Sosialisasi dapat dilakukan dalam bentuk *safety briefing.*
5. Penempatan pekerja yang berkompetensi pada bidang pekerjaan yang memiliki potensi risiko tinggi dan memastikan bahwa pekerja mampu dan mengetahui pekerjaan yang mereka lakukan.
6. Mengadakan pemeriksaan kesehatan karyawan secara berkala
7. Menyediakan air minum dan memberika himbauan kepada pekerja untuk banyak minum, karena kondisi lingkungan kerja yang lumayan panas.

V. DAFTAR PUSTAKA

Australian/ New Zealand Standard. *2004. Australian Standad/New Zealand Standar 4360:2004"Risk Management"*.

Dickson, T. 2001. *Calculating Risk: Fine's Mathematical Formula 30 Years Later*. Australian Journal of Outdoor Education.

Landquist, H. 2013. *Evaluating the needs of risk assessment methods of potentially polluting shipwrecks.* Department of Shipping and Marine

PENILAIAN RISIKO KERJA PADA PROSES PRODUKSI

Ahkmad Ipandy[1], Erin Efriansyah[2], Fero Triando[3], Tri Akhyari Romadhon[4]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Penilisan ini dilakukan karena ditemukan berbagai bahaya dan risiko pada pekerja di bagian proses produksi. Penelitian ini bertujuan untuk mengetahui besaran risiko keselamatan dan kesehatan kerja pada pekerja di bagian proses produksi *spin pack*. Hasil telitian menunjukkan bahwa pada *basic risk* terdapat 6 aktivitas yang termasuk dalam level *very high*. Pada *existing risk*, terdapat 2 aktivitas dengan risiko tinggi yang termasuk dalam level *priority 1*, yaitu pada proses pencetakan dan proses *pressing* produk yang menggunakan mesin *press*. Dalam penelitian ini juga diberikan *predictive risk* dengan rekomendasi pengendalian, sehingga risiko-risiko yang ada dapat diturunkan sampai pada level *acceptable*.

Kata kunci: Penilaian risiko, resiko kerja , proses produksi

1. PENDAHULUAN

Keselamatan dan kesehatan kerja (K3) merupakan promosi dan pemeliharaan tertinggi tingkat fisik, mental dan kesejahteraan sosial dari semua pekerjaan, pencegahan efek kesehatan yang disebabkan oleh kondisi kerja pekerja, perlindungan bagi pekerja dari resiko akibat faktor yang merugikan bagi kesehatan, menempatkan dan pemeliharaan pekerja dalam lingkungan kerja disesuaikan pada fisiologis dan psikologis dan untuk meringkas adaptasi bekerja untuk manusia dan masing-masing pekerjaannya (*ILO/WHO Join and Health Committee, 1950*). Berdasarkan definisi tersebut dapat dikatakan bahwa K3 merupakan salah satu faktor yang paling penting dan sangat dibutuhkan untuk menjamin keselamatan hidup manusia.

Kecelakaan merupakan sebuah kejadian tak terduga yang menyebabkan cedera atau kerusakan (Ridley, 2004). Kecelakaan akibat kerja adalah kecelakaan yang berkaitan dengan hubungan kerja dengan perusahaan. Hubungan kerja disini dapat berarti bahwa kecelakaan dapat terjadi dikarenakan oleh pekerjaan atau pada waktu melakukan pekerjaan (Suma'mur, 1989). Dalam hal ini kita dapat melihat bahwa kecelakaan adalah salah satu risiko yang cukup besar karena menyebabkan cedera dan kerugian yang dapat terjadi kapan saja terutama bagi pekerja.

Setiap tahunnya di dunia terjadi sekitar 340 juta kecelakaan kerja dan 160 juta korban penyakit akibat kerja (ILO, 2011). Angka ini menunjukkan bahwa kecelakaan kerja masih tergolong tinggi dan butuh tindakan pencegahan sesegera mungkin agar angka tersebut tidak

terus bertambah. Di Indonesia pun, angka kecelakaan kerja masih terus meningkat dari tahun ke tahun. Ini terbukti dari data Jamsostek selama 5 tahun terakhir. Berikut data Jamsostek mengenai angka kecelakaan kerja di Indonesia dalam kurun waktu 5 tahun terakhir.

Table 1. Angka Kecelakaan Kerja dan Klaim Kecelakaan Tahun 2008-2012

Tahun	Angka Kecelakaan Kerja (kasus)	Klaim Kecelakaan Kerja (rupiah)
2012	103.000	646,2 milyar
2011	99.491	504 milyar
2010	98.711	401,2 milyar
2009	96.314	328,5 milyar
2008	94.763	297,9 milyar

Sumber: Jamsostek

Berdasarkan data diatas kita dapat melihat bahwa angka kecelakaan kerja di Indonesia terus meningkat setiap tahunnya. Hal ini tentu menunjukkan bahwa masih lemahnya sistem keselamatan dan kesehatan kerja untuk melindungi pekerja-pekerja di Indonesia. Jika kondisi ini tidak segera ditangani, maka pengingkatan jumlah kecelakaan kerja akan cenderung untuk terjadi di tahun-tahun yang akan datang. Menurut Suma'mur (1989), kecelakaan menyebabkan lima kerugian yaitu kerusakan, kekacauan organisasi, keluhan dan kesedihan, kelainan dan cacat serta kematian.

Disamping kerugian-kerugian tersebut, perusahaan juga harus menanggung biaya-biaya lainnya yang timbul dari kecelakaan tersebut. Salah satunya adalah biaya klaim asuransi kecelakaan kerja. Berdasarkan tabel 1.1 dapat dilihat bahwa peningkatan angka kecelakaan tentunya juga diiringi dengan peningkatan klaim asuransi untuk pekerja yang mengalami kecelakaan. Selain itu perusahaan juga diharuskan untuk memberikan ganti rugi atau kompensasi kepada pekerja yang mengalami kecelakaan pada saat bekerja atau di tempat kerja. Hal ini telah diatur dalam Undang-Undang No. 34 tahun 1947 Tentang Kecelakaan Kerja dan Undang-Undang No.2 tahun 1992 tentang Jaminan Sosial Tenaga Kerja. Biaya-biaya tersebutlah yang harus ditanggung oleh perusahaan jika kecelakaan kerja masih terus terjadi.

Selain banyaknya biaya yang harus dikeluarkan perusahaan untuk kompensasi dan mengganti kerugian, kecelakaan kerja juga menyebabkan perusahaan akan dirugikan oleh hilangnya hari kerja dan menurunnya produktivitas pekerja. Jika kasus kecelakaan terus bertambah dari waktu ke waktu dapat memberikan citra buruk bagi perusahaan karena tidak

dapat menjamin keselamatan pekerjanya.

Salah satu aspek penting yang harus diperhatikan perusahaan untuk meminimalisir terjadinya kecelakaan adalah dengan melakukan manajemen risiko. Menurut AS/NZS 4360, Manajemen Risiko adalah "*the culture, process and structures that are directed towards the effective management of potential opportunities and adverse effect*". Manajemen risiko menyangkut budaya, proses dan struktur dalam mengelola suatu risiko secara efektif dan terencana dalam suatu sistem manajemen yang baik (Ramli, 2010).

Manajemen risiko tidak terlepas dari berbagai risiko-risiko K3 yang dapat timbul dari setiap kegiatan di tempat kerja. Menurut OHSAS 18001, risiko K3 adalah kombinasi dari kemungkinan terjadinya kejadian berbahaya atau paparan dengan keparahan dari cedera atau gangguan kesehatan yang disebabkan oleh kejadian atau paparan tersebut (Ramli, 2010).

Maka secara sederhana dapat dikatakan bahwa manajemen risiko merupakan proses untuk mengelola risiko yang ada dalam setiap kegiatan (Ramli, 2010).

Manajemen pengelolaan risiko dilakukan dengan sebuah prinsip utama yang disebut *Calculated Risk* atau risiko yang diperhitungkan (Ramli, 2010). *Calculated risk* dilakukan untuk mengetahui seberapa besar tingkat risiko terhadap suatu *task* atau kegiatan yang dilakukan pekerja di tempat kerja. Apabila sebuah pekerjaan telah diketahui tingkat risikonya, maka akan dapat dilakukan pengendalian risiko terhadap pekerjaan tersebut sebelum terjadi kecelakaan. Hal ini tentu akan sangat bermanfaat bagi perusahaan untuk mencegah berbagai kerugian yang mungkin terjadi apabila risiko tersebut tidak segera dikelola dan dikendalikan.

Manajemen risiko meliputi identifikasi bahaya dan risiko, analisis dan penilaian risiko dan evaluasi risiko serta tindakan pengendalian yang dilakukan selama proses kerja berlangsung. Apabila aspek-aspek dalam manajemen risiko ini tidak diperhatikan dan dikelola dengan baik maka akan menimbulkan kerugian bagi perusahaan. Tidak hanya kecelakaan pada pekerja, namun dampak lainnya dapat berpengaruh pada kerugian finansial yang harus ditanggung oleh perusahaan serta kerugian yang harus diterima perusahaan akibat citra buruk yang ditimbulkan karena tidak melaksanakan manajemen risiko dengan baik. Oleh karena itu, perusahaan perlu melaksanakan manajemen risiko dengan baik khususnya dalam mengidentifikasi bahaya dan risiko serta melakukan penilaian risiko untuk dapat menentukan pengendalian yang dapat dilakukan sehingga dapat mencegah dan mengurangi kerugian (*loss*) yang dapat timbul.

Prinsip manajemen risiko berupa penilaian risiko tentu harus diterapkan oleh seluruh

industri maupun perusahaan. Terutama bagi perusahaan-perusahaan atau industri yang mempunyai tingkat risiko K3 yang tinggi dalam proses kerjanya. Salah satu perusahaan dengan tingkat risiko K3 yang cukup tinggi adalah PT BAF. PT BAF merupakan perusahaan manufaktur yang bergerak dalam bidang produksi filter. Salah satu filter yang diproduksi oleh PT BAF adalah filter yang digunakan untuk memisahkan uap maupun gas pada industri-industri kimia. Selain itu PT BAF juga memproduksi filter untuk gas panas yang digunakan pada industri pertambangan serta masih banyak jenis filter yang telah diproduksi oleh PT BAF. Namun dari semua filter yang diproduksi, produksi paling banyak dan yang paling rutin dilakukan oleh PT BAF adalah pembuatan *screen filter* atau sering disebut *spin pack*. *Spin pack* terbuat dari bahan dasar logam, alumunium atau *wire mesh* yang diproduksi berdasarkan pesanan dari berbagai industri sesuai dengan kebutuhannya masing-masing. Pembuatan *spin pack* baik yang berbahan dasar logam, alumunium maupun *wire mesh*, tentu membutuhkan proses dan rangkaian kerja yang cukup kompleks. Proses kerja yang kompleks dan rumit serta menggunakan alat-alat dan mesin mekanis tentunya akan menimbulkan risiko kecelakaan yang cukup besar bagi pekerja. Oleh karena itu perlu dilakukan analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF untuk mengetahui tingkat risiko yang ada serta rekomendasi pengendalian yang dapat dilakukan guna mencegah dan meminimalisir terjadinya kecelakaan. Adapun tujuan dari penelitian ini adalah:

1. Tujuan Umum

   Untuk memperoleh gambaran mengenai analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF tahun 2013
2. Tujuan Khusus
   1. Mengetahui proses atau tahapan kerja apa saja yang terdapat pada proses produksi *spin pack* di PT BAF.
   2. Mengetahui bahaya yang terdapat pada tahapan kerja pada proses produksi *spin pack* di PT BAF.
   3. Mengetahui nilai *consequence, likelihood, exposure* dan *basic risk* dari risiko-risiko K3 tanpa mempertimbangkan pengendalian yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   4. Mengetahui pengendalian risiko K3 yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   5. Mengetahui nilai *consequence, likelihood, exposure* dan *existing risk* dari risiko-risiko K3 dengan mempertimbangkan pengendalian yang sudah dilakukan pada

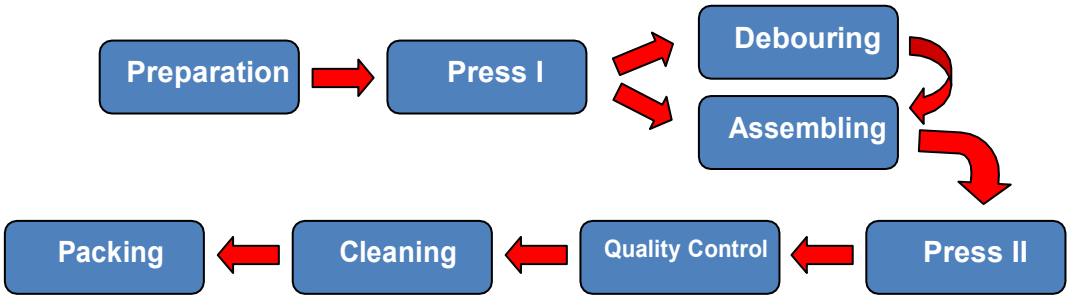
proses produksi *spin pack* di PT BAF.

6. Mengetahui nilai dari *risk reduction* pada proses produksi *spin pack* di PT BAF.
7. Mengetahui rekomendasi pengendalian yang masih memungkinkan dapat dilakukan untuk menurunkan risiko saat ini (*existing risk*) pada proses produksi *spin pack* di PT BAF.
8. Mengetahui nilai risiko prediksi (*predictive risk*) setelah ada rekomendasi pengendalian pada proses produksi *spin pack* di PT BAF.

2. HASIL PENELITIAN DAN PEMBAHASAN

2.1 Identifikasi Hazard dan Risiko

Tahap-tahap proses produksi *Spin Pack*



Gambar 1. Alur Proses Produksi *Spin Pack*

Identifikasi *hazard* dan risiko pada kegiatan proses produksi *spin pack* dilakukan dengan menggunakan *job hazard analysis* (JHA). JHA dibuat berdasarkan jenis pekerjaan dan bagiannya masing-masing. Tujuannya agar diketahui dengan jelas bahaya dan risiko disetiap masing-masing bagian.

1. Hazard dan Risiko pada Bagian *Preparation*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *preparation*, yaitu :

1. *Hazard* Mekanik : Sepihan material, mesin pemotong dan mesin perata.
   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk seprihan material, terjepit mesin calendaring, terpotong mesin pemotong material.
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban (material)

2. Hazard dan Risiko pada Bagian *Press I*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *press I*, yaitu:

1. *Hazard* Mekanik

   Risiko yang dapat ditimbulkan berupa terjepit dan tertimpa tooling, terpukul benda keras saat memasang tooling, terpotong mesin press, tergores dan tertusuk material

2. *Hazard* Fisik : Panas, bising, pencahayaan kurang baik, serpihan material.

   Risiko yang dapat ditimbulkan berupa ketidaknyamanan, kurangnya konsentrasi, kelelahan mata karena pencahayaan yang kurang baik, dan terkena percikan serpihan material. *azard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive*

   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

3. Hazard dan Risiko pada Bagian *Debouring*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *debouring*, yaitu :

1. *Hazard* Mekanik : serpihan material

   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk serpihan material

2. *Hazard* Fisik : Bising

   Risiko yang dapat ditimbulkan berupa ketdaknyamanan, kurangnya konsentrasi dan penurunan fungsi pendegaran.

3. *Hazard* Ergonomi : Postur janggal saat membawa beban

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban.

4. Hazard dan Risiko pada Bagian *Assembling*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *assembling*, yaitu :

1. *Hazard* Mekanik : produk dari logam bersisi tajam

   Risiko yang dapat ditimbulkan berupa tersayat produk

2. *Hazard* Ergonomi : Postur janggal saat membawa beban dan saat duduk terlalu lama.

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban dan duduk terlalu lama.

5. Hazard dan Risiko pada Bagian *Press II*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian

preparation, yaitu :

1. *Hazard* Mekanik : mesin press bertekanan tinggi.
   Risiko yang dapat ditimbulkan berupa terpotong mesin press.
2. *Hazard* Fisik : Panas, bising, pencahayaan yang kurang baik, serpihan material.
   Risiko yang dapat ditimbulkan berupa kelelahan mata karena, terkena percikan serpihan material
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive* serta mengangkat beban.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengangkat beban berat, duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

6. Hazard dan Risiko pada Bagian *Quality Control*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *quality control*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk
2. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

7. Hazard dan Risiko pada Bagian *Cleaning*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *cleaning*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk.
2. *Hazard* Fisik : zat kimia pembersih, getaran, radiasi gelombang *ultrasonic,* panas
   Risiko yang dapat ditimbulkan berupa terpapar zat kimia pembersih, terkena pajanan getaran dan radiasi *ultrasonic,* serta terbakar oleh panas dari *oven*.
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

8. Hazard dan Risiko pada Bagian *Packing*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *packing*, yaitu :

1. *Hazard* Mekanik : pisau mesin pemotong platik, mesin vacuum
   Risiko yang dapat ditimbulkan berupa tersayat mesin pemotong plastic dan terjepit mesin *vacuum*
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengemas produk ke dalam kardus.

2.2 Penilaian Risiko

Berikut ini penilaian beberapa risiko yang cukup signifikan dalam proses produksi:

1. Jari terpotong mesin pemotong material

   Risiko yang cukup besar pada bagian *preparation* adalah jari terpotong mesin pemotong material. Nilai *basic risk* untuk risiko tersebut adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat mengakibatkan kehilangan jari dan cacat permanen pada pekerja. *Exposure* (E) = 10 (*continuously*) karena pekerjaan tersebut dilakukan secara terus menerus dan berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena peristiwa ini memiliki kemungkinan kecil untuk terjadi.

   Pengendalian yang sudah dilakukan oleh pihak perusahaan adalah adanya program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign*, dan menyediakan sarung tangan untuk pekerja. Dari pengendalian tersebut maka nilai *existing risk* adalah 150 dengan kategori *substantial*. Penurunan risiko (*risk reduction*) sebesar 40%.

   Untuk mengurangi nilai risiko tersebut maka diberikan rekomendasi yaitu dengan pembuatan *Standard Operating Procedure (SOP)* untuk mesin pemotong, pengawasan rutin, pengecekan berkala untuk mesin, menggunakan mesin secara hati-hati dan sesuai prosedur serta disiplin dalam menggunakan alat pelindung diri (sarung tangan). Dari rekomendasi tersebut maka nilai *predictive risk* untuk risiko tersebut adalah 50 dengan kategori *priority 3.*

2. Terpotong mesin press

   Risiko yang cukup besar saat menggunakan mesin press adalah tangan atau jari dapat terpotong saat melakukan pencetakan produk. Hal ini disebabkan karena kekuatan mesin

yang cukup besar dan intensitas penggunaannya yang cukup tinggi. Nilai *basic risk* untuk risiko ini adalah 1500 (*very high*) dengan nilai *Consequences* (C) = 25 (*very serious*) karena dapat menyebabkan cacat permanen pada pekerja seperti kehilangan jari atau tangan. *Exposure* (E) = 10 (*continuously*) karena dilakukan secara terus menerus sepanjang hari selama jam kerja. *Likelihood/Probability* (P) = 6 (*likely*) karena kemungkinan untuk terjadinya kecelakaan adalah 50%-50%.

Pengendalian yang dilakukan perusahaan untuk mengurangi risiko tersebut adalah dengan menggunakan sensor otomatis pada mesin press. Sensor tersebut akan mendeteksi jika terdapat benda-benda yang melewatinya dan secara otomatis menghentikan kerja mesin press. Selain itu terdapat program pengawasan yang bernama *Bekaert Observation Program* dan pekerja juga dilengkapi dengan sarung tangan selama menggunakan mesin press. Berdasarkan risiko tersebut maka nilai *existing risk* adalah 250 dengan kategori *priority 1*. Penurunan risiko (*risk reduction*) sebesar 83,3%.

Untuk mengurangi risiko tersebut maka peneliti merekomendasikan dibuatnya *Standard Operating Procedure (SOP)* yang jelas dan ketat untuk penggunaan mesin press. Selain itu perlunya pengawasan rutin secara berkala pada pekerja. Pengecekan dan perawatan mesin dan fungsi sensor juga sangat diperlukan serta perlunya *guarding* di sisi kanan dan kiri mesin yang disesuaikan dengan kondisi dan posisi kerja karena sensor hanya berfungsi mendeteksi benda dari arah depan mesin. Berdasarkan rekomendasi tersebut maka didapatkan nilai *predictive risk* sebesar 50 dengan kategori *priority 3*.

3. Bising

Risiko bising terjadi ketika mesin *debouring* sedang beroperasi menghaluskan permukaan produk. Nilai *basic risk* untuk risiko ini adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat merusak kualitas pendengaran pekerja dan bersifat permanen. Selain itu juga menimbulkan ketidaknyamanan saat bekerja. *Exposure* (E) = 10 (*frequently*) karena terjadi lebih dari satu kali dalam sehari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya cukup kecil karena mesin dapat bekerja sendiri secara otomatis.

Pengendalian yang telah dilakukan oleh perusahaan adalah membatasi pekerja dengan cara meletakkan mesin *debouring* di dalam ruang tertutup. Program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign* di depan ruangan *debouring* serta pekerja diharuskan untuk menggunakan alat pelindung diri (*earmuff*)

ketika memasuki ruang *debouring*. Berdasarkan pengendalian tersebut maka didapatkan nilai *existing risk* sebesar 90 dengan kategori priority 3, Penurunan risiko (*risk reduction*) sebesar 64%.

Rekomendasi yang diberikan adalah membuat *Standard Operating Procedure (SOP)* dan *work permit* untuk memasuki ruang *debouring*. Selain itu diperlukan pengawasan secara rutin dan kedisplinan pekerja dalam menggunakan alat pelindung diri ketika berada di dalam ruang *debouring*. Berdasarkan rekomendasi tersebut maka didapatkan nilai predictive risk sebesar 15 dengan kategori *acceptable*.

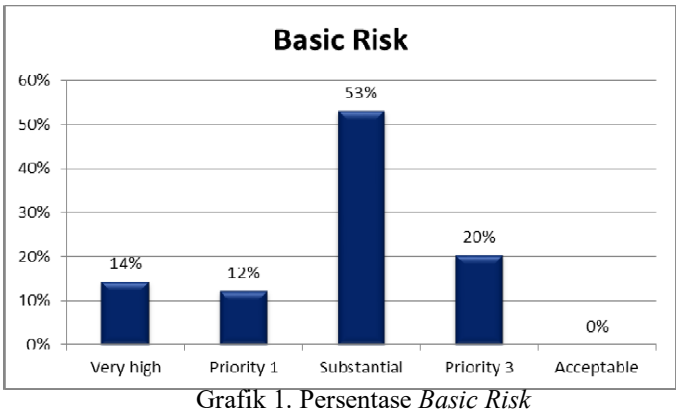
4. Postur janggal

Postur janggal dapat terjadi ketika pekerja melakukan pengemasan produk ke dalam kardus-kardus sebelum dikirimkan. Pengemasan produk dilakukan dalam bungkuk untuk memasukkan dan mengatur posisi produk di dalam kardus. Nilai *basic risk* untuk risiko ini adalah 150 dengan kategori *substantial* dengan nilai *Consequences* (C) = 15 (*serious*) karena dapat mengakibatkan nyeri dan cedera pada tulang pinggang. *Exposure* (E) = 10 (*frequently*) karena dilakukan pekerja secara berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya risiko ini cukup kecil. Belum terdapat pengendalian yang dilakukan perusahaan untuk risiko ini. Maka nilai *existing risk* sama dengan nilai *basic risk* yaitu 150 dengan kategori *substantial.*

Untuk mengurangi risiko postur janggal karena posisi bungkuk, maka peneliti merekomendasikan agar pekerja melakukan *stretching* 1 kali dalam 1 jam untuk melemaskan otot-otot tubuh agar tidak kaku. Selain itu sebaiknya pengemasan dilakukan dengan posisi yang benar agar pekerja tidak harus terlalu membungkuk. Nilai *predictive risk* dari rekomendasi tersebut adalah 15 dengan kategori *acceptable*.

Persentase Nilai *Basic Risk, Existing Risk* dan *Predictive Risk*

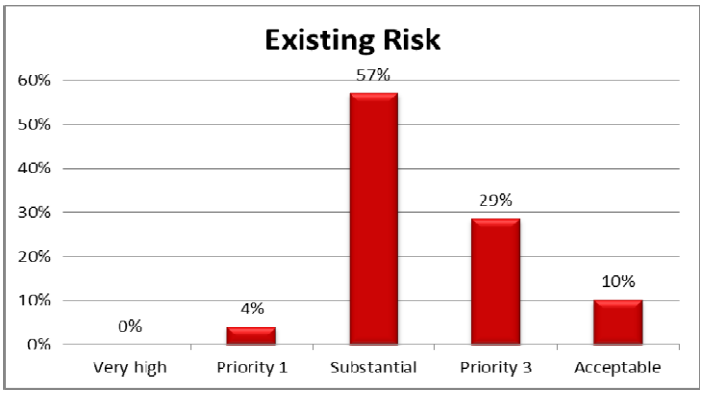
1. Basic Risk



Grafik 1. Persentase *Basic Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *basic risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 14% (7 aktivitas), kategori *priority 1* sebesar 12% (6 aktivitas), kategori *substantial* sebesar 53% (23 aktivitas), kategori *priority 3* sebesar 20% (10 aktivitas) dan kategori *acceptable* sebesar 0% (0 aktivitas).

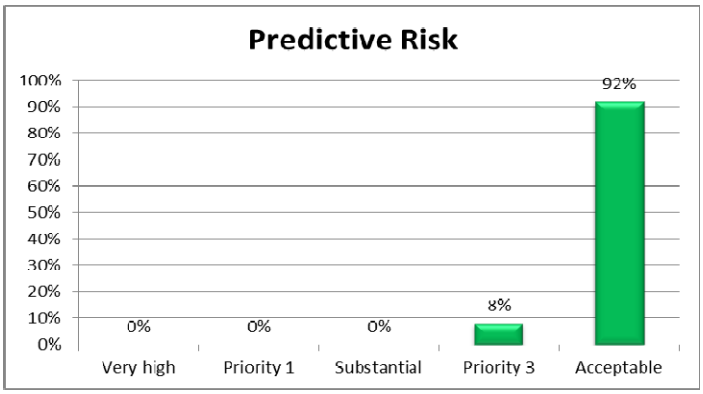
2. Existing Risk



Grafik 2. Persentase *Existing Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *existing risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 4% (2 aktivitas), kategori *substantial* sebesar 57% (28 aktivitas), kategori *priority 3* sebesar 29% (14 aktivitas) dan kategori *acceptable* sebesar 10% (5 aktivitas).

3. Predictive Risk



Grafik 3. Persentase *Predictive Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *predictive risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 0% (0 aktivitas), kategori *substantial* sebesar 0% (0 aktivitas), kategori *priority 3* sebesar 8% (4 aktivitas) dan kategori *acceptable* sebesar 92% (45 aktivitas).

3. SIMPULAN

Berdasarkan hasil dan analisis penelitian mengenai risiko keselamatan dan kesehatan kerja pada proses produksi *spin pack* di PT BAF tahun 2013, maka didapatkanlah simpulan sebagai berikut:

1. Terdapat 8 proses kerja pada proses produksi *spin pack*. Proses kerja tersebut terdiri dari *preparation* (persiapan material), *press I* (pencetakan), *debouring* (penghalusan), *assembling* (perakitan), *press II* (pressing), *quality control* (pengecekan), *cleaning* (pembersihan), *packing* (pengemasan).
2. Jenis bahaya paling dominan pada aktivitas proses produksi *spin pack* adalah bahaya mekanis seperti tertusuk, tergores, tersayat dan terpotong.
3. Ditemukan 7 risiko dalam 6 aktivitas dengan kategori *very high* pada *basic risk* di proses produksi *spin pack*. Aktivitas tersebut adalah pengambilan *tools*, pemasangan *tools,* pencetakan produk, membuka dan mengembalikan *tools* serta pada proses *pressing*.
4. Untuk *existing risk*, tidak ditemukan aktivitas dengan kategori *very high* namun terdapat 2 aktivitas dengan kategori *priority 1* yang membutuhkan perbaikan sesegera mungkin. Aktivitas tersebut yaitu pada proses pencetakan dan proses *pressing*.
5. Secara umum pengendalian yang sudah dilakukan oleh perusahaan adalah dengan

mengadakan program pengawasan yang disebut dengan *Bekaert Observation Program,* pemasangan *safety sign* dan penyediaan alat pelindung diri.

6. Berdasarkan program pengendalian yang sudah dilakukan perusahaan, berbagai risiko yang ada dapat dikurangi dengan persentase *risk reduction* antara 40% - 93,3%.
7. Pada *predictive risk*, sebagian besar risiko dapat diturunkan pada kategori *acceptable*. Namun masih terdapat 4 aktivitas yang berada pada kategori *priority 3*.

4. DAFTAR PUSTAKA

Alfiah, Suzi. 2012. *Penilaian Risiko Keselamatan dan Kesehatan Kerja pada Kegiatan Operasi dan Produksi PT Pertamina Geothermal Energy Area Lahendong Tahun 2012*. Skripsi. Depok: Fakultas Kesehatan Masyarakat Universitas Indonesia.

"Angka Kecelakaan Kerja Lima Tahun Terakhir Meningkat". http://www.poskotanews.com/2012/06/01/angka-kecelakaan-kerja-lima-tahun-terahir-cendrung-naik/ (diakses pada 14 Maret 2013 pukul 15.33 WIB)

European Agency for Safety and Health at Work. "Definitions". https://osha.europa.eu/en/topics/riskassessment/definitions

Jamsostek. "Setiap Hari Ada 9 Peserta Jamsostek Tewas Kecelakaan Kerja". http://www.jamsostek.co.id/content/news.php?id=3957

PAPER

PROSES MENEJEMEN RESIKO

Disusun Oleh :

Fandi Kurniawan
182420025

Magister Teknik Informatika
Program Pascasarjana
Universitas Bina Darma

Abtrak : *Manajemen risiko merupakan salah satu elemen penting dalam menjalanlan bisnis perusahaan akrean semakian berkembangnya dunia perusahaan, adanya persaingan yang semakin ketat, serta meningkatnya kompleksitas aktivitas perusahaan mengakibatkan meningkatnmya tingkat risiko yang dihadapi perusahaan. Risiko bisa datang kapan saja dan sulit dihindari, risiko bisa berdampak signifikan terhadap kerugian perusahaan. Sehingga risiko sangat penting untuk dikekola. Manajemen risiko bertujuan untuk mengelola risiko sehingga perusahaan atau organisasi bisa mengoptimalkan risiko tersebut.*

Keberhasilan mengkomunikasikan dan mengintegrasikan menejemen resiko dalam sebuah organisasi tidak terletak pada tekniknya saja, tetapi juga tergantung pada manusia pengambil dan pengelola risiko tersebut. tujuan penulisan paper ini adalah untuk menjelaskan konsep manajemen risiko dan cara mengelola risiko di perusahaan ataupun organisai

1. Pendahuluan

Dalam kehidupan sehari-hari kita sering mendengar kata "Resiko" dan sudah biasa dipakai dalam percakapan sehari-hari oleh kebanyakan orang. Resiko merupakan bagian dari kehidupan kerja individual maupun organisasi. Berbagai macam resiko, seperti resiko kebakaran, tertabrak kendaraan lain di jalan, resiko terkena banjir di musim hujan dan sebagainya, dapat menyebabkan kita menanggung kerugian jika resiko-resiko tersebut tidak kita antisipasi dari awal. Resiko dikaitkan dengan kemungkinan kejadian atau keadaan yang dapat mengancam pencapaian tujuan dan sasaran organisasi. Sebagaimana kita pahami dan sepakati bersama bahwa tujuan perusahaan adalah membangun dan memperluas keuntungan kompetitif organisasi.

Resiko berhubungan dengan ketidakpastian ini terjadi karena kurang atau tidak tersedianya cukup informasi tentang apa yang akan terjadi. Sesuatu yang tidak pasti (uncertain) dapat berakibat menguntungkan atau merugikan. Menurut Wideman, ketidakpastian yang menimbulkan kemungkinan menguntungkan dikenal dengan istilah peluang (opportunity), sedangkan ketidakpastian yang menimbulkan akibat yang merugikan disebut dengan istilah resiko (risk). Dalam beberapa tahun terakhir, manajemen resiko menjadi trend utama baik dalam perbincangan, praktik, maupun pelatihan kerja. Hal ini secara konkret menunjukkan pentingnya manajemen resiko dalam bisnis pada masa kini.

Secara umum resiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan di mana terdapat kemungkinan yang merugikan. Bagaimana jika kemungkinan yang dihadapi dapat memberikan keuntungan yang sangat besar, dan walaupun mengalami kerugian sangat kecil sekali. Misalnya membeli lotere. Jika beruntung maka akan mendapat hadiah yang sangat besar, tetapi jika tidak beruntung uang yang digunakan membeli lotere relatif kecil. Apakah ini juga tergolong resiko? Jawabannya adalah hal ini juga tergolong resiko. Selama mengalami kerugian walau sekecil apapun hal itu dianggap resiko.

2. Pembahasan

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 pemberdayaan/pengelolaan sumber daya. Strategi yang dapat diambil antara lain adalah memindahkan resiko kepada pihak lain,menghindari resiko, mengurangi efek negatif resiko, dan menampung sebagian atau semua konsekuensi

resiko tertentu. Manajemen resiko tradisional terfokus pada resiko- resiko yang timbul oleh penyebab fisik atau legal (seperti bencana alam atau kebakaran, kematian, dan tuntutan hukum).

Menurut Vibiznews.com, manajemen resiko adalah suatu proses mengidentifikasi, mengukur resiko, serta membentuk strategi untuk mengelolanya melalui sumber daya yang tersedia. Strategi yang dapat digunakan antara lain mentransfer resiko pada pihak lain,menghindari resiko, mengurangi efek buruk dari resiko dan menerima sebagian maupun seluruh konsekuensi dari resiko tertentu.

Sasaran dari pelaksanaan manajemen resiko adalah untuk mengurangi resiko yang berbeda-beda yang berkaitan dengan bidang yang telah dipilih pada tingkat yang dapat diterima oleh masyarakat. Hal ini dapat berupa berbagai jenis ancaman yang disebabkan oleh lingkungan, teknologi, manusia, organisasi, dan politik. Di sisi lain,pelaksanaan manajemen resiko melibatkan segala cara yang tersedia bagi manusia, khususnya entitas manajemen resiko (manusia, staff, organisasi).

a. Proses Manajemen Risiko

Manajemen menurut Nickels, McHugh and McHugh (1997) adalah sebuah proses yang dilakukan untuk mewujudkan tujuan organisasi melalui rangkaian kegiatan berupa perencanaan, pengorganisasian, pengarahan, dan pengendalian orang-orang serta sumber daya organisasi lainnya

Berdasarkan pengertian tersebut di atas maka Mamduh Hanafi (2009) membagi proses manajemen risiko menjadi beberapa tahap antara lain:

1. Perencanaan

Perencanaan manajemen risiko bisa dimulai dengan menetapkan visi, misi dan tujuan yang berkaitan dengan manajemen risiko. Kemudian perencanaan manajemen risiko bisa diteruskan dengan penetapan target, kebijakan dan prosedur yang berkaitan dengan manajemen risiko. Akan lebih baik lagi jika visi, misi, kebijakan dan prosedur tersebut dituangkan secara tertulis. Dokumen tertulis semacam itu memudahkan pengarah- an, sekaligus menegaskan dukungan manaje- men terhadap program manajemen risiko.

Contoh misi atau kebijakan dan prosedur yang berkaitan dengan manajemen risiko dari beberapa perusahaan/organisasi, seperti Peryataan Misi Manajemen Risiko Goldman Sach:

Misi dari departemen risiko adalah mengumpulkan, menganalisis, memonitor, dan mendistribusikan informasi yang berkaitan dengan risiko pasar dari posisi perusahaan supaya traders, manajer dan prsonel lain dalam organisasi dan terutama komite risiko memahami dan membuat keputusan berdasarkan informasi (informed decision) mengenai manajemen dan pengendalian risiko yang diambil.

(Goldman Sach adalah perusahaan sekuritas Amerika Serikat)

2. Pelaksanaan

Pelaksanaan manajemen risiko meliputi aktivitas operasional yang berkaitan dengan manajemen risiko. Proses identifikasi dan pengukuran risiko kemudian diteruskan dengan manajemen (pengelolaan) risiko yang merupakan aktivitas operasional yang utama dari manajemen risiko.

a. Identifikasi risiko

Identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang dihadapi oleh suatu organisasi. Teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh: kompor ditaruh dekat penyimpanan minyak tanah. Api merupakan sumber risiko, kompor yang ditaruh dekat minyak tanah merupakan kondisi yang meningkatkan terjadinya kecelakaan, bangunan yang bisa terbakar merupakan eksposur yang dihadapi perusahaan.

b. Evaluasi dan Pengukuran Risiko

Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk mengukur risiko tersebut. Sebagai contoh: kita bisa memperkirakan probabilitas (kemungkinan) risiko atau suatu kejadian jelek terjadi. Dengan probabilitas tersebut kita berusaha mengukur risiko. Misal: ada risiko perusahaan terkena jatuhan meteor atau komet, tetapi probabilitas risiko semacam ini sangat kecil (0,000000001). Karena itu risiko tersebut tidak perlu diperhatikan. Contoh lain: risiko kebakar- an dengan probabilitas (misal) 0.6. karena probabilitas yang tinggi maka risiko kebakaran perlu diberi perhatian ekstra.

c. Pengelolaan Risiko

Risiko harus dikelola, jika tidak maka konsekuensinya bisa cukup serius misal kerugian yang culup besar. Risiko bisa dikelola dengan berbagai cara antara lain dengan melakukan penghindaran, risiko tersebut ditahan, melakukan diversifikasi, mentransfer risiko, dan mengendalikan risiko dan mendanai kerugian sendiri.

3. Pengendalian

Tahap berikutnya dari proses manajemen risiko adalah pengendalian yang meliputi evaluasi secara periodik pelaksanaan manajemen risiko, output pelaporan yang dihasilkan oleh manajemen risiko dan umpan balik (feedback). Format pelaporan manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya dan dari satu kegiatan kegiatan lainnya.

b. Mengidentifikasi resiko

Pengidentifikasian resiko merupakan proses analisa untuk menemukan secara sistematis dan berkesinambungan atas resiko (kerugian yang potensial) yang dihadapi perusahaan. Oleh karena itu, diperlukan checklist untuk pendekatan yang sistematis dalam menentukan kerugian potensial. Salah satu alternatif sistem pengklasifikasian kerugian dalam suatu checklist adalah; kerugian hak milik (property losses), kewajiban mengganti kerugian orang lain (liability losses) dan kerugian personalia (personnel losses). Checklist yang dibangun sebelumnya untuk menemukan resiko dan menjelaskan jenis-jenis kerugian yang dihadapi oleh suatu perusahaan.

Perusahaan yang sifat operasinya kompleks, berdiversifikasi dan dinamis, maka diperlukan metode yang lebih sistematis untuk mengeksplorasi semua segi. Metode yang dianjurkan adalah sebagai berikut:

1. Questioner analisis resiko (risk analysis questionnaire)
2. Metode laporan Keuangan (financial statement method)
3. Metode peta aliran (flow-chart)
4. Inspeksi langsung pada objek

5. Interaksi yang terencana dengan bagian-bagian perusahaan
6. Catatan statistik dari kerugian masa lalu
7. Analisis lingkungan

Dengan mengamati langsung jalannya operasi, bekerjanya mesin, peralatan, lingkungan kerja, kebiasaan pegawai dan seterusnya, manajer resiko dapat mempelajari kemungkinan tentang hazard. Oleh karena itu, keberhasilannya dalam mengidentifikasi resiko tergantung pada kerja sama yang erat dengan bagian-bagian lain yang terkait dalam perusahaan.

4. Kesimpulan

Resiko adalah kemungkinan kejadian atau keadaan yang dapat mengancam pencapaian tujuan dan sasaran organisasi. Sedangkan Manajemen Risiko yaitu upaya-upaya dalam bentuk aturan maupun tindakan yang ditujukan untuk mengoptimalkan (meminimalisir) risiko atas suatu portfolio sesuai dengan Kebijakan Investasi masing-masing dana kelolaan. Penerapan sistem manajemen risiko mengacu pada peraturan serta ketentuan yang tertuang dalam kebijakan perusahaan.

Manajemen risiko dan pengendalian internal memiliki kesamaan materi dan komponen, dan saling terkait satu dengan lainnya. Manajemen risiko yang ada perlu dievaluasi keandalannya. Sementara itu, aktifitas pengendalian akan menjadi optimal dengan menggunakan pendekatan risiko.

5. Penutup

Demikian makalah makalah yang kami buat, kami menyadari masih banyak kekurangan dalam tulisan maupun dari referensi yang diperlukan, untuk itu kami harap kritik dan saran yang bisa membangun demi kesempurnaan makalah ini.semoga makalah inidapat bermanfaat bagi semuanya.

DAFTAR PUSTAKA

http://www.spexotics.com/2012/09/pengertian-manajemen-risiko.
Ahira, Anne. Manajemen Resiko. 2012. http://www.anneahira.com/manajemen-resiko.htm
Darmawi, Herman. Manajemen Risiko. Bumi Aksara, 2005

Analisis Resiko Pada Akademik Management System Universitas Bina Insani Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-

masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview.* Proses ini

dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden

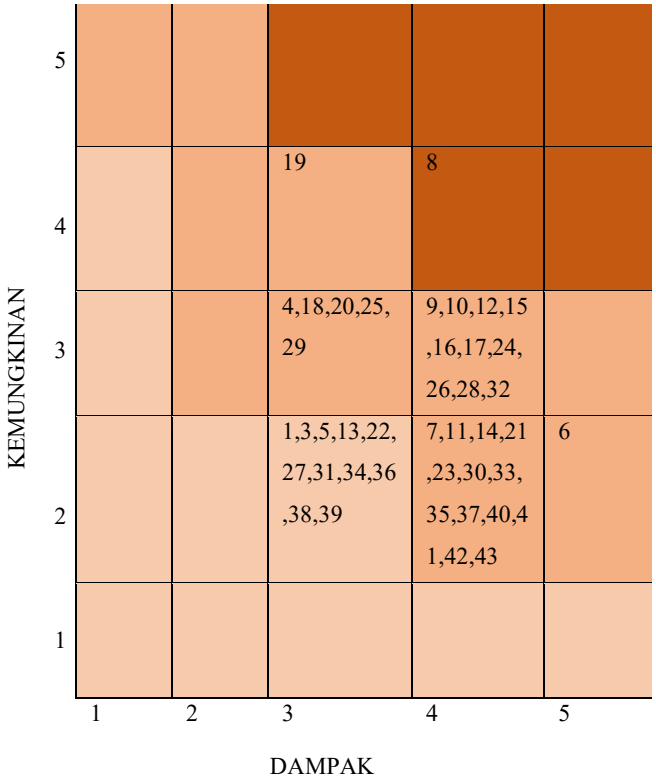
dengan menggunakan kriteria yang telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling

tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

PENILAIAN RISIKO KERJA PADA PROSES PRODUKSI

Ahkmad Ipandy[1], Erin Efriansyah[2], Fero Triando[3], Tri Akhyari Romadhon[4]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Penilisan ini dilakukan karena ditemukan berbagai bahaya dan risiko pada pekerja di bagian proses produksi. Penelitian ini bertujuan untuk mengetahui besaran risiko keselamatan dan kesehatan kerja pada pekerja di bagian proses produksi *spin pack*. Hasil telitian menunjukkan bahwa pada *basic risk* terdapat 6 aktivitas yang termasuk dalam level *very high*. Pada *existing risk*, terdapat 2 aktivitas dengan risiko tinggi yang termasuk dalam level *priority 1*, yaitu pada proses pencetakan dan proses *pressing* produk yang menggunakan mesin *press*. Dalam penelitian ini juga diberikan *predictive risk* dengan rekomendasi pengendalian, sehingga risiko-risiko yang ada dapat diturunkan sampai pada level *acceptable*.

Kata kunci: Penilaian risiko, resiko kerja , proses produksi

1. PENDAHULUAN

Keselamatan dan kesehatan kerja (K3) merupakan promosi dan pemeliharaan tertinggi tingkat fisik, mental dan kesejahteraan sosial dari semua pekerjaan, pencegahan efek kesehatan yang disebabkan oleh kondisi kerja pekerja, perlindungan bagi pekerja dari resiko akibat faktor yang merugikan bagi kesehatan, menempatkan dan pemeliharaan pekerja dalam lingkungan kerja disesuaikan pada fisiologis dan psikologis dan untuk meringkas adaptasi bekerja untuk manusia dan masing-masing pekerjaannya (*ILO/WHO Join and Health Committee, 1950*). Berdasarkan definisi tersebut dapat dikatakan bahwa K3 merupakan salah satu faktor yang paling penting dan sangat dibutuhkan untuk menjamin keselamatan hidup manusia.

Kecelakaan merupakan sebuah kejadian tak terduga yang menyebabkan cedera atau kerusakan (Ridley, 2004). Kecelakaan akibat kerja adalah kecelakaan yang berkaitan dengan hubungan kerja dengan perusahaan. Hubungan kerja disini dapat berarti bahwa kecelakaan dapat terjadi dikarenakan oleh pekerjaan atau pada waktu melakukan pekerjaan (Suma'mur, 1989). Dalam hal ini kita dapat melihat bahwa kecelakaan adalah salah satu risiko yang cukup besar karena menyebabkan cedera dan kerugian yang dapat terjadi kapan saja terutama bagi pekerja.

Setiap tahunnya di dunia terjadi sekitar 340 juta kecelakaan kerja dan 160 juta korban penyakit akibat kerja (ILO, 2011). Angka ini menunjukkan bahwa kecelakaan kerja masih tergolong tinggi dan butuh tindakan pencegahan sesegera mungkin agar angka tersebut tidak

terus bertambah. Di Indonesia pun, angka kecelakaan kerja masih terus meningkat dari tahun ke tahun. Ini terbukti dari data Jamsostek selama 5 tahun terakhir. Berikut data Jamsostek mengenai angka kecelakaan kerja di Indonesia dalam kurun waktu 5 tahun terakhir.

Table 1. Angka Kecelakaan Kerja dan Klaim Kecelakaan Tahun 2008-2012

Tahun	Angka Kecelakaan Kerja (kasus)	Klaim Kecelakaan Kerja (rupiah)
2012	103.000	646,2 milyar
2011	99.491	504 milyar
2010	98.711	401,2 milyar
2009	96.314	328,5 milyar
2008	94.763	297,9 milyar

Sumber: Jamsostek

Berdasarkan data diatas kita dapat melihat bahwa angka kecelakaan kerja di Indonesia terus meningkat setiap tahunnya. Hal ini tentu menunjukkan bahwa masih lemahnya sistem keselamatan dan kesehatan kerja untuk melindungi pekerja-pekerja di Indonesia. Jika kondisi ini tidak segera ditangani, maka pengingkatan jumlah kecelakaan kerja akan cenderung untuk terjadi di tahun-tahun yang akan datang. Menurut Suma'mur (1989), kecelakaan menyebabkan lima kerugian yaitu kerusakan, kekacauan organisasi, keluhan dan kesedihan, kelainan dan cacat serta kematian.

Disamping kerugian-kerugian tersebut, perusahaan juga harus menanggung biaya-biaya lainnya yang timbul dari kecelakaan tersebut. Salah satunya adalah biaya klaim asuransi kecelakaan kerja. Berdasarkan tabel 1.1 dapat dilihat bahwa peningkatan angka kecelakaan tentunya juga diiringi dengan peningkatan klaim asuransi untuk pekerja yang mengalami kecelakaan. Selain itu perusahaan juga diharuskan untuk memberikan ganti rugi atau kompensasi kepada pekerja yang mengalami kecelakaan pada saat bekerja atau di tempat kerja. Hal ini telah diatur dalam Undang-Undang No. 34 tahun 1947 Tentang Kecelakaan Kerja dan Undang-Undang No.2 tahun 1992 tentang Jaminan Sosial Tenaga Kerja. Biaya-biaya tersebutlah yang harus ditanggung oleh perusahaan jika kecelakaan kerja masih terus terjadi.

Selain banyaknya biaya yang harus dikeluarkan perusahaan untuk kompensasi dan mengganti kerugian, kecelakaan kerja juga menyebabkan perusahaan akan dirugikan oleh hilangnya hari kerja dan menurunnya produktivitas pekerja. Jika kasus kecelakaan terus bertambah dari waktu ke waktu dapat memberikan citra buruk bagi perusahaan karena tidak

dapat menjamin keselamatan pekerjanya.

Salah satu aspek penting yang harus diperhatikan perusahaan untuk meminimalisir terjadinya kecelakaan adalah dengan melakukan manajemen risiko. Menurut AS/NZS 4360, Manajemen Risiko adalah "*the culture, process and structures that are directed towards the effective management of potential opportunities and adverse effect*". Manajemen risiko menyangkut budaya, proses dan struktur dalam mengelola suatu risiko secara efektif dan terencana dalam suatu sistem manajemen yang baik (Ramli, 2010).

Manajemen risiko tidak terlepas dari berbagai risiko-risiko K3 yang dapat timbul dari setiap kegiatan di tempat kerja. Menurut OHSAS 18001, risiko K3 adalah kombinasi dari kemungkinan terjadinya kejadian berbahaya atau paparan dengan keparahan dari cedera atau gangguan kesehatan yang disebabkan oleh kejadian atau paparan tersebut (Ramli, 2010).

Maka secara sederhana dapat dikatakan bahwa manajemen risiko merupakan proses untuk mengelola risiko yang ada dalam setiap kegiatan (Ramli, 2010).

Manajemen pengelolaan risiko dilakukan dengan sebuah prinsip utama yang disebut *Calculated Risk* atau risiko yang diperhitungkan (Ramli, 2010). *Calculated risk* dilakukan untuk mengetahui seberapa besar tingkat risiko terhadap suatu *task* atau kegiatan yang dilakukan pekerja di tempat kerja. Apabila sebuah pekerjaan telah diketahui tingkat risikonya, maka akan dapat dilakukan pengendalian risiko terhadap pekerjaan tersebut sebelum terjadi kecelakaan. Hal ini tentu akan sangat bermanfaat bagi perusahaan untuk mencegah berbagai kerugian yang mungkin terjadi apabila risiko tersebut tidak segera dikelola dan dikendalikan.

Manajemen risiko meliputi identifikasi bahaya dan risiko, analisis dan penilaian risiko dan evaluasi risiko serta tindakan pengendalian yang dilakukan selama proses kerja berlangsung. Apabila aspek-aspek dalam manajemen risiko ini tidak diperhatikan dan dikelola dengan baik maka akan menimbulkan kerugian bagi perusahaan. Tidak hanya kecelakaan pada pekerja, namun dampak lainnya dapat berpengaruh pada kerugian finansial yang harus ditanggung oleh perusahaan serta kerugian yang harus diterima perusahaan akibat citra buruk yang ditimbulkan karena tidak melaksanakan manajemen risiko dengan baik. Oleh karena itu, perusahaan perlu melaksanakan manajemen risiko dengan baik khususnya dalam mengidentifikasi bahaya dan risiko serta melakukan penilaian risiko untuk dapat menentukan pengendalian yang dapat dilakukan sehingga dapat mencegah dan mengurangi kerugian (*loss*) yang dapat timbul.

Prinsip manajemen risiko berupa penilaian risiko tentu harus diterapkan oleh seluruh

industri maupun perusahaan. Terutama bagi perusahaan-perusahaan atau industri yang mempunyai tingkat risiko K3 yang tinggi dalam proses kerjanya. Salah satu perusahaan dengan tingkat risiko K3 yang cukup tinggi adalah PT BAF. PT BAF merupakan perusahaan manufaktur yang bergerak dalam bidang produksi filter. Salah satu filter yang diproduksi oleh PT BAF adalah filter yang digunakan untuk memisahkan uap maupun gas pada industri-industri kimia. Selain itu PT BAF juga memproduksi filter untuk gas panas yang digunakan pada industri pertambangan serta masih banyak jenis filter yang telah diproduksi oleh PT BAF. Namun dari semua filter yang diproduksi, produksi paling banyak dan yang paling rutin dilakukan oleh PT BAF adalah pembuatan *screen filter* atau sering disebut *spin pack*. *Spin pack* terbuat dari bahan dasar logam, alumunium atau *wire mesh* yang diproduksi berdasarkan pesanan dari berbagai industri sesuai dengan kebutuhannya masing-masing. Pembuatan *spin pack* baik yang berbahan dasar logam, alumunium maupun *wire mesh*, tentu membutuhkan proses dan rangkaian kerja yang cukup kompleks. Proses kerja yang kompleks dan rumit serta menggunakan alat-alat dan mesin mekanis tentunya akan menimbulkan risiko kecelakaan yang cukup besar bagi pekerja. Oleh karena itu perlu dilakukan analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF untuk mengetahui tingkat risiko yang ada serta rekomendasi pengendalian yang dapat dilakukan guna mencegah dan meminimalisir terjadinya kecelakaan. Adapun tujuan dari penelitian ini adalah:

1. Tujuan Umum

   Untuk memperoleh gambaran mengenai analisis penilaian risiko keselamatan dan kesehatan kerja pada kegiatan proses produksi *spin pack* di PT BAF tahun 2013
2. Tujuan Khusus
   1. Mengetahui proses atau tahapan kerja apa saja yang terdapat pada proses produksi *spin pack* di PT BAF.
   2. Mengetahui bahaya yang terdapat pada tahapan kerja pada proses produksi *spin pack* di PT BAF.
   3. Mengetahui nilai *consequence, likelihood, exposure* dan *basic risk* dari risiko-risiko K3 tanpa mempertimbangkan pengendalian yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   4. Mengetahui pengendalian risiko K3 yang sudah dilakukan pada proses produksi *spin pack* di PT BAF.
   5. Mengetahui nilai *consequence, likelihood, exposure* dan *existing risk* dari risiko-risiko K3 dengan mempertimbangkan pengendalian yang sudah dilakukan pada

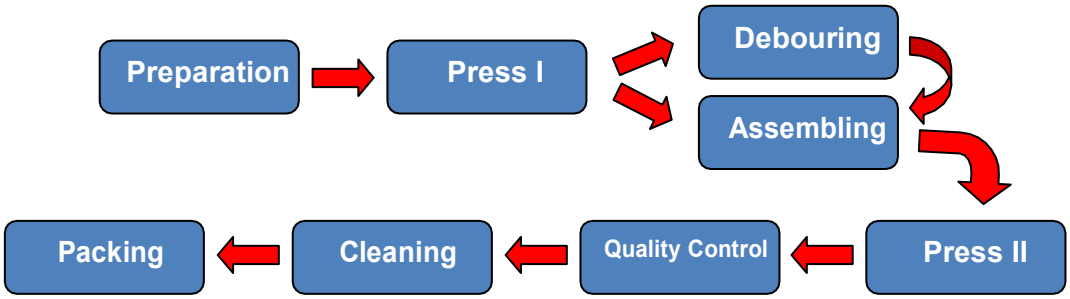
proses produksi *spin pack* di PT BAF.

6. Mengetahui nilai dari *risk reduction* pada proses produksi *spin pack* di PT BAF.
7. Mengetahui rekomendasi pengendalian yang masih memungkinkan dapat dilakukan untuk menurunkan risiko saat ini (*existing risk*) pada proses produksi *spin pack* di PT BAF.
8. Mengetahui nilai risiko prediksi (*predictive risk*) setelah ada rekomendasi pengendalian pada proses produksi *spin pack* di PT BAF.

2. HASIL PENELITIAN DAN PEMBAHASAN

2.1 Identifikasi Hazard dan Risiko

Tahap-tahap proses produksi *Spin Pack*



Gambar 1. Alur Proses Produksi *Spin Pack*

Identifikasi *hazard* dan risiko pada kegiatan proses produksi *spin pack* dilakukan dengan menggunakan *job hazard analysis* (JHA). JHA dibuat berdasarkan jenis pekerjaan dan bagiannya masing-masing. Tujuannya agar diketahui dengan jelas bahaya dan risiko disetiap masing-masing bagian.

1. Hazard dan Risiko pada Bagian *Preparation*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *preparation*, yaitu :

1. *Hazard* Mekanik : Sepihan material, mesin pemotong dan mesin perata.
   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk seprihan material, terjepit mesin calendaring, terpotong mesin pemotong material.
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban (material)

2. Hazard dan Risiko pada Bagian *Press I*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *press I*, yaitu:

1. *Hazard* Mekanik

   Risiko yang dapat ditimbulkan berupa terjepit dan tertimpa tooling, terpukul benda keras saat memasang tooling, terpotong mesin press, tergores dan tertusuk material

2. *Hazard* Fisik : Panas, bising, pencahayaan kurang baik, serpihan material.

   Risiko yang dapat ditimbulkan berupa ketidaknyamanan, kurangnya konsentrasi, kelelahan mata karena pencahayaan yang kurang baik, dan terkena percikan serpihan material. *azard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive*

   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

3. Hazard dan Risiko pada Bagian *Debouring*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *debouring*, yaitu :

1. *Hazard* Mekanik : serpihan material

   Risiko yang dapat ditimbulkan berupa tergores dan tertusuk serpihan material

2. *Hazard* Fisik : Bising

   Risiko yang dapat ditimbulkan berupa ketdaknyamanan, kurangnya konsentrasi dan penurunan fungsi pendegaran.

3. *Hazard* Ergonomi : Postur janggal saat membawa beban

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban.

4. Hazard dan Risiko pada Bagian *Assembling*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *assembling*, yaitu :

1. *Hazard* Mekanik : produk dari logam bersisi tajam

   Risiko yang dapat ditimbulkan berupa tersayat produk

2. *Hazard* Ergonomi : Postur janggal saat membawa beban dan saat duduk terlalu lama.

   Risiko yang dapat ditimbulkan berupa nyeri dan pegal pada bagian tubuh tertentu saat mengangkat beban dan duduk terlalu lama.

5. Hazard dan Risiko pada Bagian *Press II*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian

preparation, yaitu :

1. *Hazard* Mekanik : mesin press bertekanan tinggi.
   Risiko yang dapat ditimbulkan berupa terpotong mesin press.
2. *Hazard* Fisik : Panas, bising, pencahayaan yang kurang baik, serpihan material.
   Risiko yang dapat ditimbulkan berupa kelelahan mata karena, terkena percikan serpihan material
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama dan *gerakan repetitive* serta mengangkat beban.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengangkat beban berat, duduk terlalu lama dengan gerakan *repetitive* hingga dapat menyebabkan musculoskeletal disorders (MSDs).

6. Hazard dan Risiko pada Bagian *Quality Control*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *quality control*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk
2. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

7. Hazard dan Risiko pada Bagian *Cleaning*

Berdasarkan hasil observasi, terdapat tiga jenis kategori *hazard* pada bagian *cleaning*, yaitu :

1. *Hazard* Mekanik : produk bersisi tajam
   Risiko yang dapat ditimbulkan berupa tergores produk.
2. *Hazard* Fisik : zat kimia pembersih, getaran, radiasi gelombang *ultrasonic,* panas
   Risiko yang dapat ditimbulkan berupa terpapar zat kimia pembersih, terkena pajanan getaran dan radiasi *ultrasonic,* serta terbakar oleh panas dari *oven*.
3. *Hazard* Ergonomi : Postur janggal saat duduk terlalu lama.
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat duduk terlalu lama hingga dapat menyebabkan musculoskeletal disorders (MSDs).

8. Hazard dan Risiko pada Bagian *Packing*

Berdasarkan hasil observasi, terdapat dua jenis kategori *hazard* pada bagian *packing*, yaitu :

1. *Hazard* Mekanik : pisau mesin pemotong platik, mesin vacuum
   Risiko yang dapat ditimbulkan berupa tersayat mesin pemotong plastic dan terjepit mesin *vacuum*
2. *Hazard* Ergonomi : Postur janggal
   Risiko yang dapat ditimbulkan berupa nyeri pada otot saat mengemas produk ke dalam kardus.

2.2 Penilaian Risiko

Berikut ini penilaian beberapa risiko yang cukup signifikan dalam proses produksi:

1. Jari terpotong mesin pemotong material

   Risiko yang cukup besar pada bagian *preparation* adalah jari terpotong mesin pemotong material. Nilai *basic risk* untuk risiko tersebut adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat mengakibatkan kehilangan jari dan cacat permanen pada pekerja. *Exposure* (E) = 10 (*continuously*) karena pekerjaan tersebut dilakukan secara terus menerus dan berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena peristiwa ini memiliki kemungkinan kecil untuk terjadi.

   Pengendalian yang sudah dilakukan oleh pihak perusahaan adalah adanya program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign*, dan menyediakan sarung tangan untuk pekerja. Dari pengendalian tersebut maka nilai *existing risk* adalah 150 dengan kategori *substantial*. Penurunan risiko (*risk reduction*) sebesar 40%.

   Untuk mengurangi nilai risiko tersebut maka diberikan rekomendasi yaitu dengan pembuatan *Standard Operating Procedure (SOP)* untuk mesin pemotong, pengawasan rutin, pengecekan berkala untuk mesin, menggunakan mesin secara hati-hati dan sesuai prosedur serta disiplin dalam menggunakan alat pelindung diri (sarung tangan). Dari rekomendasi tersebut maka nilai *predictive risk* untuk risiko tersebut adalah 50 dengan kategori *priority 3.*

2. Terpotong mesin press

   Risiko yang cukup besar saat menggunakan mesin press adalah tangan atau jari dapat terpotong saat melakukan pencetakan produk. Hal ini disebabkan karena kekuatan mesin

yang cukup besar dan intensitas penggunaannya yang cukup tinggi. Nilai *basic risk* untuk risiko ini adalah 1500 (*very high*) dengan nilai *Consequences* (C) = 25 (*very serious*) karena dapat menyebabkan cacat permanen pada pekerja seperti kehilangan jari atau tangan. *Exposure* (E) = 10 (*continuously*) karena dilakukan secara terus menerus sepanjang hari selama jam kerja. *Likelihood/Probability* (P) = 6 (*likely*) karena kemungkinan untuk terjadinya kecelakaan adalah 50%-50%.

Pengendalian yang dilakukan perusahaan untuk mengurangi risiko tersebut adalah dengan menggunakan sensor otomatis pada mesin press. Sensor tersebut akan mendeteksi jika terdapat benda-benda yang melewatinya dan secara otomatis menghentikan kerja mesin press. Selain itu terdapat program pengawasan yang bernama *Bekaert Observation Program* dan pekerja juga dilengkapi dengan sarung tangan selama menggunakan mesin press. Berdasarkan risiko tersebut maka nilai *existing risk* adalah 250 dengan kategori *priority 1*. Penurunan risiko (*risk reduction*) sebesar 83,3%.

Untuk mengurangi risiko tersebut maka peneliti merekomendasikan dibuatnya *Standard Operating Procedure (SOP)* yang jelas dan ketat untuk penggunaan mesin press. Selain itu perlunya pengawasan rutin secara berkala pada pekerja. Pengecekan dan perawatan mesin dan fungsi sensor juga sangat diperlukan serta perlunya *guarding* di sisi kanan dan kiri mesin yang disesuaikan dengan kondisi dan posisi kerja karena sensor hanya berfungsi mendeteksi benda dari arah depan mesin. Berdasarkan rekomendasi tersebut maka didapatkan nilai *predictive risk* sebesar 50 dengan kategori *priority 3*.

3. Bising

Risiko bising terjadi ketika mesin *debouring* sedang beroperasi menghaluskan permukaan produk. Nilai *basic risk* untuk risiko ini adalah 250 dengan kategori *priority 1*. Nilai *Consequences* (C) = 25 (*very serious*) karena dapat merusak kualitas pendengaran pekerja dan bersifat permanen. Selain itu juga menimbulkan ketidaknyamanan saat bekerja. *Exposure* (E) = 10 (*frequently*) karena terjadi lebih dari satu kali dalam sehari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya cukup kecil karena mesin dapat bekerja sendiri secara otomatis.

Pengendalian yang telah dilakukan oleh perusahaan adalah membatasi pekerja dengan cara meletakkan mesin *debouring* di dalam ruang tertutup. Program pengawasan yang bernama *Bekaert Observation Program*, pemasangan *safety sign* di depan ruangan *debouring* serta pekerja diharuskan untuk menggunakan alat pelindung diri (*earmuff*)

ketika memasuki ruang *debouring*. Berdasarkan pengendalian tersebut maka didapatkan nilai *existing risk* sebesar 90 dengan kategori priority 3, Penurunan risiko (*risk reduction*) sebesar 64%.

Rekomendasi yang diberikan adalah membuat *Standard Operating Procedure (SOP)* dan *work permit* untuk memasuki ruang *debouring*. Selain itu diperlukan pengawasan secara rutin dan kedisplinan pekerja dalam menggunakan alat pelindung diri ketika berada di dalam ruang *debouring*. Berdasarkan rekomendasi tersebut maka didapatkan nilai predictive risk sebesar 15 dengan kategori *acceptable*.

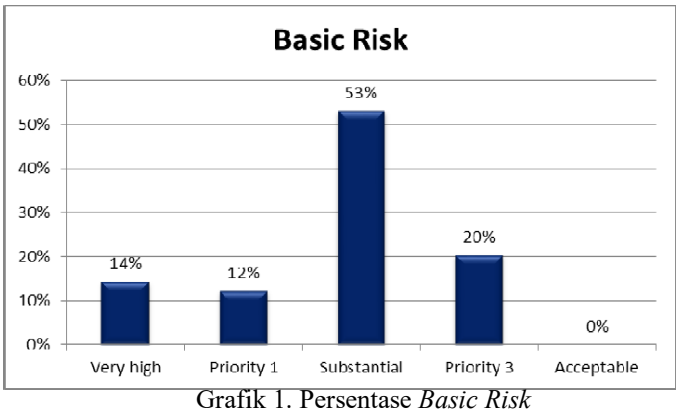
4. Postur janggal

Postur janggal dapat terjadi ketika pekerja melakukan pengemasan produk ke dalam kardus-kardus sebelum dikirimkan. Pengemasan produk dilakukan dalam bungkuk untuk memasukkan dan mengatur posisi produk di dalam kardus. Nilai *basic risk* untuk risiko ini adalah 150 dengan kategori *substantial* dengan nilai *Consequences* (C) = 15 (*serious*) karena dapat mengakibatkan nyeri dan cedera pada tulang pinggang. *Exposure* (E) = 10 (*frequently*) karena dilakukan pekerja secara berkali-kali dalam satu hari. *Likelihood/Probability* (P) = 1 (*remotely possible*) karena kemungkinan terjadinya risiko ini cukup kecil. Belum terdapat pengendalian yang dilakukan perusahaan untuk risiko ini. Maka nilai *existing risk* sama dengan nilai *basic risk* yaitu 150 dengan kategori *substantial.*

Untuk mengurangi risiko postur janggal karena posisi bungkuk, maka peneliti merekomendasikan agar pekerja melakukan *stretching* 1 kali dalam 1 jam untuk melemaskan otot-otot tubuh agar tidak kaku. Selain itu sebaiknya pengemasan dilakukan dengan posisi yang benar agar pekerja tidak harus terlalu membungkuk. Nilai *predictive risk* dari rekomendasi tersebut adalah 15 dengan kategori *acceptable*.

Persentase Nilai *Basic Risk, Existing Risk* dan *Predictive Risk*

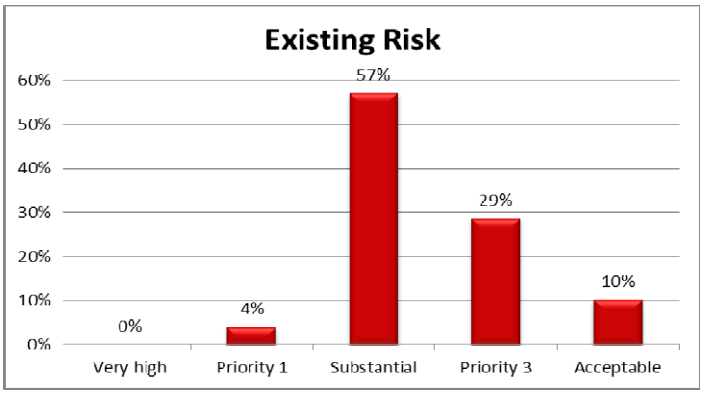
1. Basic Risk



Grafik 1. Persentase *Basic Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *basic risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 14% (7 aktivitas), kategori *priority 1* sebesar 12% (6 aktivitas), kategori *substantial* sebesar 53% (23 aktivitas), kategori *priority 3* sebesar 20% (10 aktivitas) dan kategori *acceptable* sebesar 0% (0 aktivitas).

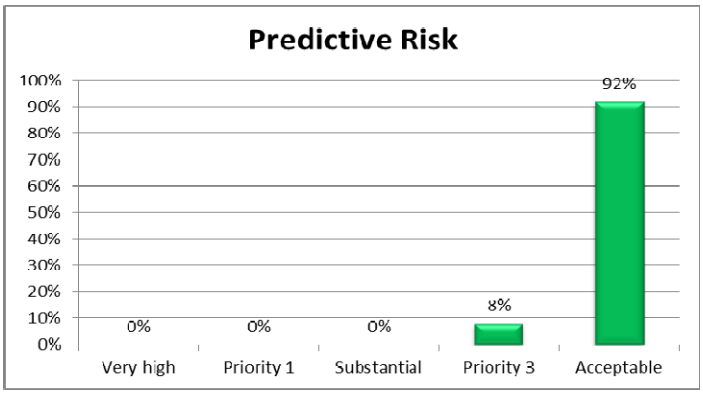
2. Existing Risk



Grafik 2. Persentase *Existing Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *existing risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 4% (2 aktivitas), kategori *substantial* sebesar 57% (28 aktivitas), kategori *priority 3* sebesar 29% (14 aktivitas) dan kategori *acceptable* sebesar 10% (5 aktivitas).

3. Predictive Risk



Grafik 3. Persentase *Predictive Risk*

Dari hasil analisis peneliti, maka didapatkanlah gambaran mengenai nilai *predictive risk* dari semua bagian dan proses produksi *spin pack* di PT BAF tahun 2013. Untuk kategori risiko *very high* sebesar 0% (0 aktivitas), kategori *priority 1* sebesar 0% (0 aktivitas), kategori *substantial* sebesar 0% (0 aktivitas), kategori *priority 3* sebesar 8% (4 aktivitas) dan kategori *acceptable* sebesar 92% (45 aktivitas).

3. SIMPULAN

Berdasarkan hasil dan analisis penelitian mengenai risiko keselamatan dan kesehatan kerja pada proses produksi *spin pack* di PT BAF tahun 2013, maka didapatkanlah simpulan sebagai berikut:

1. Terdapat 8 proses kerja pada proses produksi *spin pack*. Proses kerja tersebut terdiri dari *preparation* (persiapan material), *press I* (pencetakan), *debouring* (penghalusan), *assembling* (perakitan), *press II* (pressing), *quality control* (pengecekan), *cleaning* (pembersihan), *packing* (pengemasan).
2. Jenis bahaya paling dominan pada aktivitas proses produksi *spin pack* adalah bahaya mekanis seperti tertusuk, tergores, tersayat dan terpotong.
3. Ditemukan 7 risiko dalam 6 aktivitas dengan kategori *very high* pada *basic risk* di proses produksi *spin pack*. Aktivitas tersebut adalah pengambilan *tools*, pemasangan *tools,* pencetakan produk, membuka dan mengembalikan *tools* serta pada proses *pressing*.
4. Untuk *existing risk*, tidak ditemukan aktivitas dengan kategori *very high* namun terdapat 2 aktivitas dengan kategori *priority 1* yang membutuhkan perbaikan sesegera mungkin. Aktivitas tersebut yaitu pada proses pencetakan dan proses *pressing*.
5. Secara umum pengendalian yang sudah dilakukan oleh perusahaan adalah dengan

mengadakan program pengawasan yang disebut dengan *Bekaert Observation Program,* pemasangan *safety sign* dan penyediaan alat pelindung diri.

6. Berdasarkan program pengendalian yang sudah dilakukan perusahaan, berbagai risiko yang ada dapat dikurangi dengan persentase *risk reduction* antara 40% - 93,3%.
7. Pada *predictive risk*, sebagian besar risiko dapat diturunkan pada kategori *acceptable*. Namun masih terdapat 4 aktivitas yang berada pada kategori *priority 3*.

4. DAFTAR PUSTAKA

Alfiah, Suzi. 2012. *Penilaian Risiko Keselamatan dan Kesehatan Kerja pada Kegiatan Operasi dan Produksi PT Pertamina Geothermal Energy Area Lahendong Tahun 2012*. Skripsi. Depok: Fakultas Kesehatan Masyarakat Universitas Indonesia.

"Angka Kecelakaan Kerja Lima Tahun Terakhir Meningkat". http://www.poskotanews.com/2012/06/01/angka-kecelakaan-kerja-lima-tahun-terahir-cendrung-naik/ (diakses pada 14 Maret 2013 pukul 15.33 WIB)

European Agency for Safety and Health at Work. "Definitions". https://osha.europa.eu/en/topics/riskassessment/definitions

Jamsostek. "Setiap Hari Ada 9 Peserta Jamsostek Tewas Kecelakaan Kerja". http://www.jamsostek.co.id/content/news.php?id=3957

Analisis Resiko Pada Akademik Management System Universitas Bina Insan Lubuk Linggau

Fido Rizki[1], Safta Hastini[2], Singgih Hanata Putra[3], Febriansyah[4], Winata Nugraha[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di Universitas Bina Insan. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.

Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan

aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. Universitas Bina Insan merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan Universitas Bina Insan. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di Universitas Bina Insan. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai

kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	**Resiko**
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang

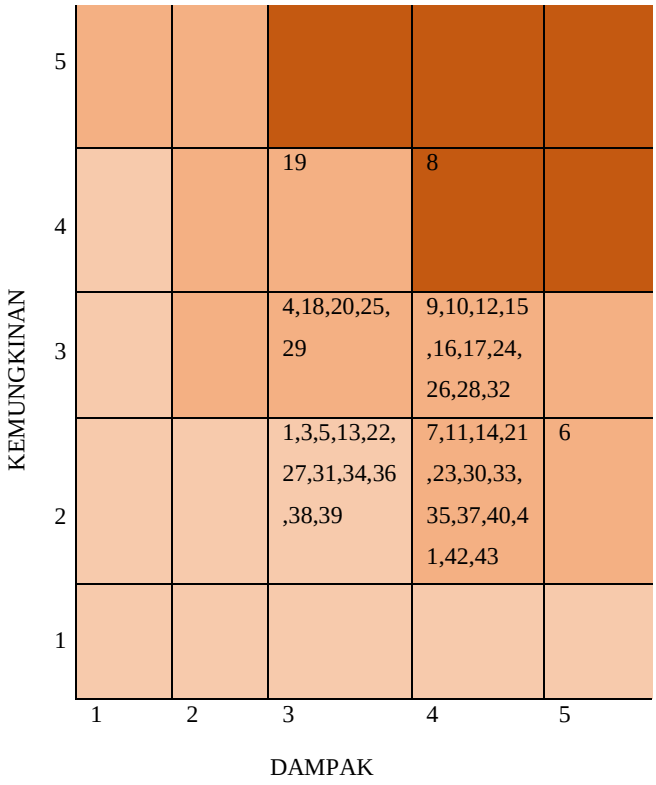
telah ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu

Database crash. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low / Rendah)	1	Resiko Kerusakan akibat bencana alamt seperti kebakaaran banjir, gempa	NTP Server
	2	Pencurian Perangkat	NTP Server

	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dll. Manfaat penggunaan database

server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1) Apa pemicu terjadinya database server down pada sistem AMS?
2) Seberapa sering database server down tersebut terjadi pada sistem AMS?
3) Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

1) Overheat
2) Overcapacity
3) Overload
4) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
   - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin sehingga perangkat terhindar dari resiko akibat overheat.
   - Menghilangkan log yang menggunakan kapasitas yang besar
   - Melakukan restart database service.

- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi-manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-manajemen.[Accessed 16 November 2014].

[9] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].

[10] [Online].Available:http://fisipuin.satugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.academia.edu/5170798/Uji_Validitas_Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri01.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed25 Februari 2015].
[15] [Online].Available:https://avicennaedu.wordpress.com/2013/03/26/resikomanajemen-risk-management/. [Accessed 10 Juni 2015].

1. Pendahuluan

Enterprise risk management. Secara singkat, pengertian dan definisi risiko cukup beragam. Sumber risiko pada dasarnya adalah ketidakpastian. Ketidakpastian memunculkan risiko. Proses manajemen risiko adalah tahapan yang dilakukan untuk mengelola risiko secara sistematis. *Enterprise Risk Management* (ERM) adalah manajemen risiko dalam suatu organisasi. Modul satu berikut ini membicarakan lebih lanjut ketiga konsep dasar manajemen risiko tersebut. Setelah mempelajari Modul 1 ini, secara umum Anda diharapkan dapat menjelaskan gambaran secara umum mengenai risiko dan pengelolaan risiko tersebut. Secara khusus, setelah mempelajari Modul 1 ini, Anda diharapkan bisa menjelaskan:

1. Beberapa pengertian dan definisi risiko.
2. Kondisi ketidakpastian sebagai sumber risiko.
3. Beberapa contoh kerugian yang dialami organisasi akibat kegagalan mengelola risiko.
4. Proses atau tahapan dalam pengelolaan risiko.
5. *Enterprise Risk Management* (pengelolaan risiko dalam suatu organisasi).
6. Komponen-komponen dalam *Enterprise Risk Management.*

A. RISIKO DAN KONDISI KETIDAKPASTIAN

Risiko merupakan kata yang sudah kita dengar hampir setiap hari. Biasanya kata tersebut mempunyai konotasi yang negatif, sesuatu yang tidak kita sukai, sesuatu yang ingin kita hindari. Sebagai contoh, jika kita jalan keluar dengan mobil, maka ada risiko mobil kita bertabrakan dengan mobil lainnya (kejadian yang tidak kita inginkan). Jika kita mempunyai saham, ada risiko harga saham yang kita pegang turun nilainya, sehingga kita tidak memperoleh keuntungan (kejadian yang tidak kita harapkan). Jika bank memberikan kredit kepada suatu perusahaan, maka ada kemungkinan perusahaan tersebut gagal bayar (tidak membayar bunga dan/atau cicilan pinjamannya).

Apa yang dimaksud dengan risiko? Risiko bisa didefinisikan dengan berbagai cara. Sebagai contoh, risiko bisa didefinisikan sebagai kejadian yang merugikan. Definisi lain yang sering dipakai untuk analisis investasi, adalah kemungkinan hasil yang diperoleh menyimpang dari yang diharapkan. Deviasi standar merupakan alat statistik yang bisa digunakan untuk mengukur penyimpangan, karena itu deviasi standar bisa dipakai untuk mengukur risiko. Pengukuran yang lain adalah menggunakan probabilitas. Sebagai contoh, pengemudi kendaraan orang muda lebih sering mengalami kecelakaan dibandingkan dengan orang dewasa. Probabilitas terjadinya kecelakaan untuk

orang muda lebih tinggi dibandingkan dengan untuk orang dewasa. Karena itu risiko kecelakaan untuk orang muda lebih tinggi dibandingkan untuk orang dewasa.

Kenapa muncul suatu risiko? Risiko berkaitan erat dengan kondisi ketidakpastian. Risiko muncul karena ada kondisi ketidakpastian. Praktis kita menghadapi banyak ketidakpastian di dunia ini. Sebagai contoh, hari ini bisa hujan, bisa juga tidak hujan. Investasi kita bisa mendatangkan keuntungan (harga naik), bisa juga menyebabkan kerugian (harga turun). Kepastian dalam dunia ini adalah ketidakpastian itu sendiri. Ketidakpastian tersebut menyebabkan munculnya risiko. Ketidakpastian itu sendiri ada banyak

tingkatannya. Tabel berikut ini menunjukkan tingkatan ketidakpastian dengan karakteristiknya.

Tabel 1.1.

Tingkatan Ketidakpastian

TINGKAT KETIDAKPASTIAN	KARAKTERISTIK	CONTOH
TIDAK ADA (PASTI)	HASIL BISA DIPREDIKSI DENGAN PASTI	HUKUM ALAM
KETIDAKPASTIAN OBJEKTIF	HASIL BISA DIIDENTIFIKASI DAN PROBABILITAS DIKETAHUI	PERMAINAN DADU, KARTU
KETIDAKPASTIAN SUBJEKTIF	HASIL BISA DIIDENTIFIKASI TAPI PROBABILITAS TIDAK DIKETAHUI	KEBAKARAN, KECELAKAAN MOBIL, INVESTASI
SANGAT TIDAK PASTI	HASIL TIDAK BISA DIIDENTIFIKASI DAN PROBABILITAS TIDAK DIKETAHUI	EKSPLORASI ANGKASA

Pada tingkatan pertama, kondisi kepastian sangat tinggi. Hasil bisa diprediksi dengan relatif pasti. Hukum alam merupakan contoh kepastian tersebut. Sebagai contoh, kita bisa memprediksi dengan pasti bahwa bumi mengitari matahari selama 360 hari (satu tahun). Tingkatan selanjutnya adalah ketidakpastian objektif, dengan contoh adalah dadu, jika kita melempar dadu, ada enam kemungkinan yaitu angka 1, 2, 3, 4, 5, dan 6 (ada enam kemungkinan hasil). Kita bisa menghitung probabilitas masing-masing angka untuk keluar, yaitu 1/6.

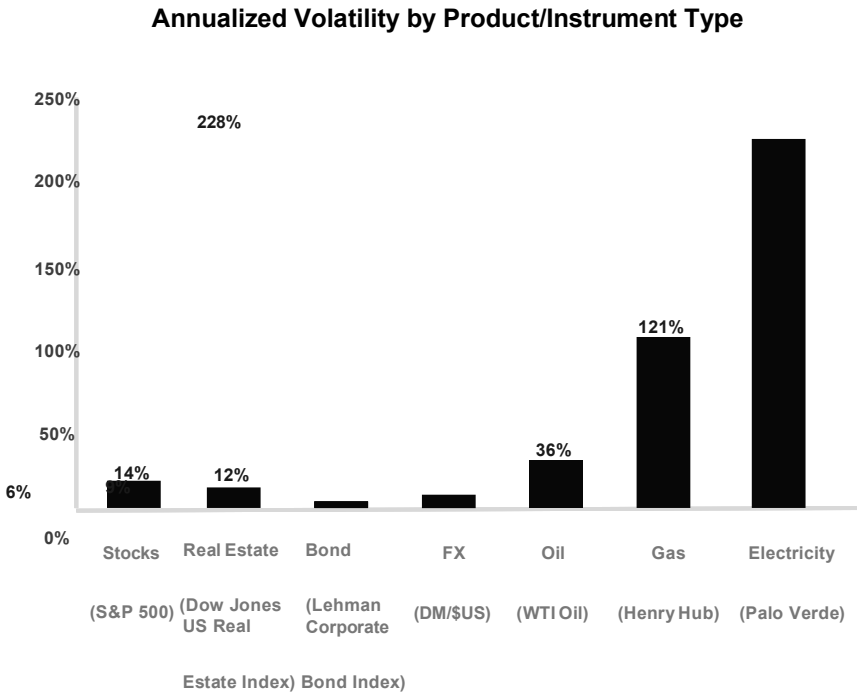
Tingkatan berikutnya adalah ketidakpastian subjektif, dengan contoh adalah kecelakaan mobil. Identifikasi hasil dan probabilitas (kemungkinan) yang berkaitan dengan kecelakaan mobil lebih sulit dilakukan. Sebagai contoh, jika kita pergi keluar dengan mobil, berapa besar probabilitas kita mengalami kecelakaan mobil? Dan jika terjadi kecelakaan, kerusakan atau kerugian yang bagaimana yang akan kita dapatkan? Tidak mudah untuk menjawab pertanyaan tersebut. Tingkatan berikutnya adalah kondisi sangat tidak pasti,

dengan contoh eksplorasi angkasa. Kita tidak tahu apa hasil yang akan diperoleh dari eksplorasi angkasa, apakah akan bertemu dengan makhluk asing (*alien*), ataukah menemukan planet yang mirip bumi, atau apa

yang akan kita temukan. Sangat sulit memprediksi atau mengidentifikasi hasil yang barangkali bisa diperoleh dari eksplorasi angkasa seperti itu. Tentu saja juga akan sangat sulit menentukan probabilitas untuk masing-masing kemungkinan hasil tersebut.

Ketidakpastian bisa tercermin dari fluktuasi pergerakan yang tinggi; Semakin tinggi fluktuasi, semakin besar tingkat ketidakpastiannya. Bagan berikut ini menunjukkan fluktuasi harga beberapa instrumen (dihitung berdasarkan deviasi standar tahunan). Terlihat bahwa semua harga instrumen berfluktuasi. Sebagai contoh, saham mempunyai fluktuasi sebesar 14%, sementara harga listrik mempunyai fluktuasi sebesar 228%.

Hasil empiris pada bagan di atas menunjukkan bahwa di dunia ini semuanya serba tidak pasti. Saham, valas (FX), harga minyak, sampai dengan harga listrik, mempunyai fluktuasi, meskipun dengan tingkat fluktuasi yang berbeda-beda. Kepastian adalah ketidakpastian itu sendiri. Dengan demikian risiko ada di mana-mana, mencakup semua instrumen.



Gambar 1.1.
Fluktuasi Tahunan Berdasarakn Tipe Instrumen

Selain itu, fluktuasi harga cenderung semakin meningkat dari tahun ke tahun. Sebagai ilustrasi, Indonesia mengalami perubahan sistem kurs dari tetap menjadi mengambang pada pertengahan tahun 1997. Sebelum krisis pada tahun 1997, Indonesia menganut sistem kurs tetap, dengan menetapkan kurs Rp/$ pada tingkat sekitar Rp2.500/$. Pada pertengahan tahun 1997, untuk mengurangi tekanan terhadap kurs karena ada krisis ekonomi, pemerintah mengambangkan kurs Rp/$. Sistem kurs mengambang tersebut masih berlaku sampai saat ini. Kurs Rp/$ tidak lagi tetap, tetapi bisa berubah tergantung mekanisme pasar. Sistem kurs mengambang tersebut mengakibatkan fluktuasi kurs Rp/$ jauh lebih tinggi dibandingkan dengan fluktuasi kurs Rp/$ pada sistem kurs tetap.

Mengapa fluktuasi cenderung meningkat? Ada beberapa faktor yang mendorong peningkatan fluktuasi tersebut, seperti:

1. Globalisasi dunia.
2. Liberalisasi dunia.
3. Proses Informasi yang semakin cepat, reaksi investor yang semakin cepat.

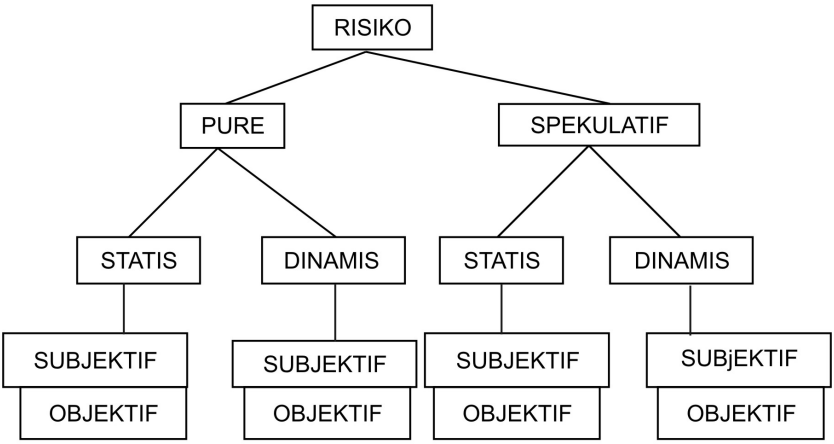
Globalisasi dunia membuat keterkaitan perekonomian dunia lebih erat. Kejadian di suatu negara akan lebih cepat mempengaruhi negara lain. Dengan kondisi seperti itu, fluktuasi akan cenderung meningkat. Liberalisasi dunia (membuka pasar domestik terhadap investor asing) mempunyai efek yang sama dengan globalisasi. Hambatan antar negara menjadi berkurang. Aliran modal menjadi lebih mudah untuk masuk atau keluar. Hal semacam ini akan meningkatkan fluktuasi dunia. Sebagai ilustrasi, krisis ekonomi di Thailand pada tahun 1997, memicu terjadinya krisis ekonomi di negara- negara sekitarnya (Indonesia, Filipina, Malaysia) dengan cepat. Investor dengan cepat memindahkan dananya dari Thailand dan negara-negara sekitarnya ke negara-negara lain yang dianggap lebih aman. Terbukanya perekonomian dunia memungkinkan pergerakan modal yang cepat semacam itu.

Teknologi yang semakin maju membuat investor atau pelaku pasar semakin canggih dalam memproses informasi. Kecanggihan tersebut akan mendorong pelaku pasar untuk lebih cepat memperoleh informasi dan bertindak lebih cepat atas informasi tersebut. Kemudahan informasi dan reaksi yang cepat dari investor akan mendorong fluktuasi harga yang semakin tinggi.

Globalisasi, liberalisasi, dan teknologi yang semakin canggih akan semakin meningkatkan fluktuasi harga, semakin meningkatkan ketidakpastian. Fluktuasi tersebut ternyata praktis dialami oleh semua atau sebagian besar instrumen keuangan atau komoditas di dunia. Dengan demikian bisa diambil kesimpulan bahwa risiko ada di mana-mana, dan risiko cenderung semakin meningkat dari tahun ke tahun.

B. TIPE-TIPE RISIKO

Risiko beragam jenisnya, mulai dari risiko kecelakaan, kebakaran, risiko kerugian, fluktuasi kurs, perubahan tingkat bunga, dan lainnya. Untuk memudahkan pemahaman dan analisis terhadap risiko, kita bisa memetakan atau mengelompokkan risiko-risiko tersebut. Salah satu cara untuk mengelompokkan risiko adalah dengan melihat tipe-tipe risiko. Bagan berikut ini menunjukkan bahwa risiko bisa dikelompokkan ke dalam dua tipe risiko: risiko murni dan risiko spekulatif, risiko subjektif dan objektif, dan dinamis dan statis.



Gambar 1.2.
Kategorisasi Risiko

Risiko bisa dikelompokkan ke dalam risiko murni dan risiko spekulatif dengan penjelasan sebagai berikut ini.

1. Risiko murni (*pure risks*) adalah risiko di mana kemungkinan kerugian ada, tetapi kemungkinan keuntungan tidak ada. Jadi kita membicarakan potensi kerugian untuk risiko tipe ini. Beberapa contoh risiko tipe ini adalah risiko kecelakaan, kebakaran, dan semacamnya. Contoh lain adalah risiko banjir menghantam rumah kita. Kejadian seperti itu akan merugikan kita. Tetapi rumah berdiri di tempat tertentu tidak secara langsung akan mendatangkan keuntungan tertentu. Jika terjadi kebakaran atau banjir, di samping individu yang terkena dampaknya, masyarakat secara keseluruhan juga akan dirugikan. Asuransi biasanya lebih banyak berurusan dengan risiko murni.
2. Risiko spekulatif adalah risiko di mana kita mengharapkan terjadinya kerugian dan juga keuntungan. Potensi kerugian dan keuntungan dibicarakan dalam jenis risiko ini. Contoh tipe risiko ini adalah usaha bisnis. Dalam kegiatan bisnis, kita mengharapkan keuntungan, meskipun ada potensi kerugian. Contoh lain adalah jika kita memegang (membeli) saham. Harga pasar bisa meningkat (kita memperoleh keuntungan), bisa juga analisis kita salah, harga saham bukannya meningkat, tetapi malah turun (kita memperoleh kerugian). Risiko spekulatif juga bisa dinamakan sebagai risiko bisnis. Kerugian akibat risiko spekulatif akan merugikan individu tertentu, tetapi akan menguntungkan individu lainnya. Misalkan suatu perusahaan mengalami kerugian karena penjualannya turun, perusahaan lain barangkali akan memperoleh keuntungan dari situasi tersebut. Secara total, masyarakat tidak dirugikan oleh risiko spekulatif tersebut.

Di samping kategorisasi murni dan spekulatif, risiko juga bisa dibedakan antara risiko yang dinamis dan yang statis.

1. Risiko statis muncul dari kondisi keseimbangan tertentu. Sebagai contoh, risiko terkena petir merupakan risiko yang muncul dari kondisi alam yang tertentu. Karakteristik risiko ini praktis tidak berubah dari waktu ke waktu.
2. Risiko dinamis muncul dari perubahan kondisi tertentu. Sebagai contoh, perubahan kondisi masyarakat, perubahan teknologi, memunculkan jenis-jenis risiko baru. Misal, jika masyarakat semakin kritis, sadar akan haknya, maka risiko hukum (*legal risk*) yang muncul karena masyarakat

lebih berani mengajukan gugatan hukum (*sue*) terhadap perusahaan, akan semakin besar.

Risiko juga bisa dikelompokkan ke dalam risiko subjektif dan objektif dengan penjelasan sebagai berikut ini.

1. Risiko objektif adalah risiko yang didasarkan pada observasi parameter yang objektif. Sebagai contoh, fluktuasi harga atau tingkat keuntungan investasi di pasar modal bisa diukur melalui standar deviasi, misal standar deviasi *return* saham adalah 25% per tahun.
2. Risiko subjektif berkaitan dengan persepsi seseorang terhadap risiko. Dengan kata lain, kondisi mental seseorang akan menentukan kesimpulan tinggi rendahnya risiko tertentu. Sebagai contoh, untuk standar deviasi *return* pasar yang sama sebesar 25%, dua orang dengan kepribadian berbeda akan mempunyai cara pandang yang berbeda. Orang yang konservatif akan menganggap risiko investasi di pasar modal terlalu tinggi. Sementara bagi orang yang agresif, risiko investasi di pasar modal dianggap tidak terlalu tinggi. Perhatikan bahwa kedua orang tersebut melihat pada risiko objektif yang sama, yaitu standar deviasi *return* sebesar 25% per tahun.

Berikut ini contoh-contoh risiko yang biasa dihadapi oleh suatu organisasi. Risiko-risiko tersebut dikelompokkan ke dalam risiko murni dan spekulatif.

Tabel 1.2.
Contoh-contoh Risiko Murni

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko Aset Fisik	Risiko yang terjadi karena kejadian tertentu berakibat buruk (kerugian) pada aset fisik organisasi.	Kebakaran yang melanda gudang atau bangunan perusahaan. Banjir mengakibatkan kerusakan pada bangunan dan peralatan
Risiko karyawan	Risiko karena karyawan organisasi mengalami peristiwa yang merugikan	Kecelakaan kerja mengakibatkan karyawan cedera, kegiatan operasional perusahaan terganggu
Risiko legal	Risiko kontrak tidak sesuai yang diharapkan, dokumentasi yang tidak benar	Terjadi perselisihan sehingga perusahaan lain menuntut ganti rugi yang signifikan

Tabel 1.3.

Contoh-Contoh Risiko Spekulatif

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko pasar	Risiko yang terjadi dari pergerakan harga atau volatilitas harga pasar	Harga pasar saham dalam portofolio perusahaan mengalami penurunan, yang mengakibatkan kerugian yang dialami perusahaan.
Risiko kredit	Risiko karena *counter party* gagal memenuhi kewajibannya kepada perusahaan	Debitur tidak bisa membayar cicilan dan bunga hutang, sehingga perusahaan mengalami kerugian. Piutang dagang tidak terbayar.
Risiko Likuiditas	Risiko tidak bisa memenuhi kebutuhan kas, risiko tidak bisa menjual dengan cepat karena ketidaklikuidan atau gangguan pasar	Perusahaan tidak mempunyai kas untuk membayar kewajibannya (misal melunasi hutang). Perusahaan terpaksa menjual tanah dengan harga murah (di bawah standar) karena sulit menjual tanah tersebut (tidak likuid), padahal perusahaan membutuhkan kas dengan cepat.
Risiko operasional	Risiko kegiatan operasional tidak berjalan lancar dan mengakibatkan kerugian: kegagalan sistem, human error, pengendalian dan prosedur yang kurang	Komputer perusahaan terkena virus sehingga operasi perusahaan terganggu. Prosedur pengendalian perusahaan tidak memadai sehingga terjadi pencurian barang-barang yang dimiliki perusahaan.

Pembagian risiko ke dalam dua tipe, yaitu risiko murni dan risiko spekulatif, barangkali tidak sepenuhnya memuaskan. Ada beberapa jenis risiko yang barangkali bisa masuk ke dalam risiko murni maupun spekulatif. Sebagai contoh, risiko tuntutan hukum bisa dimasukkan ke dalam risiko murni, tetapi jika dilihat sebagai konsekuensi kegiatan bisnis, maka risiko tersebut bisa dimasukkan ke dalam risiko spekulatif. Pembagian semacam itu bukan 'harga mati'. Pembagian semacam itu diharapkan memudahkan kita memahami jenis-jenis risiko dan karakteristiknya.

C. PROSES MANAJEMEN RISIKO

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari. Jika

risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa

mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko. Jika organisasi tersebut tidak bisa mengelola risiko dengan baik, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Karena itu risiko yang dihadapi oleh organisasi tersebut juga harus dikelola, agar organisasi bisa bertahan, atau barangkali mengoptimalkan risiko. Perusahaan sering kali secara sengaja mengambil risiko tertentu, karena melihat potensi keuntungan dibalik risiko tersebut.

Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko.
2. Evaluasi dan Pengukuran Risiko, dan
3. Pengelolaan risiko.

1. Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang dihadapi oleh suatu organisasi. Banyak risiko yang dihadapi oleh suatu organisasi, mulai dari risiko penyelewengan oleh karyawan, risiko kejatuhan meteor atau komet, dan lainnya. Ada beberapa teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh, kompor ditaruh dekat penyimpanan minyak tanah. Api merupakan sumber risiko, kompor yang ditaruh dekat minyak tanah merupakan kondisi yang meningkatkan terjadinya kecelakaan, bangunan yang bisa terbakar merupakan *eksposur* yang dihadapi perusahaan. Misalkan terjadi kebakaran, kebakaran merupakan peristiwa yang merugikan (peril). Identifikasi semacam dilakukan dengan melihat sekuen dari sumber risiko sampai ke terjadinya peristiwa yang merugikan. Pada beberapa situasi, risiko yang dihadapi oleh perusahaan cukup standar. Sebagai contoh, bank menghadapi risiko terutama adalah risiko kredit (kemungkinan debitur tidak melunasi hutangnya). Untuk bank yang juga aktif melakukan perdagangan sekuritas, maka bank tersebut akan menghadapi risiko pasar. Setiap bisnis akan menghadapi risiko yang berbeda-beda karakteristiknya.

2. Evaluasi dan Pengukuran Risiko

Langkah berikutnya adalah mengukur risiko tersebut dan mengevaluasi risiko tersebut. Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk 'mengukur' risiko tersebut.

Ada beberapa teknik untuk mengukur risiko tergantung jenis risiko tersebut. Sebagai contoh kita bisa memperkirakan probabilitas (kemungkinan) risiko atau suatu kejadian jelek terjadi. Dengan probabilitas tersebut kita berusaha 'mengukur' risiko. Sebagai contoh, ada risiko perusahaan terkena jatuhan meteor atau komet, tetapi probabilitas risiko semacam itu sangat kecil (0,000000001). Karena itu risiko tersebut tidak perlu diperhatikan. Contoh lain adalah risiko kebakaran dengan probabilitas (misal) 0,6. Karena probabilitas yang tinggi, maka risiko kebakaran perlu diberi perhatian ekstra. Contoh tersebut menunjukkan bahwa dengan menggunakan teknik probabilitas kita bisa melakukan prioritisasi risiko, sehingga kita bisa lebih memfokuskan pada risiko yang mempunyai kemungkinan yang besar untuk terjadi.

Contoh lain adalah membuat matriks dengan sumbu mendatar adalah probabilitas terjadinya risiko, dan sumbu vertikal adalah tingkat keseriusan konsekuensi risiko tersebut (*severity*, atau besarnya kerugian yang timbul akibat risiko tersebut). Setiap risiko bisa dievaluasi kemudian dimasukkan ke dalam matriks tersebut. Sebagai contoh, risiko kebakaran mempunyai probabilitas 0,6 (tinggi). Jika kebakaran terjadi, maka kerugian yang diakibatkan akan besar juga (tinggi). Dengan demikian risiko kebakaran akan ditempatkan pada kuadran probabilitas tinggi dan *severity* tinggi. Selanjutnya langkah yang lebih tepat bisa dirumuskan. Sebagai contoh, untuk risiko kebakaran seperti itu, langkah yang lebih aktif bisa ditujukan untuk menangani risiko kebakaran tersebut.

Untuk risiko lain, evaluasi dan pengukuran yang berbeda bisa dilakukan. Sebagai contoh, risiko perubahan tingkat bunga bisa diukur dengan teknik duration (durasi). Modul identifikasi dan pengukuran risiko spekulatif akan banyak membicarakan pengukuran risiko perubahan tingkat bunga. Risiko pasar bisa dievaluasi dengan menggunakan teknik VAR (*Value At Risk*). Pemahaman kita terhadap beberapa risiko sudah cukup baik sehingga teknik pengukuran risiko tersebut sudah berkembang. Sementara pemahaman kita terhadap risiko lain belum begitu baik sehingga teknik pengukuran risiko tersebut belum begitu berkembang.

Teknik lain untuk mengukur risiko adalah dengan mengevaluasi dampak risiko tersebut terhadap kinerja perusahaan.

3. Pengelolaan Risiko

Setelah analisis dan evaluasi risiko, langkah berikutnya adalah mengelola risiko. Risiko harus dikelola. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misal kerugian yang besar. Risiko bisa dikelola dengan berbagai cara, seperti penghindaran, ditahan (*retention*), diversifikasi, atau ditransfer ke pihak lainnya. Erat kaitannya dengan manajemen risiko adalah pengendalian risiko (*risk control*), dan pendanaan risiko (*risk financing*).

a. Penghindaran. Cara paling mudah dan aman untuk mengelola risiko adalah menghindar. Tetapi cara semacam ini barangkali tidak optimal. Sebagai contoh, jika kita ingin memperoleh keuntungan dari bisnis, maka mau tidak mau kita harus keluar dan menghadapi risiko tersebut. Kemudian kita akan mengelola risiko tersebut.
b. Ditahan (*Retention*). Dalam beberapa situasi, akan lebih baik jika kita menghadapi sendiri risiko tersebut (menahan risiko tersebut, atau *risk retention*). Sebagai contoh, misalkan seseorang akan keluar rumah membeli sesuatu dari supermarket terdekat, dengan menggunakan kendaraan. Kendaraan tersebut tidak diasuransikan. Orang tersebut merasa asuransi terlalu repot, mahal, sementara dia akan mengendarai kendaraan tersebut dengan hati-hati. Dalam contoh tersebut, orang tersebut memutuskan untuk menanggung sendiri (menahan, *retention*) risiko kecelakaan.
c. Diversifikasi. Diversifikasi berarti menyebar eksposur yang kita miliki sehingga tidak terkonsentrasi pada satu atau dua eksposur saja. Sebagai contoh, kita barangkali akan memegang aset tidak hanya satu, tetapi pada beberapa aset, misal saham A, saham B, obligasi C, properti, dan sebagainya. Jika terjadi kerugian pada satu aset, kerugian tersebut diharapkan bisa dikompensasi oleh keuntungan dari aset lainnya.
d. Transfer Risiko. Jika kita tidak ingin menanggung risiko tertentu, kita bisa mentransfer risiko tersebut ke pihak lain yang lebih mampu menghadapi risiko tersebut. Sebagai contoh, kita bisa membeli asuransi kecelakaan. Jika terjadi kecelakaan, perusahaan asuransi akan menanggung kerugian dari kecelakaan tersebut.

e. Pengendalian Risiko. Pengendalian risiko dilakukan untuk mencegah atau menurunkan probabilitas terjadinya risiko atau kejadian yang tidak kita inginkan. Sebagai contoh, untuk mencegah terjadinya kebakaran, kita memasang alarm asap di bangunan kita. Alarm tersebut merupakan salah satu cara kita mengendalikan risiko kebakaran.
f. Pendanaan Risiko. Pendanaan risiko mempunyai arti bagaimana 'mendanai' kerugian yang terjadi jika suatu risiko muncul. Sebagai contoh, jika terjadi kebakaran, bagaimana menanggung kerugian akibat kebakaran tersebut, apakah dari asuransi, ataukah menggunakan dana cadangan? Isu semacam itu masuk dalam wilayah pendanaan risiko.

Di samping proses manajemen risiko seperti yang disebutkan di muka, manajemen risiko suatu organisasi juga memerlukan infrastruktur baik keras maupun lunak. Sebagai contoh, manajemen risiko barangkali akan memerlukan sistem komputer untuk analisis risiko. Manajemen risiko juga memerlukan staf dan struktur organisasi yang tepat. Infrastruktur manajemen risiko tidak dibahas secara khusus dalam modul ini. Modul enam menyajikan ilustrasi bagaimana perusahaan terkemuka dunia mengembangkan manajemen risiko dalam organisasinya.

Enterprise Risk Management

Makhluk hidup secara natural akan mengantisipasi dan 'mengelola' risiko. Sebagai contoh, jika kita keluar mengendarai mobil, maka kita akan waspada dengan kondisi sekitarnya. Jika dari arah yang berlawanan ada mobil yang agak ke tengah jalannya, kita akan menghindari mobil tersebut dengan jalan mengendarainya agak ke kiri, supaya tidak terjadi tabrakan. Konon binatang mempunyai indera keenam yang bisa mendeteksi risiko lebih baik dibandingkan manusia. Pada waktu tsunami melanda wilayah Asia pada tahun 2004, binatang (gajah, dan sebagainya) yang menjadi korban tsunami jauh lebih kecil dibandingkan manusia. Binatang tersebut sepertinya mampu mendeteksi datangnya bahaya, kemudian menyingkir sebelum bahaya tersebut datang. Konon manusia dulu juga mempunyai kemampuan yang serupa, tetapi karena tidak banyak digunakan, karena manusia lebih banyak mengandalkan otak mereka, kemampuan indera keenam tersebut menghilang. Bagaimana dengan organisasi? Organisasi tidak mempunyai kemampuan mengelola risiko seperti halnya manusia atau makhluk hidup mengelola risiko, karena organisasi bukan makhluk hidup. Tugas dari manajer suatu organisasi adalah membuat agar organisasi bisa mengantisipasi dan mengelola risiko

sebagaimana halnya makhluk hidup mengelola risiko yang dihadapinya. Dengan kata lain, tugas manajer adalah membuat organisasi menjadi sadar risiko, sehingga risiko bisa diantisipasi dan dikelola dengan baik.

Tabel 1.4 berikut ini menyajikan konsekuensi merugikan jika suatu organisasi gagal mengelola risiko

Tabel 1.4.
Beberapa Contoh Kegagalan Mengelola Risiko

Tahun	Penjelasan
1997	Trader Bank Baring (Nick Leeson) membeli *instrument derivative* saham Jepang (futures Nikkei). Bank Baring adalah Bank dari Inggris. Ekonomi Jepang turun drastic karena ada bencana gempa Kobe. Akibatnya dia mengalami kerugian besar. Transaksi selanjutnya (jual opsi) tidak mengurangi kerugian, tetapi memperparah kerugian. Pada akhirnya Bank Baring mengalami kerugian sebesar $1,3 miliar. Bank Baring terpaksa bangkrut karena kerugiannya sudah melebihi modalnya.

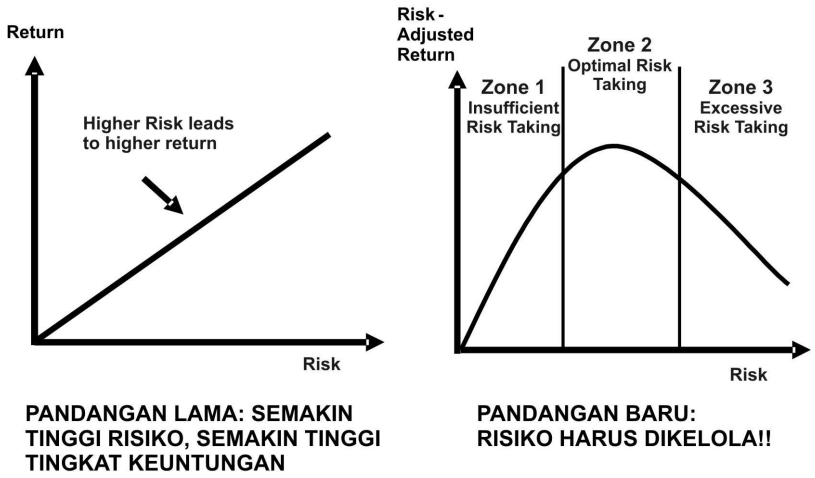
Tahun	Penjelasan
1997	Long Term Capital (LTC), perusahaan investasi di Amerika Serikat, mempunyai posisi pada mata uang Rusia Rubel yang cukup besar. Mereka memperkirakan Rusia tidak akan bangkrut. Tetapi Rusia ternyata bangkrut, mendeklarasikan tidak mampu dan tidak akan membayar hutang-hutangnya. Akibatnya *Long Term Capital* mengalami kerugian yang sangat besar, sekitar $3,5 miliar, dan pada akhirnya LTC terpaksa bangkrut.
2001	Enron merupakan perusahaan yang memperdagangkan energi (jual beli energi). Mereka juga masuk ke kontrak *derivative* energi. Usaha mereka cukup kompleks sehingga transparansi menjadi lebih sulit. Transparansi yang kompleks dimanfaatkan untuk menjalankan sistem akuntansi yang tidak wajar. Di samping itu Enron melakukan beberapa *manuever* agar laporan keuangannya kelihatan baik. Akhirnya investor mengetahui trik-trik mereka. Keuntungan mereka yang sesungguhnya ternyata tidak sebesar yang dilaporkan. Harga saham Enron jatuh dari $80 per lembar menjadi hanya $0,5. Mereka mempunyai kewajiban jangka pendek yang segera jatuh tempo. Mereka tidak bisa memperoleh bantuan dana. Tidak ada yang percaya dengan mereka. Enron akhirnya bangkrut.
1980-an	*Saving Loan* (S & L) *Association* (bank yang memberi pinjaman kredit rumah di Amerika Serikat) mempunyai struktur neraca: memberi kredit rumah dengan bunga tetap jangka panjang (misal 20 tahun), sementara memperoleh dana melalui deposito jangka pendek (misal 1 tahun). Struktur semacam itu rentan terhadap risiko perubahan tingkat bunga. Pada waktu tingkat bunga di Amerika Serikat naik signifikan pada tahun 1980-an, banyak S & L yang mengalami masalah dan puluhan S & L bangkrut karenanya.
1995	Bank Duta (Indonesia) mengalami kerugian yang sangat besar karena mereka melakukan perdagangan valas dan mengalami kerugian besar dari perdagangan valas tersebut.

Pertanyaan yang muncul adalah bisakah organisasi-organisasi di atas menghindari kerugian besar karena munculnya risiko-risiko tersebut? Manajemen risiko organisasi bertujuan menciptakan sistem atau mekanisme dalam organisasi sehingga risiko yang bisa merugikan organisasi bisa diantisipasi dan dikelola untuk tujuan meningkatkan nilai perusahaan.

Pentingnya pengelolaan risiko juga bisa dilihat melalui Bagan 1.1 berikut ini. Bagan 1.1 tersebut menggambarkan pandangan lama (sebelah kiri) dan baru (sebelah kanan) dalam kaitannya antara risiko dengan tingkat keuntungan. Pandangan lama menganggap ada hubungan positif antara risiko dengan tingkat keuntungan. Semakin tinggi risiko, akan semakin tinggi tingkat keuntungan yang diharapkan. Jika suatu organisasi ingin meningkatkan tingkat

keuntungannya, maka organisasi tersebut harus menaikkan risikonya.

Pandangan baru mengatakan bahwa hubungan antara risiko dengan tingkat keuntungan tidak bersifat linear, tetapi non-linear. Pada wilayah satu, risiko yang diambil oleh perusahaan terlalu kecil, sehingga keuntungan yang diperoleh juga kecil. Pada tahap ini, risiko masih bisa ditingkatkan untuk meningkatkan tingkat keuntungan. Contoh ekstrem situasi ini adalah jika manajer hanya tinggal di rumah, tidak pergi ke mana-mana. Dia bisa menghindari banyak risiko (risiko kecelakaan, dan sebagainya), tetapi dia juga tidak mendapatkan banyak keuntungan. Di tahap ini, pengelolaan risiko belum optimal.



Gambar 1.3.
Hubungan Risiko dan Tingkat Keuntungan (*Return*): Pandangan Lama dan Baru

Pada tahap berikutnya (zona 2), penambahan risiko tidak banyak meningkatkan tingkat keuntungan. Tahap ini merupakan tahap optimal. Tahap berikutnya (zona 3), risiko yang diambil organisasi terlalu tinggi, sehingga penambahan risiko akan berakibat negatif terhadap organisasi. Sebagai contoh, bank memberi pinjaman pada sektor-sektor yang risikonya terlalu tinggi, misal usaha burung walet, usaha perjudian. Risiko yang terlalu tinggi menjadi sulit untuk dikendalikan, sehingga bisa berakibat membahayakan dan merugikan perusahaan. Berdasarkan kerangka tersebut, pengelolaan risiko organisasi seharusnya berada pada wilayah tengah (zona 2), yang merupakan zona optimal.

Pengelolaan risiko yang digambarkan dalam bagan di atas bisa diilustrasikan melalui perjalanan dengan menggunakan kendaraan (mobil). Mobil yang berjalan terlalu lambat barangkali tidak menguntungkan, karena beberapa hal, misal terlalu lama, atau bahkan bisa membahayakan kendaraan lainnya. Mobil tersebut perlu dipacu lebih cepat. Jika mobil berjalan terlalu cepat (misal, ngebut), maka risiko bertabrakan atau kehilangan kendali menjadi semakin besar. Tentu saja hal ini tidak menguntungkan. Yang paling optimal adalah mobil berjalan dengan kecepatan optimal, yaitu cukup cepat tetapi bisa dikendalikan. Pengelolaan risiko bisa diilustrasikan sebagai kombinasi penekanan gas (mempercepat kendaraan) dan penekanan rem (memperlambat kendaraan). Kombinasi yang ideal bisa membuat mobil berjalan kencang tetapi tetap terkendali.

B. DEFINISI DAN PENGERTIAN MANAJEMEN RISIKO

Manajemen risiko organisasi adalah suatu sistem pengelolaan risiko yang dihadapi oleh organisasi secara komprehensif untuk tujuan meningkatkan nilai perusahaan. Meskipun pengertian manajemen risiko organisasi adalah seperti yang disebutkan di atas, tetapi ada banyak definisi dan pengertian manajemen risiko organisasi. Berikut ini beberapa definisi manajemen risiko organisasi.

Manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi, untuk mengelola, memonitor, dan mengendalikan eksposur organisasi terhadap risiko (SBC Warburg, *The Practice of Risk Management*, Euromoney Book, 2004)

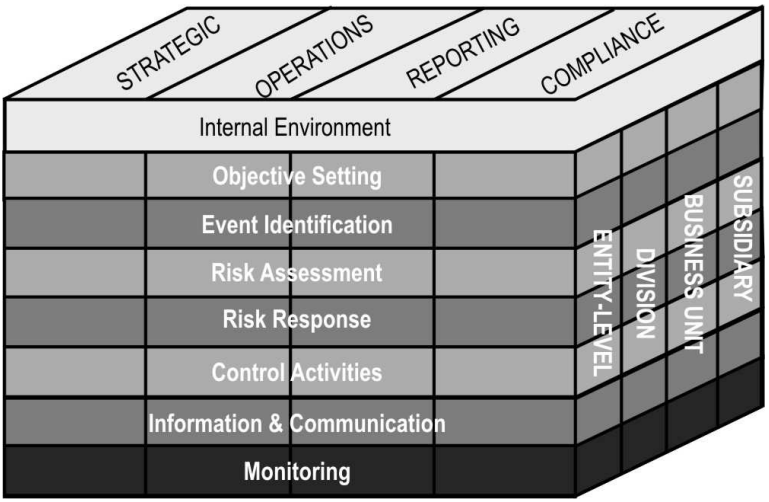
Enterprise Risk Management adalah kerangka yang komprehensif, terintegrasi, untuk mengelola risiko kredit, risiko pasar, modal ekonomis, transfer risiko, untuk memaksimumkan nilai perusahaan (Lam, James, *Enterprise Risk Management*, Wiley, 2004)

Manajemen risiko organisasi mempunyai elemen-elemen berikut ini:
Identifikasi Misi: Menetapkan Tujuan manajemen risiko.
Penilaian Risiko dan Ketidakpastian: Mengidentifikasi dan mengukur risiko.
Pengendalian Risiko: Mengendalikan risiko melalui diversifikasi, asuransi, hedging, penghindaran, dan lain-lain.

Pendanaan Risiko: Bagaimana membiayai manajemen risiko.
Administrasi program: Administrasi organisasi, seperti manual, dan sebagainya.
(Williams, Smith, Young, *Risk Management and Insurance*, McGraw Hill, 1998)

Enterprise Risk Management (ERM) adalah suatu proses, yang dipengaruhi oleh manajemen, board of directors, dan personel lain dari suatu organisasi, diterapkan dalam setting strategi, dan mencakup organisasi secara keseluruhan, didisain untuk mengidentifikasi kejadian potensial yang mempengaruhi suatu organisasi, mengelola risiko dalam toleransi suatu organisasi, untuk memberikan jaminan yang cukup pantas berkaitan dengan pencapaian tujuan organisasi. (COSO, *COSO Enterprise Risk Management – Integrated Framework.* COSO, 2004) .

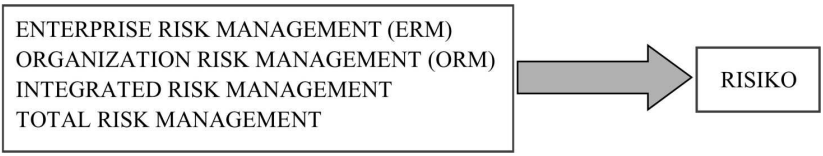
Selanjutnya COSO menampilkan format berikut ini yang menunjukkan bahwa ERM adalah manajemen risiko yang komprehensif (Lihat bagan berikut ini).



Gambar 1.4.
COSO – *Enterprise Risk Management*

Gambar 1.4 tersebut menunjukkan delapan komponen ERM yaitu (1) lingkungan internal, (2) penentuan tujuan, (3) Identifikasi kejadian, (4) Evaluasi (*assessment*) risiko, (5) Respons terhadap risiko, (6) Aktivitas pengendalian, (7) Informasi dan komunikasi, (8) Monitoring. Risiko yang dikelola mencakup risiko strategis, operasi, pelaporan, dan kepatuhan (*compliance*). Kemudian ERM mencakup keseluruhan organisasi, mulai dari level perusahaan keseluruhan (*entity level*), level divisi, level unit bisnis, dan level anak perusahaan (*subsidiary*).

Perhatikan bahwa definisi-definisi tersebut menggunakan istilah yang beragam untuk menjelaskan manajemen risiko organisasi, seperti terlihat pada bagan berikut ini.



Gambar 1.5.
Beberapa Istilah Manajemen Risiko Organisasi

Kemudian, ciri lain dari definisi tersebut adalah pengelolaan risiko yang komprehensif, dan bertujuan mencapai tujuan organisasi. Dengan menggabungkan beberapa karakteristik tersebut, bagan berikut ini menyajikan pengertian manajemen risiko suatu organisasi yang menjadi acuan modul ini.

Gambar 1.6.
Kerangka Manajemen Risiko Organisasi

Gambar 1.6 tersebut menunjukkan manajemen risiko organisasi (*enterprise risk management*) terdiri dari dua elemen besar: (1) Infrastruktur atau prasarana, yang terdiri dari prasarana lunak dan keras, dan (2) Proses Manajemen Risiko. Kemudian manajemen risiko organisasi bertujuan membantu pencapaian tujuan organisasi, dalam hal ini dirumuskan secara eksplisit menjadi memaksimumkan nilai perusahaan.

C. ELEMEN MANAJEMEN RISIKO ORGANISASI

Misalkan kita ditugaskan untuk membuat dan memimpin departemen manajemen risiko suatu perusahaan, bagaimana kita memulainya? Bagan di atas menunjukkan kerangka yang bisa digunakan untuk memulai membangun departemen manajemen risiko. Pertama, kita harus menyiapkan prasarana yang diperlukan untuk memulai pekerjaan manajemen risiko, yang meliputi prasarana lunak (non-fisik) dan prasarana keras (fisik).

1. Prasarana Manajemen Risiko

Salah satu hal yang penting dikerjakan untuk mempersiapkan manajemen risiko adalah menyiapkan prasarana yang mendukung manajemen risiko, yang meliputi prasarana lunak dan keras.

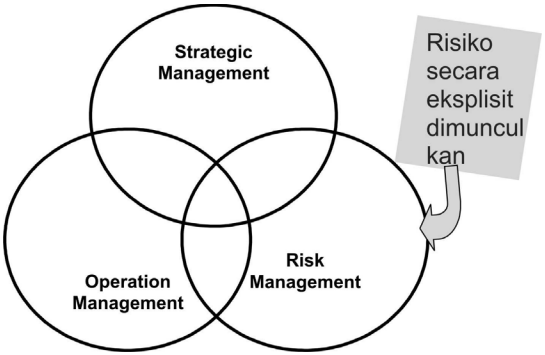
a. Prasarana lunak

Ada beberapa isu yang berkaitan dengan penyiapan prasarana lunak untuk manajemen risiko, yaitu: (1) Mengembangkan budaya sadar risiko untuk anggota organisasi, (2) Dukungan manajemen.

Mengembangkan Budaya Sadar Risiko. Tujuan dari budaya sadar risiko adalah agar setiap anggota organisasi sadar adanya risiko, dan mengambil keputusan tertentu dengan mempertimbangkan aspek risikonya. Dengan singkat, tujuan budaya sadar risiko adalah agar anggota lebih berhati-hati dalam pengambilan keputusan. Jika anggota tersebut sadar akan risiko, maka organisasi (yang terdiri dari kumpulan individu) akan menjadi lebih peka terhadap risiko.

Bagaimana mengembangkan perilaku yang sadar risiko untuk anggota organisasi? Salah satu cara yang bisa dilakukan adalah dengan memaksa mereka untuk berpikir risiko untuk setiap keputusan yang akan diambil. Pebisnis secara natural adalah orang yang optimis (karena itu mereka berani terjun ke dunia bisnis), dan cenderung melupakan aspek risiko (yang mendorong mereka untuk lebih berhati-hati). Jika dipaksa untuk berpikir mengenai risiko, maka mereka akan lebih seimbang dalam memutuskan sesuatu.

Sebagai contoh, bagan berikut ini menunjukkan tiga aspek yang harus dipikirkan oleh manajer dalam pengambilan keputusan, yaitu aspek strategis, operasi, dan risiko. Evaluasi terhadap risiko yang mungkin terjadi harus dipikirkan dan dilaporkan secara eksplisit.



Gambar 1.7.
Aspek Risiko Yang Dimunculkan Secara Eksplisit

Misalkan seorang manajer akan meluncurkan produk baru. Dia harus memikirkan tiga aspek yang disebutkan di atas, dengan pertanyaan seperti berikut ini.

1) Aspek Strategis: Apakah produk ini bisa memenuhi kebutuhan konsumen? Apakah produk ini bisa membantu pencapaian tujuan perusahaan (mencapai target keuntungan tertentu)?
2) Aspek Operasi: Bagaimana memproduksi produk ini? Apakah perusahaan mempunyai kemampuan memproduksi produk ini? Bagaimana memasarkan dan mengembangkan jaringan distribusi untuk produk ini?
3) Aspek Risiko: Risiko apa saja yang bisa muncul berkaitan dengan peluncuran produk ini? Bagaimana perusahaan bisa mengendalikan risiko-risiko tersebut?

Perhatikan pertanyaan aspek risiko secara eksplisit dimunculkan. Misalkan seorang manajer akan meluncurkan program promosi/iklan. Dia harus memikirkan tiga aspek yang disebutkan di atas, melalui pertanyaan-pertanyaan berikut ini.

1) Aspek Strategis: Bagaimana strategi promosi yang efektif? Bagaimana kontribusi promosi ini terhadap tujuan organisasi?
2) Aspek Operasi: Bagaimana menjalankan program promosi ini? Media apa yang paling efektif? Bagaimana *timing* (waktu yang tepat) untuk promosi ini? Bagaimana aspek detil lainnya dari promosi ini? Bagaimana

mengendalikan risiko-risiko yang barangkali muncul akibat peluncuran program promosi ini?

3) Aspek Risiko: Risiko apa yang potensial muncul akibat dari program promosi ini? Apakah promosi ini bisa menimbulkan gugatan hukum? Apakah promosi ini sudah etis? Pihak-pihak mana saja yang barangkali berkeberatan dengan promosi ini?

Perhatikan bahwa sama seperti sebelumnya, aspek risiko secara eksplisit perlu dipikirkan dan dimunculkan. Jika manajer terbiasa berpikir secara eksplisit mengenai risiko-risiko yang mungkin muncul, maka manajer tersebut akan semakin sadar terhadap risiko. Jika semua anggota organisasi sadar akan risiko, maka organisasi menjadi lebih sadar dan lebih peka terhadap risiko.

Mengembangkan kesadaran risiko juga bisa dilakukan melalui *workshop* atau pertemuan secara berkala antar manajer atau anggota organisasi. Agenda dalam *workshop* tersebut adalah membicarakan kejadian-kejadian yang bisa menimbulkan dampak yang negatif terhadap organisasi, alternatif-alternatif pemecahannya. *Workshop* tersebut bisa dikelola oleh manajer risiko perusahaan atau departemen risiko perusahaan. Melalui *workshop* atau pertemuan yang regular yang membicarakan risiko dengan segala aspeknya yang relevan, anggota organisasi diharapkan menjadi lebih sadar akan risiko yang dihadapi organisasi.

Teknik lain yang bisa digunakan adalah memasukkan risiko ke dalam elemen penilaian kinerja. Sebagai contoh, alokasi modal diberikan kepada usulan investasi yang memberikan *risk-adjusted return* (tingkat keuntungan setelah disesuaikan dengan risikonya) yang paling tinggi. Jika kriteria semacam itu yang akan dipakai, maka organisasi akan secara langsung 'menghukum' manajer yang berperilaku risiko tinggi. Risiko tinggi bisa dibenarkan sepanjang memberikan tingkat keuntungan yang diharapkan yang lebih tinggi juga. Dengan mekanisme evaluasi semacam itu, manajer diharapkan akan lebih sadar mengenai risiko, dan budaya risiko di organisasi akan menjadi semakin baik (semakin sadar akan risiko).

Dukungan Manajemen. Sama seperti program lainnya, dukungan manajemen khususnya manajemen puncak terhadap program manajemen risiko penting diberikan. Bentuk dukungan bisa eksplisit maupun implisit. Dukungan manajemen puncak bisa dituangkan antara lain ke dalam pernyataan tertulis, misal manajemen puncak mendukung atau ikut

merumuskan/menyetujui misi dan visi, prosedur dan kebijakan, yang berkaitan dengan manajemen risiko. Dukungan manajemen juga bisa ditunjukkan melalui partisipasi manajemen pada program-program manajemen risiko.

b. Prasarana keras

Di samping prasaran lunak, prasarana keras juga perlu disiapkan. Contoh prasarana keras yang perlu disiapkan adalah ruangan perkantoran, komputer, dan prasarana fisik lainnya. Prasarana fisik tersebut perlu dipersiapkan agar pekerjaan manajemen risiko berjalan sebagaimana mestinya.

2. Proses Manajemen Risiko

Elemen yang lebih penting lagi adalah proses manajemen risiko. Proses atau fungsi manajemen sering diterjemahkan ke dalam tiga langkah: perencanaan, pelaksanaan, dan pengendalian. Mengikuti kebiasaan tersebut, proses manajemen risiko juga bisa dibagi ke dalam tiga tahap yaitu perencanaan, pelaksanaan, dan pengendalian manajemen risiko.

a. Perencanaan

Perencanaan manajemen risiko bisa dimulai dengan menetapkan visi, misi, dan tujuan, yang berkaitan dengan manajemen risiko. Kemudian perencanaan manajemen risiko bisa diteruskan dengan penetapan target, kebijakan, dan prosedur yang berkaitan dengan manajemen risiko. Akan lebih baik lagi jika visi, misi, kebijakan, dan prosedur tersebut dituangkan secara tertulis. Dokumen tertulis semacam itu memudahkan pengarahan, sekaligus menegaskan dukungan manajemen terhadap program manajemen risiko.

Berikut ini beberapa contoh misi atau kebijakan dan prosedur yang berkaitan dengan manajemen risiko dari beberapa perusahaan/organisasi.

PERNYATAAN MISI MANAJEMEN RISIKO GOLDMAN SACH:
Misi dari departemen risiko adalah mengumpulkan, menganalisis, memonitor, dan mendistribusikan informasi yang berkaitan dengan risiko pasar dari posisi perusahaan supaya traders, manajer, dan personel lain dalam organisasi dan terutama komite risiko memahami dan membuat keputusan berdasarkan informasi (informed decisions) mengenai manajemen dan pengendalian risiko yang diambil.
(Goldman Sach adalah perusahaan sekuritas Amerika Serikat)

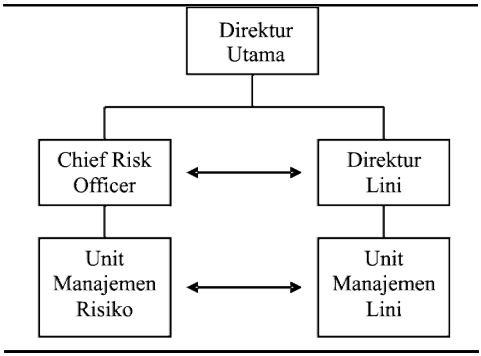
PERNYATAAN MISI SWISS BANK CORPORATION:
Pengendalian risiko Swiss Bank memfokuskan pada perlindungan terhadap modal dan memungkinkan pengambilan risiko yang sesuai. Kepentingan investor Swiss Bank adalah hal yang utama. Modal yang mereka investasikan harus dikompensasi untuk risiko yang ditanggung, baik untuk transaksi individual maupun portofolio.

Setelah misi dan kebijakan serta prosedur yang umum ditetapkan, langkah berikutnya adalah menyusun kebijakan serta prosedur yang lebih spesifik.

b. Pelaksanaan

Pelaksanaan manajemen risiko meliputi aktivitas operasional yang berkaitan dengan manajemen risiko. Proses identifikasi dan pengukuran risiko, kemudian diteruskan dengan manajemen (pengelolaan) risiko merupakan aktivitas operasional yang utama dari manajemen risiko. Identifikasi, pengukuran, dan manajemen risiko akan dibicarakan lebih detil di bagian dua, tiga, dan empat, dari modul ini. Bagian empat khusus membicarakan ilustrasi bagaimana perusahaan menerapkan manajemen risiko secara terencana dan sistematis di organisasinya.

Untuk melaksanakan pekerjaan manajemen risiko, diperlukan organisasi (struktur organisasi) dan *staffing* (personel). Struktur organisasi manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya. Berikut ini contoh struktur organisasi manajemen risiko.

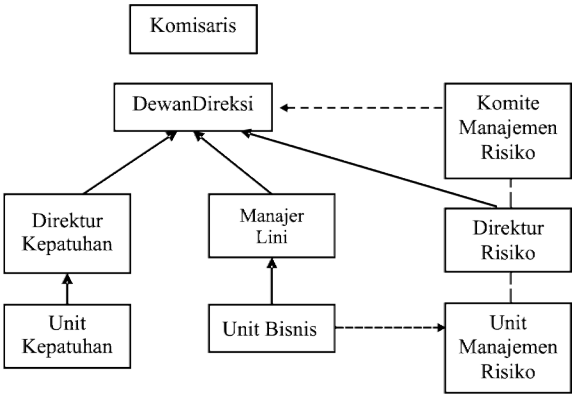


Gambar 1.8.
Struktur Organisasi Manajemen Risiko

Dalam Gambar 1.8 di atas, unit manajemen risiko bertanggung jawab ke manajer risiko yang disebut sebagai *chief risk officer* (CRO). CRO kemudian melapor (bertanggung jawab) langsung ke direktur utama. Pemisahan unit manajemen risiko menjadi bagian sendiri diharapkan mampu menjaga independensi unit manajemen risiko. Unit manajemen risiko mempunyai kedudukan yang sejajar dengan unit lini (pemasaran, keuangan, produksi). Status sebagai unit lini memungkinkan kekuatan yang cukup dalam organisasi untuk mendorong praktek manajemen risiko yang baik dalam suatu organisasi. Unit lini berkomunikasi dengan unit manajemen risiko (seperti ditunjukkan panah dua arah). Komunikasi semacam itu penting agar unit manajemen risiko memperoleh gambaran yang lengkap mengenai risiko yang dihadapi oleh perusahaan.

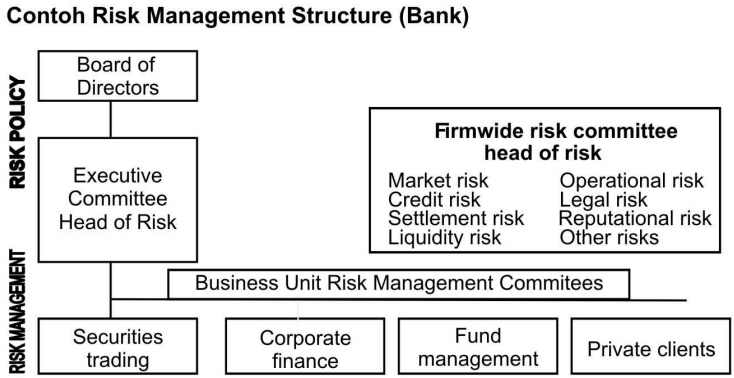
Aspek perilaku dari struktur organisasi manajemen risiko juga perlu diperhatikan. Pekerjaan manajemen risiko cenderung bertentangan dengan pekerjaan manajemen lini. Manajemen lini (misal pemasaran) ingin berjalan cepat tanpa memperhitungkan risiko. Manajemen risiko cenderung menahan keinginan semacam itu dengan mengingatkan risiko-risiko yang mungkin muncul. Struktur organisasi bisa diakomodasi untuk mengatasi potensi konflik semacam itu. Sebagai contoh, unit manajemen risiko bisa dibuat untuk melapor ke manajer risiko dan manajer lini sekaligus. Tetapi cara semacam itu barangkali tidak sempurna, karena pelaporan menjadi tidak jelas (ambigu). Contoh lain, unit manajemen risiko bertanggung jawab ke manajer lini dan memberikan laporan (hubungan garis terputus) kepada manajer risiko. Contoh lain adalah sebaliknya, unit lini bertanggung jawab ke manajer lini dan memberikan laporan ke manajer risiko. Contoh terakhir mirip seperti struktur organisasi pada bagan di atas.

Berikut ini dua contoh variasi dari struktur manajemen risiko.



Gambar 1.9.
Struktur Organisasi Manajemen Risiko Bank

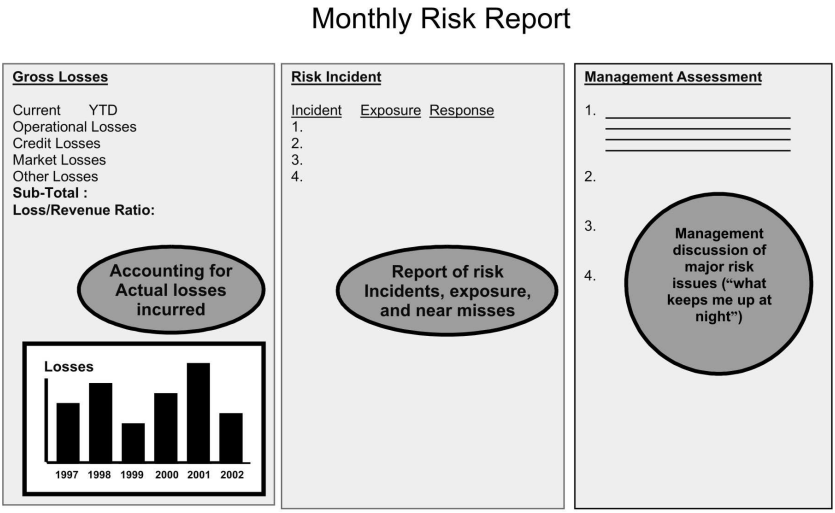
Pada struktur di atas, komite manajemen risiko mengawasi manajemen risiko organisasi. Direktur risiko mengelola kegiatan operasional manajemen risiko. Unit bisnis berkomunikasi dengan unit manajemen risiko untuk melaporkan hal-hal yang berkaitan dengan risiko organisasi. Direktur risiko mempunyai garis keanggotaan kepada komite manajemen risiko.



Gambar 1.10.
Struktur Organisasi Manajemen Risiko Bank (2)

c. Pengendalian

Tahap berikutnya dari proses manajemen risiko adalah pengendalian yang meliputi evaluasi secara periodik pelaksanaan manajemen risiko, output pelaporan yang dihasilkan oleh manajemen risiko, dan umpan balik (*feedback*). Format pelaporan manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya, dan dari satu kegiatan ke kegiatan lainnya. Sebagai contoh, bagan berikut ini menampilkan laporan profil risiko regular (misal bulanan).

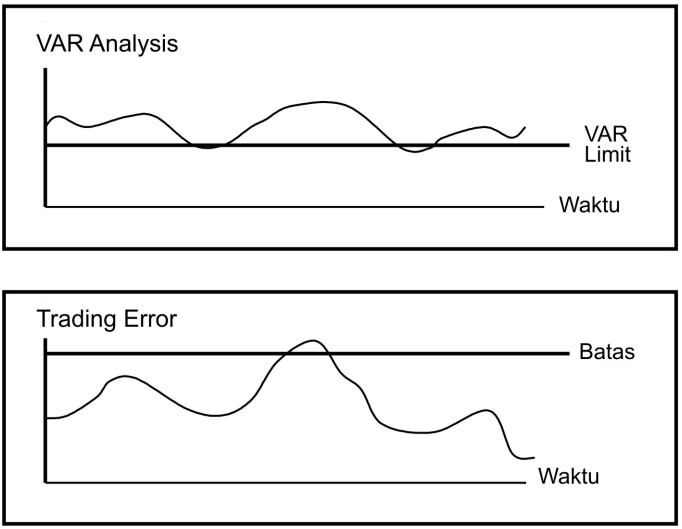


Gambar 1.11.
Contoh Laporan Risiko Bulanan

Gambar 1.11 tersebut menunjukkan laporan kerugian (keuntungan) di sebelah kiri. Gambar di tengah menunjukkan laporan mengenai kejadian-kejadian penting yang menyebabkan perusahaan mengalami kerugian, atau hampir rugi, eksposur perusahaan terhadap kejadian tersebut, dan respons yang dilakukan oleh organisasi. Sebagai contoh, perusahaan barangkali melaporkan kejadian naiknya tingkat bunga sebesar 1% (cukup tinggi). Kemudian perusahaan melaporkan eksposur yaitu posisi obligasi dengan nilai
$10 juta (sepuluh juta dolar AS). Jika tingkat bunga naik, maka nilai obligasi akan turun (yang berarti perusahaan mengalami kerugian). Kolom berikutnya menyajikan respons yang dilakukan perusahaan dalam situasi tersebut (misal

melakukan *hedging*). Bagan paling kanan menunjukkan evaluasi dan diskusi oleh manajemen terhadap risiko-risiko utama yang dihadapi oleh perusahaan.

Unit manajemen risiko bisa juga menampilkan laporan berikut ini.



Gambar 1.12.
Contoh Laporan Risiko Untuk VAR dan *Trading Error*

Kedua bagan tersebut menunjukkan perkembangan VAR (*Value At Risk*, yang merupakan indikator risiko pasar) dan kesalahan perdagangan dari waktu ke waktu. Perusahaan juga menampilkan batas untuk masing-masing variabel risiko tersebut. Jika variabel risiko tersebut masih berada di bawah batas toleransi, maka risiko tersebut belum menunjukkan tingkat keseriusan yang tinggi. Tetapi jika variabel yang diamati tersebut bergerak melewati batas toleransi perusahaan, maka perusahaan harus lebih aktif untuk mengelola risiko tersebut.

Manajer risiko bisa juga menampilkan profil risiko untuk kegiatan tertentu. Sebagai contoh tabel berikut ini menunjukkan profil risiko untuk dua proyek A dan B. Risiko dilihat berdasarkan dimensi keuangan, sosial, dan politik.

Tabel 1.4.
Profil Risiko Usulan Investasi

	Keuangan	Sosial	Politik
Proyek A	1) Tinggi	3)Tinggi 4)Tinggi	5) Tinggi
Proyek B	1)Medium 2)Rendah	3)Medium 4)Rendah	5) Rendah

Keuangan: (1) Risiko kesulitan akses dana, (2) Risiko perubahan kurs
Sosial: (3) Penerimaan masyarakat sekitar, (4) Dukungan pemerintah lokal
Politik: (5) Stabilitas politik, (6) Perubahan Peraturan

Tabel 1.4 tersebut menunjukkan beberapa item risiko untuk keuangan, sosial, dan politik yang dievaluasi. Sebagai contoh, untuk keuangan ada dua item yang dievaluasi, yaitu risiko kesulitan akses dana dan risiko perubahan kurs. Proyek A tidak mempunyai risiko perubahan kurs karena lebih banyak beroperasi di pasar domestik. Dari tabel tersebut terlihat bahwa proyek A nampaknya mempunyai risiko yang lebih besar dibandingkan dengan proyek B. Semua item risiko untuk proyek A mempunyai penilaian risiko yang tinggi. Sedangkan untuk proyek B, kebanyakan item risiko dinilai medium atau rendah. Dengan demikian bisa diambil kesimpulan bahwa proyek A mempunyai risiko yang lebih tinggi dibandingkan dengan proyek B.

Jika pelaporan tersebut belum memuaskan (misal belum cukup informatif), maka format pelaporan bisa di rubah-rubah lagi. Proses umpan balik (*feedback*) harus dijamin bisa berjalan sebagaimana mestinya. Di samping itu hasil evaluasi dari manajemen risiko harus dikomunikasikan ke pihak-pihak yang berkepentingan dan relevan (*stakeholders*). Komunikasi yang baik menjamin disclosure dan transparansi yang baik, yang merupakan elemen manajemen risiko yang baik. Kasus Enron yang bangkrut pada tahun 2001 menunjukkan bahwa organisasi tersebut gagal membangun komunikasi dan transparansi yang baik. Manajemen risiko yang baik harus menjamin terjadinya good corporate governance, diantaranya terjaminnya disclosure dan transparansi yang baik.

Daftar Pustaka

Anderson, Sweeny, and Williams. (1999). *Statistics for Business and Economics*, South-Western Publishing, Cincinnati.

Barton, Thomas, William G. Shenkir, Paul L. Walker. (2002). *Making Enterprise Risk Management Pay Off.* New Jersey: Prentice Hall.

Boodie, Zvi and Robert C. Merton. (2000). *Finance.* New Jersey: Prentice Hall.

Doherty, Neil. (2000). *Integrated Risk Management.* New York: McGraw Hill.

Hanafi, Mamduh. (2005). *Manajemen Keuangan.* Yogyakarta: BPFE.

Hanafi, Mamduh. (2004). *Manajemen Keuangan Internasional.* Yogyakarta: BPFE.

Harrington, Scott E., dan Gregory R. Niehaus. (2003). *Risk Management and Insurance.* Boston: McGraw Hill.

Lam, James. (2004). *Enterprise Risk Management.* Wiley.

Marshall, John F., dan Vipul K. Bansal. (1992). *Financial Engineering, A Complete Guide to Financial Innovation.* New York: Institute of Finance.

Pande, Pete and Larry Holpp. (2002). *What is Six Sigma.* New York.

Risk Group (ed.). (2001). *Advances in Operational Risk.* London: Risk Water Group Ltd.

Saunders and Cornett. (2003). *Financial Institutions Management, A Risk Management Approach*, McGraw Hill.

SBC Warburg. (2004). *The Practice of Risk Management*, Euromoney Book.

Stulz, Rene M. (2003). *Risk Management and Derivatives.* Thomson-South Western.

Trieschmann, dan Gustavson. (1995). *Risk Management and Insurance*, South Western College Publishing.

Williams, C. Arthur, Michael Smith, and Peter C. Young. (1998). *Risk Management and Insurance*, Boston: McGraw Hill.

http ://www. wikip edia. corn.

Analisis Resiko Pada Akademik Management System STKIP Muhammadyah Bangka Belitung

Yuniarti Denita Sari[1], Zena Lusi[2], Reni Septiyanti[3], Anggari Ayu P[4], Gina Agiyani[5]
Magister Teknik Informatika, Universitas Bina Darma Palembang

ABSTRAK

Akademik *Management System* merupakan sistem akademik yang ada di STKIP Muhammadyah Bangka Belitung. Sistem ini merupakan penhubung antara civitas akademik baik itu dosen dan mahasiswa. Hal ini menjadikan aktivitas-aktivitas yang terjadi di dalamnya menjadi sangat krusial. Berjalannya elemen dan komponen sistem dengan baik menjadi hal yang sangat penting guna menunjang kinerja dari sistem itu sendiri. Namun, tidak dapat dipungkiri bahwa kemungkinan munculnya berbagai ancaman dan resiko dapat menghambat bahkan melumpuhkan aktivitas di dalam sistem, salah satunya disebabkan oleh teknologi informasi yang digunakan. Untuk itu, perlu dilakukan analisis resiko terhadap berbagai kemungkinan resiko yang muncul di dalam sistem. Berdasarkan hasil analisis akan didapatkan gambaran mengenai aset fisik beserta kemungkinan resiko yang muncul pada aset tersebut. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* menggunakan ISO 31000 dan difokuskan pada perangkat keras dan infrastruktur jaringan pada sistem AMS. Dari hasil penelitian didapatkan Nilai Prioritas Resiko (RPN) berdasarkan proses pengukuran yang telah dilakukan pada tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Sehingga organisasi dapat melakukan pencegahan, penanganan serta perbaikan untuk ke depannya sesuai dengan tingkat prioritas resiko.
Kata kunci: Akademik *Management System*, *Risk Management*

I. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu perusahaan atau sebuah lembaga pendidikan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional akademik dan proses bisnis organisasi. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama di dalamnya demi memenuhi kebutuhan informasi para pengguna. STKIP Muhammadyah Bangka Belitung merupakan salah satu lembaga pendidikan yang telah menerapkan dan melibatkan teknologi informasi di dalamnya, salah satu nya adalah penggunaan AMS (Akademik Management System) yang merupakan

aplikasi akademik untuk mahasiswa, dosen, maupun pegawai untuk semua Fakultas di lingkungan STKIP Muhammadyah Bangka Belitung. AMS merupakan sistem terintegrasi berbagai kegiatan akademik maupun non akademik di STKIP Muhammadyah Bangka Belitung. Oleh sebab itu, kehadiran AMS dinilai sangat penting dalam penyampaian informasi ke seluruh civitas akademik, hal ini membuat AMS harus tetap berjalan baik dan konsisten. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan resiko yang muncul dalam sistem akan mengganggu bahkan melumpuhkan aktivitas di dalam sistem sehingga sistem tidak dapat berjalan secara optimal. Berangkat dari permasalahan diatas, maka perlu dilakukan suatu analisis resiko terhadap kemungkinan ancaman dan resiko yang muncul di dalam sistem. Sehingga perusahaan atau organisasi dapat melakukan pencegahan, penanganan serta perbaikan terhadap kemungkinan-kemungkinan resiko tersebut. Berdasarkan hasil analisis tersebut, didapatkan gambaran mengenai aset fisik beserta kemungkinan ancaman dan resiko yang muncul pada tiap-tiap aset tersebut. Selain itu juga didapatkan nilai resiko yang diperoleh dari proses pengukuran tingkat resiko untuk tiap-tiap resiko yang telah diidentifikasi dan dianalisis sebelumnya. Analisis Resiko Teknologi Informasi Berbasis *Risk Management* ini menggunakan ISO 31000 yang difokuskan pada Teknologi dan Infrastruktur jaringan sistem AMS.

II. PEMBAHASAN

1. Penilaian Resiko

Pada Penilaian resiko terdapat beberapa tahapan yang harus dilakukan antara lain :

a. Identifikasi Aset

Tahapan identifikasi aset akan memberikan suatu gambaran mengenai aset-aset yang berhubungan dengan sistem AMS dilihat dari sisi Teknologi dan Infrastrukturnya melalui proses observasi dan *interview* dengan pihak-pihak terkait.

b. Identifikasi Resiko

Tahap Identifikasi resiko bertujuan untuk mengidentifikasi berbagai kemungkinan resiko yang muncul pada aset melalui proses *studi literature* dan *interview*. Proses ini dimulai dari mengidentifikasi berbagai kemungkinan resiko yang muncul pada teknologi dan infrastruktur sistem AMS. Setelah diperoleh daftar resiko yang dapat terjadi maka mulai dianalisis mengapa hal tersebut dapat terjadi dan

bagaimana dampak yang ditimbulkan dari resiko tersebut.

Tabel 1. Identifikasi Resiko

Sumber Resiko	Resiko
Alam Lingkungan	Kebakaran
	Banjir
	Gempa Bumi
	Petir
	Badai
	Embun
	Radiasi Panas
	Suhu Yang Bervariasi
	Debu / Kotoran
	Kelembapan
Manusia	Pencurian Perangkat
	Informasi diakses oleh pihak yang tidak berwenang
	Kebocoran data atau informasi internal perusahaan / institusi
	Data dan informasi tidak sesuai fakta
	Penyalahgunaan hak akses / user ID
	Mantan user / karyawan masih memiliki akses informasi
	Akses fisik yang tidak terotorisasi
	Hilangnya data
	Human error
	Resiko kerusakan akbiat ulah manusia seperti cybercrime, terorisme, pembajakan dan vandalism
Sistem dan Infrastruktur	Kegagalan / kerusakan hardware
	Server down
	Overheat
	Koneksi jaringan terputus
	Sistem crash
	Overcapacity
	Overload
	Data corrupt
	Backup failure
	Gagal update
	Kurang baiknya kualitas jaringan
	Teknologi using
	Resiko kerusakan akibat masalah caturdaya / tegangan listrik

c. Analisis Resiko

Analisis resiko adalah upaya untuk memahami resiko lebih dalam. Hasil analisis resiko ini akan menjadi masukan bagi evaluasi resiko dan proses pengambilan keputusan mengenai perlakuan resiko terhadap resiko tersebut. Analisis resiko meninjau dua aspek resiko, yaitu dampak dan kemungkinan. Tingkat resiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis resiko ini dilakukan penilaian terhadap resiko-resiko yang muncul pada sistem AMS. Hal ini mencakup penilaian terhadap dampak (*impact*) apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko (*likelihood*) dengan menggunakan kuisioner dengan melihat dari sisi para ahli atau orang-orang yang memiliki pengetahuan, pengalaman dan berhubungan langsung dengan sistem.

d. Kuisioner

Merupakan salah satu alat bantu atau instrument pengumpul data dalam penelitian untuk memperoleh keterangan dari sejumlah responden dengan menggunakan kriteria yang telah

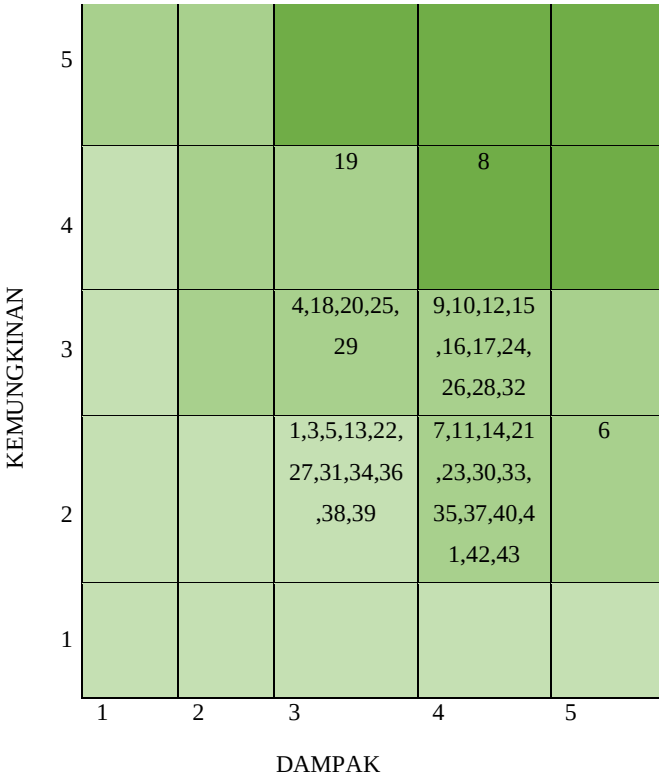
ditetapkan sebelumnya. Penggunaan kuesioner dalam penelitian ini bertujuan untuk memperoleh informasi mengenai penilaian terhadap dampak *(impact)* apabila suatu resiko terjadi, serta kemungkinan terjadinya resiko *(likelihood)* pada Teknologi dan Infrastruktur AMS.

Tabel 2. Pilihan Jawaban untuk Kriteria Kemungkinan

Jawaban	Singkatan	Nilai
Sangat Kecil	SK	1
Kecil	K	2
Sedang	S	3
Besar	B	4
Sangat Besar	SB	5

e. Evaluasi Resiko

Tujuan dari evaluasi resiko adalah membantu proses pengambilan keputusan berdasarkan hasil analisis resiko. Proses evaluasi resiko akan menentukan resiko-resiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas resiko-resiko tersebut. Untuk menentukan peringkat resiko diperlukan matriks yang berisi kombinasi kemungkinan dan dampak. Dengan tetap menggunakan data dari tabel sebelumnya maka dilakukan penampilan grafis peringkat resiko dengan cara mengambil hasil perkalian dari nilai kemungkinan dan nilai dampak. Matriks tersebut kemudian dibagi ke dalam tiga kuadran sesuai dengan tingkat keutamaan atau level prioritas penanganan dari resiko-resiko yang telah terdefinisi.



Gambar 1. Matriks Kemungkinan Dan Dampak Resiko

Keterangan :

Resiko Tinggi

Resiko Mengah

Resiko Rendah

Dari matriks kemungkinan dan dampak diatas, maka diketahui bahwa resiko yang

memiliki nilai resiko paling tinggi adalah resiko nomor 14 yaitu *Database crash*. Sedangkan yang berada pada kuadran resiko menengah terdapat 30 resiko dan yang berada pada kuadran resiko rendah terdapat 12 resiko.

Tingkat Keutamaan	No Resiko	Resiko	Nama Aset
Level 1 (High / Tinggi)	8	Database Server Down	Datbase Server
Level II (Medium / Menengah)	19	Human error	Database Server
	4	Server Down	NTP Server
	18	Backup Failure	Database Server
	20	Gagal Update	Database Server
	25	Kurang Baiknya Jaringan	APP Server
	29	Backup Failure	Backup
	9	Koneksi Database	Database Server
	10	Informasi diakses oleh pihak yang tidak berwenang	Database Server
	12	Penyalahgunaan Hak Akses/user ID	Database Server
	15	Overload	Database Server
	16	Hilangnya Data	Database Server
	17	Data Corrupt	
	24	Server Down	APP Server
	26	Overcapacity	APP Server
	28	Load Balancer Down	Load Balancer
	32	Jaringan Terputus	Network Link
	7	Pencurian Perangkat	Datbase Server
	11	Kebocoran Data atau informais internal	Datbase Server
	14	Database crash	Database Server
	21	Resiko Akibat Bencana Alam	APP Server
	23	Pencurian Perangkat	APP Server
	30	Kerusakan Hardware	Storage
	33	Kegagalan Hardware	Core Router
	35	UPS tidak Berfungsi	UPS
	37	Genset tidak berfungsi / rusak	Genset
	40	Resiko kerusakan akibat bencana alam yang mempengaruhi fasilitas, asset dan lokasi data center	Data Center
	41	Kerusakan akibat ulah manusia	Data Center
	42	Resiko kehilangan baik pada data maupun perangkat keras	Data Center
	43	Resiko kerusakan akibat masalah catu daya / tegangan listrik	Data Center
	6	Resiko kerusakan akibat bencana alam seperti kebakaran, banjir, gempa bumi	Database Server
Level III (Low /	1	Resiko Kerusakan akibat bencana alamt	NTP Server

Rendah)		seperti kebakaaran banjir, gempa	
	2	Pencurian Perangkat	NTP Server
	3	Kegagalan / Kerusakan hardware	NTP Server
	5	Overheat	NTP Server
	13	Mantan user / karyawan masih memilik akses informasi	Database Server
	22	Kegagalan / Kerusakan Hardware	NTP Server
	27	SVN Down	SVN
	31	Penyimpanan Penuh	Storage
	34	CDN Down	CDN
	36	Baterai UPS lemah	UPS
	38	Baterai Lemah atau Mati	Genset
	39	AC Mati	AC

f. Perlakuan Resiko

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

1) Menghindari resiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan resiko tersebut.
2) Berbagi resiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya resiko atau dampak resiko.
3) Mitigasi (mitigation), yaitu melakukan perlakuan resiko untuk mengurangi kemungkinan timbulnya resiko, atau mengurangi dampak resiko bila terjadi, atau mengurangi keduanya.
4) Menerima resiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap resiko tersebut.

Penanganan resiko difokuskan pada resiko-resiko yang berada pada Level I (High/ Tinggi) yaitu:

Database Server Down. Database Server adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/server. Istilah ini juga merujuk kepada sebuah komputer (umumnya

merupakan server) yang didedikasikan untuk menjalankan program yang bersangkutan. Database server dapat digunakan untuk beberapa kegiatan seperti analisis data, penyimpanan data, pengarsipan, dan lain-lain. Manfaat penggunaan database server salah satunya dapat menyimpan data secara teratur dan banyak pengguna yang dapat mengakses database pada waktu yang sama. Penggunaan database server ini sangat berguna bagi organisasi, perusahaan atau institusi yang menyimpan banyak data dan informasi, termasuk sistem AMS sendiri. Database server down berdampak pada seluruh layanan AMS yang tidak dapat berjalan / diakses. Mengingat besarnya dampak yang ditimbulkan, maka menjadi kajian tersendiri perlu dilakukannya identifikasi terkait dengan pemicu, upaya serta penanganan yang dilakukan ketika resiko tersebut terjadi. Dalam mengambil langkah-langkah untuk menangani resiko terkait sebaiknya terlebih dahulu memperhatikan hal-hal berikut ini :

1. Apa pemicu terjadinya database server down pada sistem AMS?
2. Seberapa sering database server down tersebut terjadi pada sistem AMS?
3. Kapan biasanya database server down paling sering terjadi?

Berdasarkan studi literatur dan analisis yang dilakukan dapat disimpulkan bahwa terdapat beberapa pemicu terjadinya resiko database server down antara lain :

a) Overheat
b) Overcapacity
c) Overload
d) Tingginya jumlah user dalam satu waktu Database server down biasanya paling sering terjadi pada waktu-waktu tertentu atau ketika memasuki event-event tertentu seperti pada saat registrasi mata kuliah dan penginputan geladi. Pada waktu-waktu tersebut tingginya jumlah user yang mengakses sistem pada waktu yang bersamaan sehingga beban kerja server semakin bertambah dan dapat memicu terjadinya server down. Jika dilihat dari pemicunya, berikut adalah beberapa hal yang dapat dilakukan untuk mencegah dan menangani terjadinya resiko database server down,antara lain :
    - Menggunakan pendingin ruangan yang cukup untuk menjaga suhu dan temperatur ruangan agar tetap dingin

sehingga perangkat terhindar dari resiko akibat overheat.

- Menghilangkan log yang menggunakan kapasitas yang besar
- Melakukan restart database service.
- Memprioritaskan query yang berat.

III. KESIMPULAN

Berdasarkan hasil analisis resiko yang dilakukan dapat disimpulkan bahwa :

1. Setelah melakukan serangkaian proses manajemen resiko, maka didapatkan hasil tingkatan resiko pada sistem AMS. Resiko yang berada pada level tinggi adalah resiko yang memiliki nilai kemungkinan dan nilai dampak yang tinggi. Pada sistem AMS, resiko yang memiliki nilai resiko paling tinggi adalah Database Server Down. Dampak yang ditimbulkan apabila resiko tersebut terjadi adalah seluruh layanan tidak dapat berjalan sehingga perlu dilakukan penanganan secara cepat terhadap resiko tersebut.
2. Berdasarkan hasil analisis, diketahui bahwa hampir semua aset atau perangkat pendukung jaringan pada sistem membutuhkan koneksi dan asupan listrik yang baik dan konstan agar perangkat dapat berjalan dengan optimal, oleh sebab itu perlu diperhatikan hal-hal yang berhubungan dengan listrik dan koneksi jaringan untuk mendukung jalannya sistem dengan baik

DAFTAR PUSTAKA

[1] Online].Available:https://www.academia.edu/5415980/Pengertia_Manajemen_Management_dan_Manajer_Man ager_. [Accessed 5 Juni 2015].

[2] [Online].Available:http://mobelos.blogspot.com/2013/12/pengertian-manajemen definisi manajemen.html. [Accessed 15 Mei 2015].

[3] [Online].Available:http://id.wikipedia.org/wiki/Manajemen_resiko.[Accessed 28 Mei 2015].

[4] [Online]. Available: https://avicennaedu.wordpress.com/2013/03/26/ resiko-manajemen-risk-management/.[Accessed 14 Juni 2015].

[5] [Online].Available:https://www.academia.edu/9860893/PROSES_MANAJEMEN_RESIKO. [Accessed 1 Juni2015].

[6] [Online]. Available: http://chilemiam.blogspot.com/2009/10/sistem-informasisistem-adalah-suatu.html. [Accessed 5 April 2015].

[7] [Online].Available:http://dosen.gufron.com/artikel/pengertian-dandefinisi-teknologi informasi/1/. [Accessed 3 Juni 2012].

[8] [Online].Available:http://www.darakonsultanasuransi.com/index.php/risk-management-and-resiko/48-

manajemen.[Accessed 16 November 2014].
[9] [Online].Available:http://dosen.guf ron.com/artikel/pengertian-dandefinisi-teknologi-informasi/1/. [Accessed 3 Juni 2015].
[10] [Online].Available:http://fisipuin.sa tugen.com/blog/PengertianSistem-Informasi Menurut-Para-AhliDefinisi. [Accessed 17 Februari 2015].
[11] [Online]. Available: http://www.apbgroup.com/asesmen-manajemen-resikoberbasis-iso-310002009/.[Accessed 8 Maret 2015].
[12] L. J. Susilo, "Manajemen Resiko Berbasis ISO 31000".
[13] [Online].Available:https://www.aca demia.edu/5170798/Uji_Validitas_ Dan_Reliabilias.[Accessed 6 Maret 2015].
[14] [Online].Available:http://setabasri0 1.blogspot.com/2012/04/ujivalidita s-dan reliabilitas-item.html.[Accessed 25 Februari 2015].
[15] [Online].Available:https://avicenna edu.wordpress.com/2013/03/26/resi komanajemen-risk-management/. [Accessed 10 Juni 2015].

1. Pendahuluan

Enterprise risk management. Secara singkat, pengertian dan definisi risiko cukup beragam. Sumber risiko pada dasarnya adalah ketidakpastian. Ketidakpastian memunculkan risiko. Proses manajemen risiko adalah tahapan yang dilakukan untuk mengelola risiko secara sistematis. *Enterprise Risk Management* (ERM) adalah manajemen risiko dalam suatu organisasi. Modul satu berikut ini membicarakan lebih lanjut ketiga konsep dasar manajemen risiko tersebut. Setelah mempelajari Modul 1 ini, secara umum Anda diharapkan dapat menjelaskan gambaran secara umum mengenai risiko dan pengelolaan risiko tersebut. Secara khusus, setelah mempelajari Modul 1 ini, Anda diharapkan bisa menjelaskan:

1. Beberapa pengertian dan definisi risiko.
2. Kondisi ketidakpastian sebagai sumber risiko.
3. Beberapa contoh kerugian yang dialami organisasi akibat kegagalan mengelola risiko.
4. Proses atau tahapan dalam pengelolaan risiko.
5. *Enterprise Risk Management* (pengelolaan risiko dalam suatu organisasi).
6. Komponen-komponen dalam *Enterprise Risk Management.*

A. RISIKO DAN KONDISI KETIDAKPASTIAN

Risiko merupakan kata yang sudah kita dengar hampir setiap hari. Biasanya kata tersebut mempunyai konotasi yang negatif, sesuatu yang tidak kita sukai, sesuatu yang ingin kita hindari. Sebagai contoh, jika kita jalan keluar dengan mobil, maka ada risiko mobil kita bertabrakan dengan mobil lainnya (kejadian yang tidak kita inginkan). Jika kita mempunyai saham, ada risiko harga saham yang kita pegang turun nilainya, sehingga kita tidak memperoleh keuntungan (kejadian yang tidak kita harapkan). Jika bank memberikan kredit kepada suatu perusahaan, maka ada kemungkinan perusahaan tersebut gagal bayar (tidak membayar bunga dan/atau cicilan pinjamannya).

Apa yang dimaksud dengan risiko? Risiko bisa didefinisikan dengan berbagai cara. Sebagai contoh, risiko bisa didefinisikan sebagai kejadian yang merugikan. Definisi lain yang sering dipakai untuk analisis investasi, adalah kemungkinan hasil yang diperoleh menyimpang dari yang diharapkan. Deviasi standar merupakan alat statistik yang bisa digunakan untuk mengukur penyimpangan, karena itu deviasi standar bisa dipakai untuk mengukur risiko. Pengukuran yang lain adalah menggunakan probabilitas. Sebagai contoh, pengemudi kendaraan orang muda lebih sering mengalami kecelakaan dibandingkan dengan orang dewasa. Probabilitas terjadinya kecelakaan untuk

orang muda lebih tinggi dibandingkan dengan untuk orang dewasa. Karena itu risiko kecelakaan untuk orang muda lebih tinggi dibandingkan untuk orang dewasa.

Kenapa muncul suatu risiko? Risiko berkaitan erat dengan kondisi ketidakpastian. Risiko muncul karena ada kondisi ketidakpastian. Praktis kita menghadapi banyak ketidakpastian di dunia ini. Sebagai contoh, hari ini bisa hujan, bisa juga tidak hujan. Investasi kita bisa mendatangkan keuntungan (harga naik), bisa juga menyebabkan kerugian (harga turun). Kepastian dalam dunia ini adalah ketidakpastian itu sendiri. Ketidakpastian tersebut menyebabkan munculnya risiko. Ketidakpastian itu sendiri ada banyak

tingkatannya. Tabel berikut ini menunjukkan tingkatan ketidakpastian dengan karakteristiknya.

Tabel 1.1.

Tingkatan Ketidakpastian

TINGKAT KETIDAKPASTIAN	KARAKTERISTIK	CONTOH
TIDAK ADA (PASTI)	HASIL BISA DIPREDIKSI DENGAN PASTI	HUKUM ALAM
KETIDAKPASTIAN OBJEKTIF	HASIL BISA DIIDENTIFIKASI DAN PROBABILITAS DIKETAHUI	PERMAINAN DADU, KARTU
KETIDAKPASTIAN SUBJEKTIF	HASIL BISA DIIDENTIFIKASI TAPI PROBABILITAS TIDAK DIKETAHUI	KEBAKARAN, KECELAKAAN MOBIL, INVESTASI
SANGAT TIDAK PASTI	HASIL TIDAK BISA DIIDENTIFIKASI DAN PROBABILITAS TIDAK DIKETAHUI	EKSPLORASI ANGKASA

Pada tingkatan pertama, kondisi kepastian sangat tinggi. Hasil bisa diprediksi dengan relatif pasti. Hukum alam merupakan contoh kepastian tersebut. Sebagai contoh, kita bisa memprediksi dengan pasti bahwa bumi mengitari matahari selama 360 hari (satu tahun). Tingkatan selanjutnya adalah ketidakpastian objektif, dengan contoh adalah dadu, jika kita melempar dadu, ada enam kemungkinan yaitu angka 1, 2, 3, 4, 5, dan 6 (ada enam kemungkinan hasil). Kita bisa menghitung probabilitas masing-masing angka untuk keluar, yaitu 1/6.

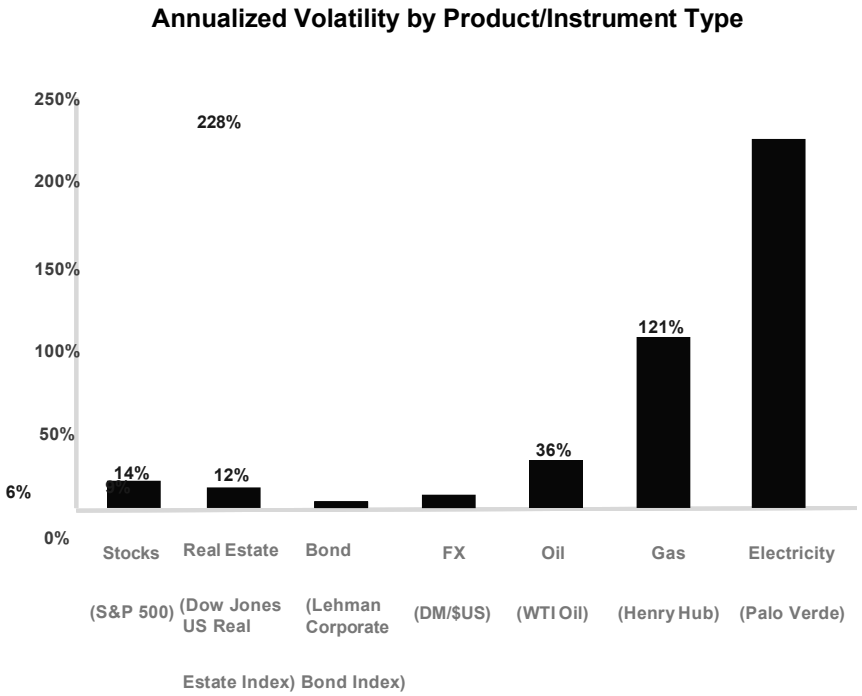
Tingkatan berikutnya adalah ketidakpastian subjektif, dengan contoh adalah kecelakaan mobil. Identifikasi hasil dan probabilitas (kemungkinan) yang berkaitan dengan kecelakaan mobil lebih sulit dilakukan. Sebagai contoh, jika kita pergi keluar dengan mobil, berapa besar probabilitas kita mengalami kecelakaan mobil? Dan jika terjadi kecelakaan, kerusakan atau kerugian yang bagaimana yang akan kita dapatkan? Tidak mudah untuk menjawab pertanyaan tersebut. Tingkatan berikutnya adalah kondisi sangat tidak pasti,

dengan contoh eksplorasi angkasa. Kita tidak tahu apa hasil yang akan diperoleh dari eksplorasi angkasa, apakah akan bertemu dengan makhluk asing (*alien*), ataukah menemukan planet yang mirip bumi, atau apa

yang akan kita temukan. Sangat sulit memprediksi atau mengidentifikasi hasil yang barangkali bisa diperoleh dari eksplorasi angkasa seperti itu. Tentu saja juga akan sangat sulit menentukan probabilitas untuk masing-masing kemungkinan hasil tersebut.

Ketidakpastian bisa tercermin dari fluktuasi pergerakan yang tinggi; Semakin tinggi fluktuasi, semakin besar tingkat ketidakpastiannya. Bagan berikut ini menunjukkan fluktuasi harga beberapa instrumen (dihitung berdasarkan deviasi standar tahunan). Terlihat bahwa semua harga instrumen berfluktuasi. Sebagai contoh, saham mempunyai fluktuasi sebesar 14%, sementara harga listrik mempunyai fluktuasi sebesar 228%.

Hasil empiris pada bagan di atas menunjukkan bahwa di dunia ini semuanya serba tidak pasti. Saham, valas (FX), harga minyak, sampai dengan harga listrik, mempunyai fluktuasi, meskipun dengan tingkat fluktuasi yang berbeda-beda. Kepastian adalah ketidakpastian itu sendiri. Dengan demikian risiko ada di mana-mana, mencakup semua instrumen.



Gambar 1.1.
Fluktuasi Tahunan Berdasarakn Tipe Instrumen

Selain itu, fluktuasi harga cenderung semakin meningkat dari tahun ke tahun. Sebagai ilustrasi, Indonesia mengalami perubahan sistem kurs dari tetap menjadi mengambang pada pertengahan tahun 1997. Sebelum krisis pada tahun 1997, Indonesia menganut sistem kurs tetap, dengan menetapkan kurs Rp/$ pada tingkat sekitar Rp2.500/$. Pada pertengahan tahun 1997, untuk mengurangi tekanan terhadap kurs karena ada krisis ekonomi, pemerintah mengambangkan kurs Rp/$. Sistem kurs mengambang tersebut masih berlaku sampai saat ini. Kurs Rp/$ tidak lagi tetap, tetapi bisa berubah tergantung mekanisme pasar. Sistem kurs mengambang tersebut mengakibatkan fluktuasi kurs Rp/$ jauh lebih tinggi dibandingkan dengan fluktuasi kurs Rp/$ pada sistem kurs tetap.

Mengapa fluktuasi cenderung meningkat? Ada beberapa faktor yang mendorong peningkatan fluktuasi tersebut, seperti:

1. Globalisasi dunia.
2. Liberalisasi dunia.
3. Proses Informasi yang semakin cepat, reaksi investor yang semakin cepat.

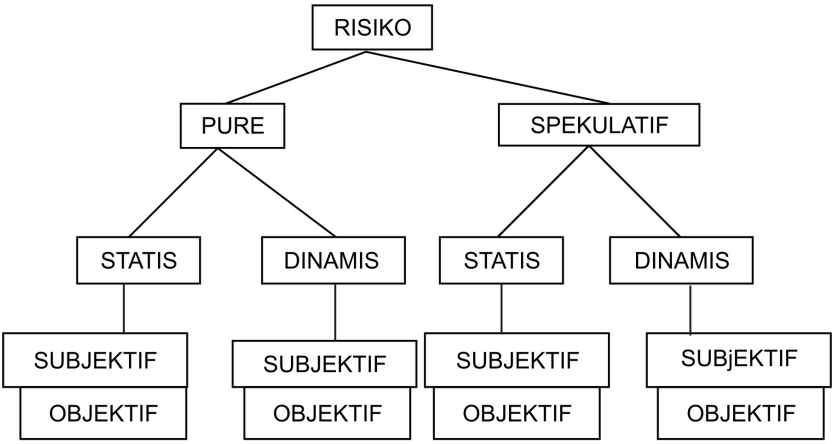
Globalisasi dunia membuat keterkaitan perekonomian dunia lebih erat. Kejadian di suatu negara akan lebih cepat mempengaruhi negara lain. Dengan kondisi seperti itu, fluktuasi akan cenderung meningkat. Liberalisasi dunia (membuka pasar domestik terhadap investor asing) mempunyai efek yang sama dengan globalisasi. Hambatan antar negara menjadi berkurang. Aliran modal menjadi lebih mudah untuk masuk atau keluar. Hal semacam ini akan meningkatkan fluktuasi dunia. Sebagai ilustrasi, krisis ekonomi di Thailand pada tahun 1997, memicu terjadinya krisis ekonomi di negara- negara sekitarnya (Indonesia, Filipina, Malaysia) dengan cepat. Investor dengan cepat memindahkan dananya dari Thailand dan negara-negara sekitarnya ke negara-negara lain yang dianggap lebih aman. Terbukanya perekonomian dunia memungkinkan pergerakan modal yang cepat semacam itu.

Teknologi yang semakin maju membuat investor atau pelaku pasar semakin canggih dalam memproses informasi. Kecanggihan tersebut akan mendorong pelaku pasar untuk lebih cepat memperoleh informasi dan bertindak lebih cepat atas informasi tersebut. Kemudahan informasi dan reaksi yang cepat dari investor akan mendorong fluktuasi harga yang semakin tinggi.

Globalisasi, liberalisasi, dan teknologi yang semakin canggih akan semakin meningkatkan fluktuasi harga, semakin meningkatkan ketidakpastian. Fluktuasi tersebut ternyata praktis dialami oleh semua atau sebagian besar instrumen keuangan atau komoditas di dunia. Dengan demikian bisa diambil kesimpulan bahwa risiko ada di mana-mana, dan risiko cenderung semakin meningkat dari tahun ke tahun.

B. TIPE-TIPE RISIKO

Risiko beragam jenisnya, mulai dari risiko kecelakaan, kebakaran, risiko kerugian, fluktuasi kurs, perubahan tingkat bunga, dan lainnya. Untuk memudahkan pemahaman dan analisis terhadap risiko, kita bisa memetakan atau mengelompokkan risiko-risiko tersebut. Salah satu cara untuk mengelompokkan risiko adalah dengan melihat tipe-tipe risiko. Bagan berikut ini menunjukkan bahwa risiko bisa dikelompokkan ke dalam dua tipe risiko: risiko murni dan risiko spekulatif, risiko subjektif dan objektif, dan dinamis dan statis.



Gambar 1.2.
Kategorisasi Risiko

Risiko bisa dikelompokkan ke dalam risiko murni dan risiko spekulatif dengan penjelasan sebagai berikut ini.

1. Risiko murni (*pure risks*) adalah risiko di mana kemungkinan kerugian ada, tetapi kemungkinan keuntungan tidak ada. Jadi kita membicarakan potensi kerugian untuk risiko tipe ini. Beberapa contoh risiko tipe ini adalah risiko kecelakaan, kebakaran, dan semacamnya. Contoh lain adalah risiko banjir menghantam rumah kita. Kejadian seperti itu akan merugikan kita. Tetapi rumah berdiri di tempat tertentu tidak secara langsung akan mendatangkan keuntungan tertentu. Jika terjadi kebakaran atau banjir, di samping individu yang terkena dampaknya, masyarakat secara keseluruhan juga akan dirugikan. Asuransi biasanya lebih banyak berurusan dengan risiko murni.
2. Risiko spekulatif adalah risiko di mana kita mengharapkan terjadinya kerugian dan juga keuntungan. Potensi kerugian dan keuntungan dibicarakan dalam jenis risiko ini. Contoh tipe risiko ini adalah usaha bisnis. Dalam kegiatan bisnis, kita mengharapkan keuntungan, meskipun ada potensi kerugian. Contoh lain adalah jika kita memegang (membeli) saham. Harga pasar bisa meningkat (kita memperoleh keuntungan), bisa juga analisis kita salah, harga saham bukannya meningkat, tetapi malah turun (kita memperoleh kerugian). Risiko spekulatif juga bisa dinamakan sebagai risiko bisnis. Kerugian akibat risiko spekulatif akan merugikan individu tertentu, tetapi akan menguntungkan individu lainnya. Misalkan suatu perusahaan mengalami kerugian karena penjualannya turun, perusahaan lain barangkali akan memperoleh keuntungan dari situasi tersebut. Secara total, masyarakat tidak dirugikan oleh risiko spekulatif tersebut.

Di samping kategorisasi murni dan spekulatif, risiko juga bisa dibedakan antara risiko yang dinamis dan yang statis.

1. Risiko statis muncul dari kondisi keseimbangan tertentu. Sebagai contoh, risiko terkena petir merupakan risiko yang muncul dari kondisi alam yang tertentu. Karakteristik risiko ini praktis tidak berubah dari waktu ke waktu.
2. Risiko dinamis muncul dari perubahan kondisi tertentu. Sebagai contoh, perubahan kondisi masyarakat, perubahan teknologi, memunculkan jenis-jenis risiko baru. Misal, jika masyarakat semakin kritis, sadar akan haknya, maka risiko hukum (*legal risk*) yang muncul karena masyarakat

lebih berani mengajukan gugatan hukum (*sue*) terhadap perusahaan, akan semakin besar.

Risiko juga bisa dikelompokkan ke dalam risiko subjektif dan objektif dengan penjelasan sebagai berikut ini.

1. Risiko objektif adalah risiko yang didasarkan pada observasi parameter yang objektif. Sebagai contoh, fluktuasi harga atau tingkat keuntungan investasi di pasar modal bisa diukur melalui standar deviasi, misal standar deviasi *return* saham adalah 25% per tahun.
2. Risiko subjektif berkaitan dengan persepsi seseorang terhadap risiko. Dengan kata lain, kondisi mental seseorang akan menentukan kesimpulan tinggi rendahnya risiko tertentu. Sebagai contoh, untuk standar deviasi *return* pasar yang sama sebesar 25%, dua orang dengan kepribadian berbeda akan mempunyai cara pandang yang berbeda. Orang yang konservatif akan menganggap risiko investasi di pasar modal terlalu tinggi. Sementara bagi orang yang agresif, risiko investasi di pasar modal dianggap tidak terlalu tinggi. Perhatikan bahwa kedua orang tersebut melihat pada risiko objektif yang sama, yaitu standar deviasi *return* sebesar 25% per tahun.

Berikut ini contoh-contoh risiko yang biasa dihadapi oleh suatu organisasi. Risiko-risiko tersebut dikelompokkan ke dalam risiko murni dan spekulatif.

Tabel 1.2.
Contoh-contoh Risiko Murni

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko Aset Fisik	Risiko yang terjadi karena kejadian tertentu berakibat buruk (kerugian) pada aset fisik organisasi.	Kebakaran yang melanda gudang atau bangunan perusahaan. Banjir mengakibatkan kerusakan pada bangunan dan peralatan
Risiko karyawan	Risiko karena karyawan organisasi mengalami peristiwa yang merugikan	Kecelakaan kerja mengakibatkan karyawan cedera, kegiatan operasional perusahaan terganggu
Risiko legal	Risiko kontrak tidak sesuai yang diharapkan, dokumentasi yang tidak benar	Terjadi perselisihan sehingga perusahaan lain menuntut ganti rugi yang signifikan

Tabel 1.3.

Contoh-Contoh Risiko Spekulatif

TIPE RISIKO	DEFINISI	ILUSTRASI
Risiko pasar	Risiko yang terjadi dari pergerakan harga atau volatilitas harga pasar	Harga pasar saham dalam portofolio perusahaan mengalami penurunan, yang mengakibatkan kerugian yang dialami perusahaan.
Risiko kredit	Risiko karena *counter party* gagal memenuhi kewajibannya kepada perusahaan	Debitur tidak bisa membayar cicilan dan bunga hutang, sehingga perusahaan mengalami kerugian. Piutang dagang tidak terbayar.
Risiko Likuiditas	Risiko tidak bisa memenuhi kebutuhan kas, risiko tidak bisa menjual dengan cepat karena ketidaklikuidan atau gangguan pasar	Perusahaan tidak mempunyai kas untuk membayar kewajibannya (misal melunasi hutang). Perusahaan terpaksa menjual tanah dengan harga murah (di bawah standar) karena sulit menjual tanah tersebut (tidak likuid), padahal perusahaan membutuhkan kas dengan cepat.
Risiko operasional	Risiko kegiatan operasional tidak berjalan lancar dan mengakibatkan kerugian: kegagalan sistem, human error, pengendalian dan prosedur yang kurang	Komputer perusahaan terkena virus sehingga operasi perusahaan terganggu. Prosedur pengendalian perusahaan tidak memadai sehingga terjadi pencurian barang-barang yang dimiliki perusahaan.

Pembagian risiko ke dalam dua tipe, yaitu risiko murni dan risiko spekulatif, barangkali tidak sepenuhnya memuaskan. Ada beberapa jenis risiko yang barangkali bisa masuk ke dalam risiko murni maupun spekulatif. Sebagai contoh, risiko tuntutan hukum bisa dimasukkan ke dalam risiko murni, tetapi jika dilihat sebagai konsekuensi kegiatan bisnis, maka risiko tersebut bisa dimasukkan ke dalam risiko spekulatif. Pembagian semacam itu bukan 'harga mati'. Pembagian semacam itu diharapkan memudahkan kita memahami jenis-jenis risiko dan karakteristiknya.

C. PROSES MANAJEMEN RISIKO

Risiko ada di mana-mana, bisa datang kapan saja, dan sulit dihindari. Jika

risiko tersebut menimpa suatu organisasi, maka organisasi tersebut bisa

mengalami kerugian yang signifikan. Dalam beberapa situasi, risiko tersebut bisa mengakibatkan kehancuran organisasi tersebut. Karena itu risiko penting untuk dikelola. Manajemen risiko bertujuan untuk mengelola risiko tersebut sehingga kita bisa memperoleh hasil yang paling optimal. Dalam konteks organisasi, organisasi juga akan menghadapi banyak risiko. Jika organisasi tersebut tidak bisa mengelola risiko dengan baik, maka organisasi tersebut bisa mengalami kerugian yang signifikan. Karena itu risiko yang dihadapi oleh organisasi tersebut juga harus dikelola, agar organisasi bisa bertahan, atau barangkali mengoptimalkan risiko. Perusahaan sering kali secara sengaja mengambil risiko tertentu, karena melihat potensi keuntungan dibalik risiko tersebut.

Manajemen risiko pada dasarnya dilakukan melalui proses-proses berikut ini.

1. Identifikasi risiko.
2. Evaluasi dan Pengukuran Risiko, dan
3. Pengelolaan risiko.

1. Identifikasi Risiko

Identifikasi risiko dilakukan untuk mengidentifikasi risiko-risiko apa saja yang dihadapi oleh suatu organisasi. Banyak risiko yang dihadapi oleh suatu organisasi, mulai dari risiko penyelewengan oleh karyawan, risiko kejatuhan meteor atau komet, dan lainnya. Ada beberapa teknik untuk mengidentifikasi risiko, misal dengan menelusuri sumber risiko sampai terjadinya peristiwa yang tidak diinginkan. Sebagai contoh, kompor ditaruh dekat penyimpanan minyak tanah. Api merupakan sumber risiko, kompor yang ditaruh dekat minyak tanah merupakan kondisi yang meningkatkan terjadinya kecelakaan, bangunan yang bisa terbakar merupakan *eksposur* yang dihadapi perusahaan. Misalkan terjadi kebakaran, kebakaran merupakan peristiwa yang merugikan (peril). Identifikasi semacam dilakukan dengan melihat sekuen dari sumber risiko sampai ke terjadinya peristiwa yang merugikan. Pada beberapa situasi, risiko yang dihadapi oleh perusahaan cukup standar. Sebagai contoh, bank menghadapi risiko terutama adalah risiko kredit (kemungkinan debitur tidak melunasi hutangnya). Untuk bank yang juga aktif melakukan perdagangan sekuritas, maka bank tersebut akan menghadapi risiko pasar. Setiap bisnis akan menghadapi risiko yang berbeda-beda karakteristiknya.

2. Evaluasi dan Pengukuran Risiko

Langkah berikutnya adalah mengukur risiko tersebut dan mengevaluasi risiko tersebut. Tujuan evaluasi risiko adalah untuk memahami karakteristik risiko dengan lebih baik. Jika kita memperoleh pemahaman yang lebih baik, maka risiko akan lebih mudah dikendalikan. Evaluasi yang lebih sistematis dilakukan untuk 'mengukur' risiko tersebut.

Ada beberapa teknik untuk mengukur risiko tergantung jenis risiko tersebut. Sebagai contoh kita bisa memperkirakan probabilitas (kemungkinan) risiko atau suatu kejadian jelek terjadi. Dengan probabilitas tersebut kita berusaha 'mengukur' risiko. Sebagai contoh, ada risiko perusahaan terkena jatuhan meteor atau komet, tetapi probabilitas risiko semacam itu sangat kecil (0,000000001). Karena itu risiko tersebut tidak perlu diperhatikan. Contoh lain adalah risiko kebakaran dengan probabilitas (misal) 0,6. Karena probabilitas yang tinggi, maka risiko kebakaran perlu diberi perhatian ekstra. Contoh tersebut menunjukkan bahwa dengan menggunakan teknik probabilitas kita bisa melakukan prioritisasi risiko, sehingga kita bisa lebih memfokuskan pada risiko yang mempunyai kemungkinan yang besar untuk terjadi.

Contoh lain adalah membuat matriks dengan sumbu mendatar adalah probabilitas terjadinya risiko, dan sumbu vertikal adalah tingkat keseriusan konsekuensi risiko tersebut (*severity*, atau besarnya kerugian yang timbul akibat risiko tersebut). Setiap risiko bisa dievaluasi kemudian dimasukkan ke dalam matriks tersebut. Sebagai contoh, risiko kebakaran mempunyai probabilitas 0,6 (tinggi). Jika kebakaran terjadi, maka kerugian yang diakibatkan akan besar juga (tinggi). Dengan demikian risiko kebakaran akan ditempatkan pada kuadran probabilitas tinggi dan *severity* tinggi. Selanjutnya langkah yang lebih tepat bisa dirumuskan. Sebagai contoh, untuk risiko kebakaran seperti itu, langkah yang lebih aktif bisa ditujukan untuk menangani risiko kebakaran tersebut.

Untuk risiko lain, evaluasi dan pengukuran yang berbeda bisa dilakukan. Sebagai contoh, risiko perubahan tingkat bunga bisa diukur dengan teknik duration (durasi). Modul identifikasi dan pengukuran risiko spekulatif akan banyak membicarakan pengukuran risiko perubahan tingkat bunga. Risiko pasar bisa dievaluasi dengan menggunakan teknik VAR (*Value At Risk*). Pemahaman kita terhadap beberapa risiko sudah cukup baik sehingga teknik pengukuran risiko tersebut sudah berkembang. Sementara pemahaman kita terhadap risiko lain belum begitu baik sehingga teknik pengukuran risiko tersebut belum begitu berkembang.

Teknik lain untuk mengukur risiko adalah dengan mengevaluasi dampak risiko tersebut terhadap kinerja perusahaan.

3. Pengelolaan Risiko

Setelah analisis dan evaluasi risiko, langkah berikutnya adalah mengelola risiko. Risiko harus dikelola. Jika organisasi gagal mengelola risiko, maka konsekuensi yang diterima bisa cukup serius, misal kerugian yang besar. Risiko bisa dikelola dengan berbagai cara, seperti penghindaran, ditahan (*retention*), diversifikasi, atau ditransfer ke pihak lainnya. Erat kaitannya dengan manajemen risiko adalah pengendalian risiko (*risk control*), dan pendanaan risiko (*risk financing*).

a. Penghindaran. Cara paling mudah dan aman untuk mengelola risiko adalah menghindar. Tetapi cara semacam ini barangkali tidak optimal. Sebagai contoh, jika kita ingin memperoleh keuntungan dari bisnis, maka mau tidak mau kita harus keluar dan menghadapi risiko tersebut. Kemudian kita akan mengelola risiko tersebut.
b. Ditahan (*Retention*). Dalam beberapa situasi, akan lebih baik jika kita menghadapi sendiri risiko tersebut (menahan risiko tersebut, atau *risk retention*). Sebagai contoh, misalkan seseorang akan keluar rumah membeli sesuatu dari supermarket terdekat, dengan menggunakan kendaraan. Kendaraan tersebut tidak diasuransikan. Orang tersebut merasa asuransi terlalu repot, mahal, sementara dia akan mengendarai kendaraan tersebut dengan hati-hati. Dalam contoh tersebut, orang tersebut memutuskan untuk menanggung sendiri (menahan, *retention*) risiko kecelakaan.
c. Diversifikasi. Diversifikasi berarti menyebar eksposur yang kita miliki sehingga tidak terkonsentrasi pada satu atau dua eksposur saja. Sebagai contoh, kita barangkali akan memegang aset tidak hanya satu, tetapi pada beberapa aset, misal saham A, saham B, obligasi C, properti, dan sebagainya. Jika terjadi kerugian pada satu aset, kerugian tersebut diharapkan bisa dikompensasi oleh keuntungan dari aset lainnya.
d. Transfer Risiko. Jika kita tidak ingin menanggung risiko tertentu, kita bisa mentransfer risiko tersebut ke pihak lain yang lebih mampu menghadapi risiko tersebut. Sebagai contoh, kita bisa membeli asuransi kecelakaan. Jika terjadi kecelakaan, perusahaan asuransi akan menanggung kerugian dari kecelakaan tersebut.

e. Pengendalian Risiko. Pengendalian risiko dilakukan untuk mencegah atau menurunkan probabilitas terjadinya risiko atau kejadian yang tidak kita inginkan. Sebagai contoh, untuk mencegah terjadinya kebakaran, kita memasang alarm asap di bangunan kita. Alarm tersebut merupakan salah satu cara kita mengendalikan risiko kebakaran.
f. Pendanaan Risiko. Pendanaan risiko mempunyai arti bagaimana 'mendanai' kerugian yang terjadi jika suatu risiko muncul. Sebagai contoh, jika terjadi kebakaran, bagaimana menanggung kerugian akibat kebakaran tersebut, apakah dari asuransi, ataukah menggunakan dana cadangan? Isu semacam itu masuk dalam wilayah pendanaan risiko.

Di samping proses manajemen risiko seperti yang disebutkan di muka, manajemen risiko suatu organisasi juga memerlukan infrastruktur baik keras maupun lunak. Sebagai contoh, manajemen risiko barangkali akan memerlukan sistem komputer untuk analisis risiko. Manajemen risiko juga memerlukan staf dan struktur organisasi yang tepat. Infrastruktur manajemen risiko tidak dibahas secara khusus dalam modul ini. Modul enam menyajikan ilustrasi bagaimana perusahaan terkemuka dunia mengembangkan manajemen risiko dalam organisasinya.

Enterprise Risk Management

Makhluk hidup secara natural akan mengantisipasi dan 'mengelola' risiko. Sebagai contoh, jika kita keluar mengendarai mobil, maka kita akan waspada dengan kondisi sekitarnya. Jika dari arah yang berlawanan ada mobil yang agak ke tengah jalannya, kita akan menghindari mobil tersebut dengan jalan mengendarainya agak ke kiri, supaya tidak terjadi tabrakan. Konon binatang mempunyai indera keenam yang bisa mendeteksi risiko lebih baik dibandingkan manusia. Pada waktu tsunami melanda wilayah Asia pada tahun 2004, binatang (gajah, dan sebagainya) yang menjadi korban tsunami jauh lebih kecil dibandingkan manusia. Binatang tersebut sepertinya mampu mendeteksi datangnya bahaya, kemudian menyingkir sebelum bahaya tersebut datang. Konon manusia dulu juga mempunyai kemampuan yang serupa, tetapi karena tidak banyak digunakan, karena manusia lebih banyak mengandalkan otak mereka, kemampuan indera keenam tersebut menghilang. Bagaimana dengan organisasi? Organisasi tidak mempunyai kemampuan mengelola risiko seperti halnya manusia atau makhluk hidup mengelola risiko, karena organisasi bukan makhluk hidup. Tugas dari manajer suatu organisasi adalah membuat agar organisasi bisa mengantisipasi dan mengelola risiko

sebagaimana halnya makhluk hidup mengelola risiko yang dihadapinya. Dengan kata lain, tugas manajer adalah membuat organisasi menjadi sadar risiko, sehingga risiko bisa diantisipasi dan dikelola dengan baik.

Tabel 1.4 berikut ini menyajikan konsekuensi merugikan jika suatu organisasi gagal mengelola risiko

Tabel 1.4.
Beberapa Contoh Kegagalan Mengelola Risiko

Tahun	Penjelasan
1997	Trader Bank Baring (Nick Leeson) membeli *instrument derivative* saham Jepang (futures Nikkei). Bank Baring adalah Bank dari Inggris. Ekonomi Jepang turun drastic karena ada bencana gempa Kobe. Akibatnya dia mengalami kerugian besar. Transaksi selanjutnya (jual opsi) tidak mengurangi kerugian, tetapi memperparah kerugian. Pada akhirnya Bank Baring mengalami kerugian sebesar $1,3 miliar. Bank Baring terpaksa bangkrut karena kerugiannya sudah melebihi modalnya.

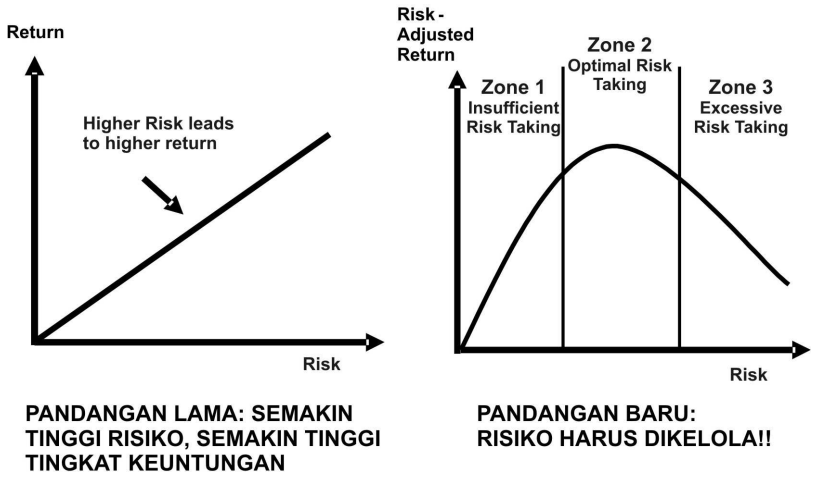
Tahun	Penjelasan
1997	Long Term Capital (LTC), perusahaan investasi di Amerika Serikat, mempunyai posisi pada mata uang Rusia Rubel yang cukup besar. Mereka memperkirakan Rusia tidak akan bangkrut. Tetapi Rusia ternyata bangkrut, mendeklarasikan tidak mampu dan tidak akan membayar hutang-hutangnya. Akibatnya *Long Term Capital* mengalami kerugian yang sangat besar, sekitar $3,5 miliar, dan pada akhirnya LTC terpaksa bangkrut.
2001	Enron merupakan perusahaan yang memperdagangkan energi (jual beli energi). Mereka juga masuk ke kontrak *derivative* energi. Usaha mereka cukup kompleks sehingga transparansi menjadi lebih sulit. Transparansi yang kompleks dimanfaatkan untuk menjalankan sistem akuntansi yang tidak wajar. Di samping itu Enron melakukan beberapa *manuever* agar laporan keuangannya kelihatan baik. Akhirnya investor mengetahui trik-trik mereka. Keuntungan mereka yang sesungguhnya ternyata tidak sebesar yang dilaporkan. Harga saham Enron jatuh dari $80 per lembar menjadi hanya $0,5. Mereka mempunyai kewajiban jangka pendek yang segera jatuh tempo. Mereka tidak bisa memperoleh bantuan dana. Tidak ada yang percaya dengan mereka. Enron akhirnya bangkrut.
1980-an	*Saving Loan* (S & L) *Association* (bank yang memberi pinjaman kredit rumah di Amerika Serikat) mempunyai struktur neraca: memberi kredit rumah dengan bunga tetap jangka panjang (misal 20 tahun), sementara memperoleh dana melalui deposito jangka pendek (misal 1 tahun). Struktur semacam itu rentan terhadap risiko perubahan tingkat bunga. Pada waktu tingkat bunga di Amerika Serikat naik signifikan pada tahun 1980-an, banyak S & L yang mengalami masalah dan puluhan S & L bangkrut karenanya.
1995	Bank Duta (Indonesia) mengalami kerugian yang sangat besar karena mereka melakukan perdagangan valas dan mengalami kerugian besar dari perdagangan valas tersebut.

Pertanyaan yang muncul adalah bisakah organisasi-organisasi di atas menghindari kerugian besar karena munculnya risiko-risiko tersebut? Manajemen risiko organisasi bertujuan menciptakan sistem atau mekanisme dalam organisasi sehingga risiko yang bisa merugikan organisasi bisa diantisipasi dan dikelola untuk tujuan meningkatkan nilai perusahaan.

Pentingnya pengelolaan risiko juga bisa dilihat melalui Bagan 1.1 berikut ini. Bagan 1.1 tersebut menggambarkan pandangan lama (sebelah kiri) dan baru (sebelah kanan) dalam kaitannya antara risiko dengan tingkat keuntungan. Pandangan lama menganggap ada hubungan positif antara risiko dengan tingkat keuntungan. Semakin tinggi risiko, akan semakin tinggi tingkat keuntungan yang diharapkan. Jika suatu organisasi ingin meningkatkan tingkat

keuntungannya, maka organisasi tersebut harus menaikkan risikonya.

Pandangan baru mengatakan bahwa hubungan antara risiko dengan tingkat keuntungan tidak bersifat linear, tetapi non-linear. Pada wilayah satu, risiko yang diambil oleh perusahaan terlalu kecil, sehingga keuntungan yang diperoleh juga kecil. Pada tahap ini, risiko masih bisa ditingkatkan untuk meningkatkan tingkat keuntungan. Contoh ekstrem situasi ini adalah jika manajer hanya tinggal di rumah, tidak pergi ke mana-mana. Dia bisa menghindari banyak risiko (risiko kecelakaan, dan sebagainya), tetapi dia juga tidak mendapatkan banyak keuntungan. Di tahap ini, pengelolaan risiko belum optimal.



Gambar 1.3.
Hubungan Risiko dan Tingkat Keuntungan (*Return*): Pandangan Lama dan Baru

Pada tahap berikutnya (zona 2), penambahan risiko tidak banyak meningkatkan tingkat keuntungan. Tahap ini merupakan tahap optimal. Tahap berikutnya (zona 3), risiko yang diambil organisasi terlalu tinggi, sehingga penambahan risiko akan berakibat negatif terhadap organisasi. Sebagai contoh, bank memberi pinjaman pada sektor-sektor yang risikonya terlalu tinggi, misal usaha burung walet, usaha perjudian. Risiko yang terlalu tinggi menjadi sulit untuk dikendalikan, sehingga bisa berakibat membahayakan dan merugikan perusahaan. Berdasarkan kerangka tersebut, pengelolaan risiko organisasi seharusnya berada pada wilayah tengah (zona 2), yang merupakan zona optimal.

Pengelolaan risiko yang digambarkan dalam bagan di atas bisa diilustrasikan melalui perjalanan dengan menggunakan kendaraan (mobil). Mobil yang berjalan terlalu lambat barangkali tidak menguntungkan, karena beberapa hal, misal terlalu lama, atau bahkan bisa membahayakan kendaraan lainnya. Mobil tersebut perlu dipacu lebih cepat. Jika mobil berjalan terlalu cepat (misal, ngebut), maka risiko bertabrakan atau kehilangan kendali menjadi semakin besar. Tentu saja hal ini tidak menguntungkan. Yang paling optimal adalah mobil berjalan dengan kecepatan optimal, yaitu cukup cepat tetapi bisa dikendalikan. Pengelolaan risiko bisa diilustrasikan sebagai kombinasi penekanan gas (mempercepat kendaraan) dan penekanan rem (memperlambat kendaraan). Kombinasi yang ideal bisa membuat mobil berjalan kencang tetapi tetap terkendali.

B. DEFINISI DAN PENGERTIAN MANAJEMEN RISIKO

Manajemen risiko organisasi adalah suatu sistem pengelolaan risiko yang dihadapi oleh organisasi secara komprehensif untuk tujuan meningkatkan nilai perusahaan. Meskipun pengertian manajemen risiko organisasi adalah seperti yang disebutkan di atas, tetapi ada banyak definisi dan pengertian manajemen risiko organisasi. Berikut ini beberapa definisi manajemen risiko organisasi.

Manajemen risiko adalah seperangkat kebijakan, prosedur yang lengkap, yang dipunyai organisasi, untuk mengelola, memonitor, dan mengendalikan eksposur organisasi terhadap risiko (SBC Warburg, *The Practice of Risk Management*, Euromoney Book, 2004)

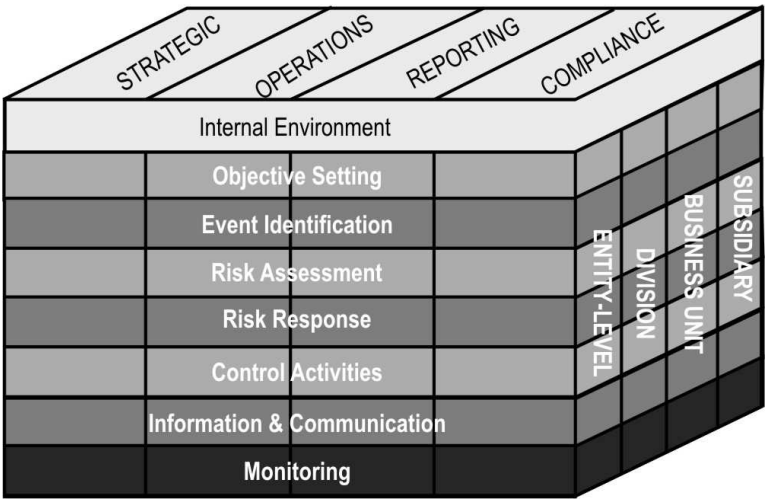
Enterprise Risk Management adalah kerangka yang komprehensif, terintegrasi, untuk mengelola risiko kredit, risiko pasar, modal ekonomis, transfer risiko, untuk memaksimumkan nilai perusahaan (Lam, James, *Enterprise Risk Management*, Wiley, 2004)

Manajemen risiko organisasi mempunyai elemen-elemen berikut ini:
Identifikasi Misi: Menetapkan Tujuan manajemen risiko.
Penilaian Risiko dan Ketidakpastian: Mengidentifikasi dan mengukur risiko.
Pengendalian Risiko: Mengendalikan risiko melalui diversifikasi, asuransi, hedging, penghindaran, dan lain-lain.

Pendanaan Risiko: Bagaimana membiayai manajemen risiko.
Administrasi program: Administrasi organisasi, seperti manual, dan sebagainya.
(Williams, Smith, Young, *Risk Management and Insurance*, McGraw Hill, 1998)

Enterprise Risk Management (ERM) adalah suatu proses, yang dipengaruhi oleh manajemen, board of directors, dan personel lain dari suatu organisasi, diterapkan dalam setting strategi, dan mencakup organisasi secara keseluruhan, didisain untuk mengidentifikasi kejadian potensial yang mempengaruhi suatu organisasi, mengelola risiko dalam toleransi suatu organisasi, untuk memberikan jaminan yang cukup pantas berkaitan dengan pencapaian tujuan organisasi. (COSO, *COSO Enterprise Risk Management – Integrated Framework.* COSO, 2004) .

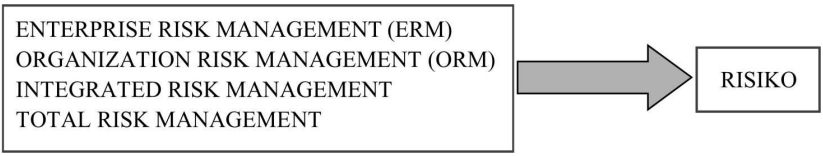
Selanjutnya COSO menampilkan format berikut ini yang menunjukkan bahwa ERM adalah manajemen risiko yang komprehensif (Lihat bagan berikut ini).



Gambar 1.4.
COSO – *Enterprise Risk Management*

Gambar 1.4 tersebut menunjukkan delapan komponen ERM yaitu (1) lingkungan internal, (2) penentuan tujuan, (3) Identifikasi kejadian, (4) Evaluasi (*assessment*) risiko, (5) Respons terhadap risiko, (6) Aktivitas pengendalian, (7) Informasi dan komunikasi, (8) Monitoring. Risiko yang dikelola mencakup risiko strategis, operasi, pelaporan, dan kepatuhan (*compliance*). Kemudian ERM mencakup keseluruhan organisasi, mulai dari level perusahaan keseluruhan (*entity level*), level divisi, level unit bisnis, dan level anak perusahaan (*subsidiary*).

Perhatikan bahwa definisi-definisi tersebut menggunakan istilah yang beragam untuk menjelaskan manajemen risiko organisasi, seperti terlihat pada bagan berikut ini.



Gambar 1.5.
Beberapa Istilah Manajemen Risiko Organisasi

Kemudian, ciri lain dari definisi tersebut adalah pengelolaan risiko yang komprehensif, dan bertujuan mencapai tujuan organisasi. Dengan menggabungkan beberapa karakteristik tersebut, bagan berikut ini menyajikan pengertian manajemen risiko suatu organisasi yang menjadi acuan modul ini.

Gambar 1.6.
Kerangka Manajemen Risiko Organisasi

Gambar 1.6 tersebut menunjukkan manajemen risiko organisasi (*enterprise risk management*) terdiri dari dua elemen besar: (1) Infrastruktur atau prasarana, yang terdiri dari prasarana lunak dan keras, dan (2) Proses Manajemen Risiko. Kemudian manajemen risiko organisasi bertujuan membantu pencapaian tujuan organisasi, dalam hal ini dirumuskan secara eksplisit menjadi memaksimumkan nilai perusahaan.

C. ELEMEN MANAJEMEN RISIKO ORGANISASI

Misalkan kita ditugaskan untuk membuat dan memimpin departemen manajemen risiko suatu perusahaan, bagaimana kita memulainya? Bagan di atas menunjukkan kerangka yang bisa digunakan untuk memulai membangun departemen manajemen risiko. Pertama, kita harus menyiapkan prasarana yang diperlukan untuk memulai pekerjaan manajemen risiko, yang meliputi prasarana lunak (non-fisik) dan prasarana keras (fisik).

1. Prasarana Manajemen Risiko

Salah satu hal yang penting dikerjakan untuk mempersiapkan manajemen risiko adalah menyiapkan prasarana yang mendukung manajemen risiko, yang meliputi prasarana lunak dan keras.

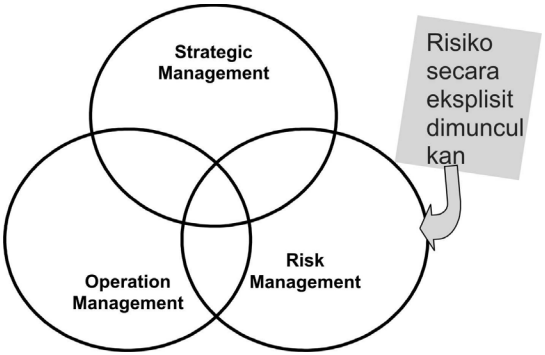
a. Prasarana lunak

Ada beberapa isu yang berkaitan dengan penyiapan prasarana lunak untuk manajemen risiko, yaitu: (1) Mengembangkan budaya sadar risiko untuk anggota organisasi, (2) Dukungan manajemen.

Mengembangkan Budaya Sadar Risiko. Tujuan dari budaya sadar risiko adalah agar setiap anggota organisasi sadar adanya risiko, dan mengambil keputusan tertentu dengan mempertimbangkan aspek risikonya. Dengan singkat, tujuan budaya sadar risiko adalah agar anggota lebih berhati-hati dalam pengambilan keputusan. Jika anggota tersebut sadar akan risiko, maka organisasi (yang terdiri dari kumpulan individu) akan menjadi lebih peka terhadap risiko.

Bagaimana mengembangkan perilaku yang sadar risiko untuk anggota organisasi? Salah satu cara yang bisa dilakukan adalah dengan memaksa mereka untuk berpikir risiko untuk setiap keputusan yang akan diambil. Pebisnis secara natural adalah orang yang optimis (karena itu mereka berani terjun ke dunia bisnis), dan cenderung melupakan aspek risiko (yang mendorong mereka untuk lebih berhati-hati). Jika dipaksa untuk berpikir mengenai risiko, maka mereka akan lebih seimbang dalam memutuskan sesuatu.

Sebagai contoh, bagan berikut ini menunjukkan tiga aspek yang harus dipikirkan oleh manajer dalam pengambilan keputusan, yaitu aspek strategis, operasi, dan risiko. Evaluasi terhadap risiko yang mungkin terjadi harus dipikirkan dan dilaporkan secara eksplisit.



Gambar 1.7.
Aspek Risiko Yang Dimunculkan Secara Eksplisit

Misalkan seorang manajer akan meluncurkan produk baru. Dia harus memikirkan tiga aspek yang disebutkan di atas, dengan pertanyaan seperti berikut ini.

1) Aspek Strategis: Apakah produk ini bisa memenuhi kebutuhan konsumen? Apakah produk ini bisa membantu pencapaian tujuan perusahaan (mencapai target keuntungan tertentu)?
2) Aspek Operasi: Bagaimana memproduksi produk ini? Apakah perusahaan mempunyai kemampuan memproduksi produk ini? Bagaimana memasarkan dan mengembangkan jaringan distribusi untuk produk ini?
3) Aspek Risiko: Risiko apa saja yang bisa muncul berkaitan dengan peluncuran produk ini? Bagaimana perusahaan bisa mengendalikan risiko-risiko tersebut?

Perhatikan pertanyaan aspek risiko secara eksplisit dimunculkan. Misalkan seorang manajer akan meluncurkan program promosi/iklan. Dia harus memikirkan tiga aspek yang disebutkan di atas, melalui pertanyaan-pertanyaan berikut ini.

1) Aspek Strategis: Bagaimana strategi promosi yang efektif? Bagaimana kontribusi promosi ini terhadap tujuan organisasi?
2) Aspek Operasi: Bagaimana menjalankan program promosi ini? Media apa yang paling efektif? Bagaimana *timing* (waktu yang tepat) untuk promosi ini? Bagaimana aspek detil lainnya dari promosi ini? Bagaimana

mengendalikan risiko-risiko yang barangkali muncul akibat peluncuran program promosi ini?

3) Aspek Risiko: Risiko apa yang potensial muncul akibat dari program promosi ini? Apakah promosi ini bisa menimbulkan gugatan hukum? Apakah promosi ini sudah etis? Pihak-pihak mana saja yang barangkali berkeberatan dengan promosi ini?

Perhatikan bahwa sama seperti sebelumnya, aspek risiko secara eksplisit perlu dipikirkan dan dimunculkan. Jika manajer terbiasa berpikir secara eksplisit mengenai risiko-risiko yang mungkin muncul, maka manajer tersebut akan semakin sadar terhadap risiko. Jika semua anggota organisasi sadar akan risiko, maka organisasi menjadi lebih sadar dan lebih peka terhadap risiko.

Mengembangkan kesadaran risiko juga bisa dilakukan melalui *workshop* atau pertemuan secara berkala antar manajer atau anggota organisasi. Agenda dalam *workshop* tersebut adalah membicarakan kejadian-kejadian yang bisa menimbulkan dampak yang negatif terhadap organisasi, alternatif-alternatif pemecahannya. *Workshop* tersebut bisa dikelola oleh manajer risiko perusahaan atau departemen risiko perusahaan. Melalui *workshop* atau pertemuan yang regular yang membicarakan risiko dengan segala aspeknya yang relevan, anggota organisasi diharapkan menjadi lebih sadar akan risiko yang dihadapi organisasi.

Teknik lain yang bisa digunakan adalah memasukkan risiko ke dalam elemen penilaian kinerja. Sebagai contoh, alokasi modal diberikan kepada usulan investasi yang memberikan *risk-adjusted return* (tingkat keuntungan setelah disesuaikan dengan risikonya) yang paling tinggi. Jika kriteria semacam itu yang akan dipakai, maka organisasi akan secara langsung 'menghukum' manajer yang berperilaku risiko tinggi. Risiko tinggi bisa dibenarkan sepanjang memberikan tingkat keuntungan yang diharapkan yang lebih tinggi juga. Dengan mekanisme evaluasi semacam itu, manajer diharapkan akan lebih sadar mengenai risiko, dan budaya risiko di organisasi akan menjadi semakin baik (semakin sadar akan risiko).

Dukungan Manajemen. Sama seperti program lainnya, dukungan manajemen khususnya manajemen puncak terhadap program manajemen risiko penting diberikan. Bentuk dukungan bisa eksplisit maupun implisit. Dukungan manajemen puncak bisa dituangkan antara lain ke dalam pernyataan tertulis, misal manajemen puncak mendukung atau ikut

merumuskan/menyetujui misi dan visi, prosedur dan kebijakan, yang berkaitan dengan manajemen risiko. Dukungan manajemen juga bisa ditunjukkan melalui partisipasi manajemen pada program-program manajemen risiko.

b. Prasarana keras

Di samping prasaran lunak, prasarana keras juga perlu disiapkan. Contoh prasarana keras yang perlu disiapkan adalah ruangan perkantoran, komputer, dan prasarana fisik lainnya. Prasarana fisik tersebut perlu dipersiapkan agar pekerjaan manajemen risiko berjalan sebagaimana mestinya.

2. Proses Manajemen Risiko

Elemen yang lebih penting lagi adalah proses manajemen risiko. Proses atau fungsi manajemen sering diterjemahkan ke dalam tiga langkah: perencanaan, pelaksanaan, dan pengendalian. Mengikuti kebiasaan tersebut, proses manajemen risiko juga bisa dibagi ke dalam tiga tahap yaitu perencanaan, pelaksanaan, dan pengendalian manajemen risiko.

a. Perencanaan

Perencanaan manajemen risiko bisa dimulai dengan menetapkan visi, misi, dan tujuan, yang berkaitan dengan manajemen risiko. Kemudian perencanaan manajemen risiko bisa diteruskan dengan penetapan target, kebijakan, dan prosedur yang berkaitan dengan manajemen risiko. Akan lebih baik lagi jika visi, misi, kebijakan, dan prosedur tersebut dituangkan secara tertulis. Dokumen tertulis semacam itu memudahkan pengarahan, sekaligus menegaskan dukungan manajemen terhadap program manajemen risiko.

Berikut ini beberapa contoh misi atau kebijakan dan prosedur yang berkaitan dengan manajemen risiko dari beberapa perusahaan/organisasi.

PERNYATAAN MISI MANAJEMEN RISIKO GOLDMAN SACH:
Misi dari departemen risiko adalah mengumpulkan, menganalisis, memonitor, dan mendistribusikan informasi yang berkaitan dengan risiko pasar dari posisi perusahaan supaya traders, manajer, dan personel lain dalam organisasi dan terutama komite risiko memahami dan membuat keputusan berdasarkan informasi (informed decisions) mengenai manajemen dan pengendalian risiko yang diambil.
(Goldman Sach adalah perusahaan sekuritas Amerika Serikat)

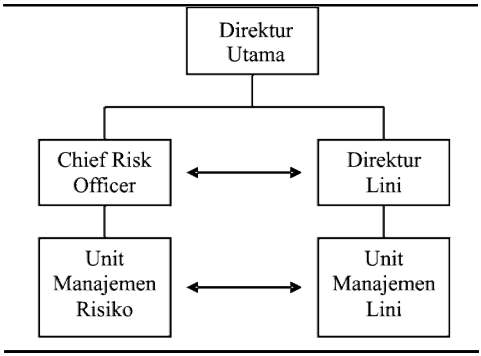
PERNYATAAN MISI SWISS BANK CORPORATION:
Pengendalian risiko Swiss Bank memfokuskan pada perlindungan terhadap modal dan memungkinkan pengambilan risiko yang sesuai. Kepentingan investor Swiss Bank adalah hal yang utama. Modal yang mereka investasikan harus dikompensasi untuk risiko yang ditanggung, baik untuk transaksi individual maupun portofolio.

Setelah misi dan kebijakan serta prosedur yang umum ditetapkan, langkah berikutnya adalah menyusun kebijakan serta prosedur yang lebih spesifik.

b. Pelaksanaan

Pelaksanaan manajemen risiko meliputi aktivitas operasional yang berkaitan dengan manajemen risiko. Proses identifikasi dan pengukuran risiko, kemudian diteruskan dengan manajemen (pengelolaan) risiko merupakan aktivitas operasional yang utama dari manajemen risiko. Identifikasi, pengukuran, dan manajemen risiko akan dibicarakan lebih detil di bagian dua, tiga, dan empat, dari modul ini. Bagian empat khusus membicarakan ilustrasi bagaimana perusahaan menerapkan manajemen risiko secara terencana dan sistematis di organisasinya.

Untuk melaksanakan pekerjaan manajemen risiko, diperlukan organisasi (struktur organisasi) dan *staffing* (personel). Struktur organisasi manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya. Berikut ini contoh struktur organisasi manajemen risiko.

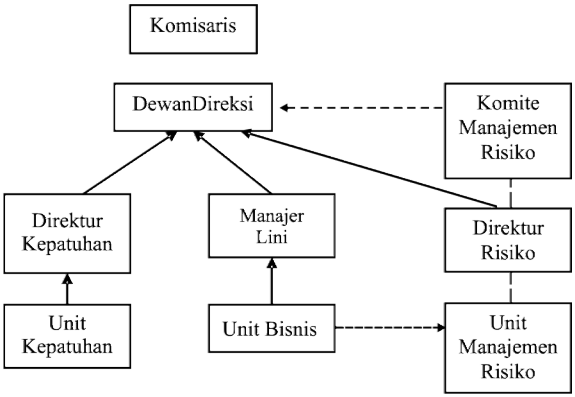


Gambar 1.8.
Struktur Organisasi Manajemen Risiko

Dalam Gambar 1.8 di atas, unit manajemen risiko bertanggung jawab ke manajer risiko yang disebut sebagai *chief risk officer* (CRO). CRO kemudian melapor (bertanggung jawab) langsung ke direktur utama. Pemisahan unit manajemen risiko menjadi bagian sendiri diharapkan mampu menjaga independensi unit manajemen risiko. Unit manajemen risiko mempunyai kedudukan yang sejajar dengan unit lini (pemasaran, keuangan, produksi). Status sebagai unit lini memungkinkan kekuatan yang cukup dalam organisasi untuk mendorong praktek manajemen risiko yang baik dalam suatu organisasi. Unit lini berkomunikasi dengan unit manajemen risiko (seperti ditunjukkan panah dua arah). Komunikasi semacam itu penting agar unit manajemen risiko memperoleh gambaran yang lengkap mengenai risiko yang dihadapi oleh perusahaan.

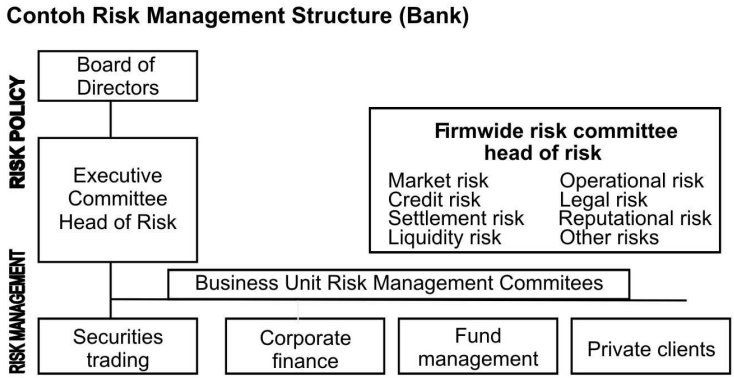
Aspek perilaku dari struktur organisasi manajemen risiko juga perlu diperhatikan. Pekerjaan manajemen risiko cenderung bertentangan dengan pekerjaan manajemen lini. Manajemen lini (misal pemasaran) ingin berjalan cepat tanpa memperhitungkan risiko. Manajemen risiko cenderung menahan keinginan semacam itu dengan mengingatkan risiko-risiko yang mungkin muncul. Struktur organisasi bisa diakomodasi untuk mengatasi potensi konflik semacam itu. Sebagai contoh, unit manajemen risiko bisa dibuat untuk melapor ke manajer risiko dan manajer lini sekaligus. Tetapi cara semacam itu barangkali tidak sempurna, karena pelaporan menjadi tidak jelas (ambigu). Contoh lain, unit manajemen risiko bertanggung jawab ke manajer lini dan memberikan laporan (hubungan garis terputus) kepada manajer risiko. Contoh lain adalah sebaliknya, unit lini bertanggung jawab ke manajer lini dan memberikan laporan ke manajer risiko. Contoh terakhir mirip seperti struktur organisasi pada bagan di atas.

Berikut ini dua contoh variasi dari struktur manajemen risiko.



Gambar 1.9.
Struktur Organisasi Manajemen Risiko Bank

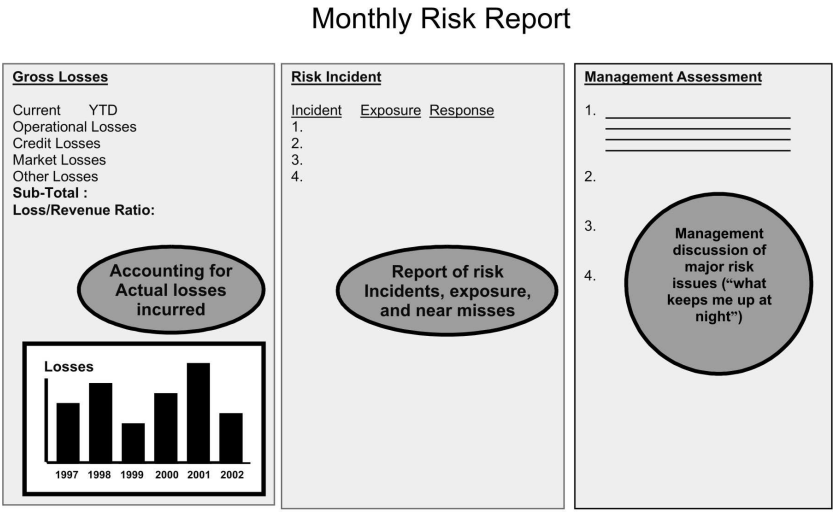
Pada struktur di atas, komite manajemen risiko mengawasi manajemen risiko organisasi. Direktur risiko mengelola kegiatan operasional manajemen risiko. Unit bisnis berkomunikasi dengan unit manajemen risiko untuk melaporkan hal-hal yang berkaitan dengan risiko organisasi. Direktur risiko mempunyai garis keanggotaan kepada komite manajemen risiko.



Gambar 1.10.
Struktur Organisasi Manajemen Risiko Bank (2)

c. Pengendalian

Tahap berikutnya dari proses manajemen risiko adalah pengendalian yang meliputi evaluasi secara periodik pelaksanaan manajemen risiko, output pelaporan yang dihasilkan oleh manajemen risiko, dan umpan balik (*feedback*). Format pelaporan manajemen risiko bervariasi dari satu organisasi ke organisasi lainnya, dan dari satu kegiatan ke kegiatan lainnya. Sebagai contoh, bagan berikut ini menampilkan laporan profil risiko regular (misal bulanan).

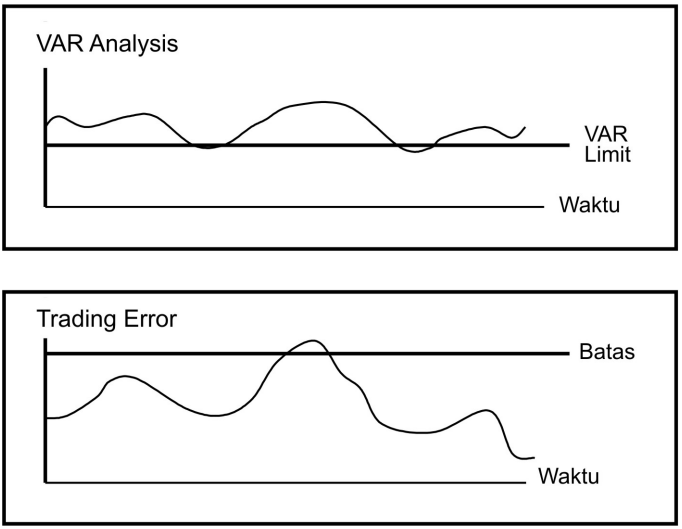


Gambar 1.11.
Contoh Laporan Risiko Bulanan

Gambar 1.11 tersebut menunjukkan laporan kerugian (keuntungan) di sebelah kiri. Gambar di tengah menunjukkan laporan mengenai kejadian-kejadian penting yang menyebabkan perusahaan mengalami kerugian, atau hampir rugi, eksposur perusahaan terhadap kejadian tersebut, dan respons yang dilakukan oleh organisasi. Sebagai contoh, perusahaan barangkali melaporkan kejadian naiknya tingkat bunga sebesar 1% (cukup tinggi). Kemudian perusahaan melaporkan eksposur yaitu posisi obligasi dengan nilai
$10 juta (sepuluh juta dolar AS). Jika tingkat bunga naik, maka nilai obligasi akan turun (yang berarti perusahaan mengalami kerugian). Kolom berikutnya menyajikan respons yang dilakukan perusahaan dalam situasi tersebut (misal

melakukan *hedging*). Bagan paling kanan menunjukkan evaluasi dan diskusi oleh manajemen terhadap risiko-risiko utama yang dihadapi oleh perusahaan.

Unit manajemen risiko bisa juga menampilkan laporan berikut ini.



Gambar 1.12.
Contoh Laporan Risiko Untuk VAR dan *Trading Error*

Kedua bagan tersebut menunjukkan perkembangan VAR (*Value At Risk*, yang merupakan indikator risiko pasar) dan kesalahan perdagangan dari waktu ke waktu. Perusahaan juga menampilkan batas untuk masing-masing variabel risiko tersebut. Jika variabel risiko tersebut masih berada di bawah batas toleransi, maka risiko tersebut belum menunjukkan tingkat keseriusan yang tinggi. Tetapi jika variabel yang diamati tersebut bergerak melewati batas toleransi perusahaan, maka perusahaan harus lebih aktif untuk mengelola risiko tersebut.

Manajer risiko bisa juga menampilkan profil risiko untuk kegiatan tertentu. Sebagai contoh tabel berikut ini menunjukkan profil risiko untuk dua proyek A dan B. Risiko dilihat berdasarkan dimensi keuangan, sosial, dan politik.

Tabel 1.4.
Profil Risiko Usulan Investasi

	Keuangan	Sosial	Politik
Proyek A	1) Tinggi	3)Tinggi 4)Tinggi	5) Tinggi
Proyek B	1)Medium 2)Rendah	3)Medium 4)Rendah	5) Rendah

Keuangan: (1) Risiko kesulitan akses dana, (2) Risiko perubahan kurs
Sosial: (3) Penerimaan masyarakat sekitar, (4) Dukungan pemerintah lokal
Politik: (5) Stabilitas politik, (6) Perubahan Peraturan

Tabel 1.4 tersebut menunjukkan beberapa item risiko untuk keuangan, sosial, dan politik yang dievaluasi. Sebagai contoh, untuk keuangan ada dua item yang dievaluasi, yaitu risiko kesulitan akses dana dan risiko perubahan kurs. Proyek A tidak mempunyai risiko perubahan kurs karena lebih banyak beroperasi di pasar domestik. Dari tabel tersebut terlihat bahwa proyek A nampaknya mempunyai risiko yang lebih besar dibandingkan dengan proyek B. Semua item risiko untuk proyek A mempunyai penilaian risiko yang tinggi. Sedangkan untuk proyek B, kebanyakan item risiko dinilai medium atau rendah. Dengan demikian bisa diambil kesimpulan bahwa proyek A mempunyai risiko yang lebih tinggi dibandingkan dengan proyek B.

Jika pelaporan tersebut belum memuaskan (misal belum cukup informatif), maka format pelaporan bisa di rubah-rubah lagi. Proses umpan balik (*feedback*) harus dijamin bisa berjalan sebagaimana mestinya. Di samping itu hasil evaluasi dari manajemen risiko harus dikomunikasikan ke pihak-pihak yang berkepentingan dan relevan (*stakeholders*). Komunikasi yang baik menjamin disclosure dan transparansi yang baik, yang merupakan elemen manajemen risiko yang baik. Kasus Enron yang bangkrut pada tahun 2001 menunjukkan bahwa organisasi tersebut gagal membangun komunikasi dan transparansi yang baik. Manajemen risiko yang baik harus menjamin terjadinya good corporate governance, diantaranya terjaminnya disclosure dan transparansi yang baik.

Daftar Pustaka

Anderson, Sweeny, and Williams. (1999). *Statistics for Business and Economics*, South-Western Publishing, Cincinnati.

Barton, Thomas, William G. Shenkir, Paul L. Walker. (2002). *Making Enterprise Risk Management Pay Off.* New Jersey: Prentice Hall.

Boodie, Zvi and Robert C. Merton. (2000). *Finance.* New Jersey: Prentice Hall.

Doherty, Neil. (2000). *Integrated Risk Management.* New York: McGraw Hill.

Hanafi, Mamduh. (2005). *Manajemen Keuangan.* Yogyakarta: BPFE.

Hanafi, Mamduh. (2004). *Manajemen Keuangan Internasional.* Yogyakarta: BPFE.

Harrington, Scott E., dan Gregory R. Niehaus. (2003). *Risk Management and Insurance.* Boston: McGraw Hill.

Lam, James. (2004). *Enterprise Risk Management.* Wiley.

Marshall, John F., dan Vipul K. Bansal. (1992). *Financial Engineering, A Complete Guide to Financial Innovation.* New York: Institute of Finance.

Pande, Pete and Larry Holpp. (2002). *What is Six Sigma.* New York.

Risk Group (ed.). (2001). *Advances in Operational Risk.* London: Risk Water Group Ltd.

Saunders and Cornett. (2003). *Financial Institutions Management, A Risk Management Approach*, McGraw Hill.

SBC Warburg. (2004). *The Practice of Risk Management*, Euromoney Book.

Stulz, Rene M. (2003). *Risk Management and Derivatives.* Thomson-South Western.

Trieschmann, dan Gustavson. (1995). *Risk Management and Insurance*, South Western College Publishing.

Williams, C. Arthur, Michael Smith, and Peter C. Young. (1998). *Risk Management and Insurance*, Boston: McGraw Hill.

http ://www. wikip edia. corn.

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **DITA RAHMAWATI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa oranguntuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci: *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak

sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada websiteHyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang

memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

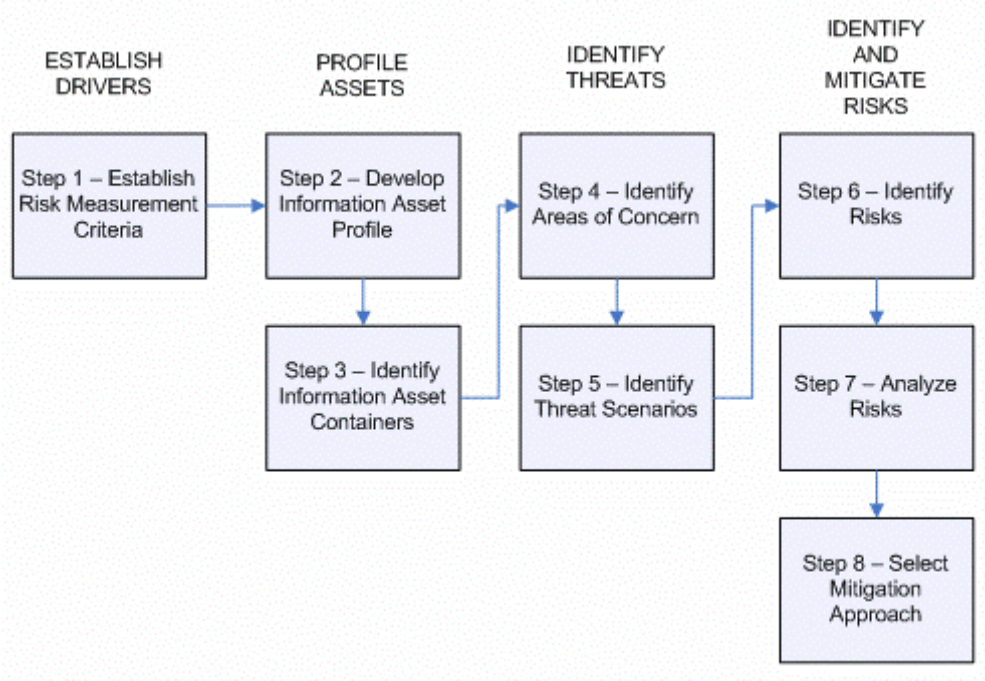
C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untukmencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi.(Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset

informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilaiseberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang

mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian

mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang mengkontak calon pelamar perusahaan tersebut dan data harus diamankan	

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	**Area of Concern**
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat

	dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**

Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	***Risk***			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	Mitigation Approach
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensifdi dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1),43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

Nama : Indri Endang Lestari

Nim : 182420046

Kelas : MTI19AR2

Risk Assessment

Abstrak

Artikel menjelaskan pengukuran tingkat risiko Teknologi Informasi (TI) dan identifikasi praktik keamanan yang cocok dalam penanggulangan risiko, di XYZ. Diharapkan juga perusahaan dapat lebih waspada terhadap dampak risiko TI yang mungkin terjadi dalam PT. XYZ. Metode analisis yang digunakan adalah metode OCTAVE-S. Metode ini digunakan dalam pengukuran risiko TI, dengan beberapa langkah yang berperan penting dalam mencari hasil pengukuran secara efektif dan efisien, yang diterapka pada PT. XYZ. Hasil yang ingin dicapai adalah memberikan keseluruhan hasil pengukuran risiko yang terjadi pada perusahaan, baik kelebihannya maupun kekurangannya, serta memberikan rekomendasi-rekomendasi yang diharapkan dapat mengatasi dan memperbaiki kekurangan maupun permasalahan yang terjadi dalam PT. XYZ. Disimpulkan pengukuran risiko TI yang dilakukan pada PT. XYZ telah berhasil meminimalisasi risiko-risiko yang dapat mengancam keamanan perusahaan.

Pendahuluan

Berkembangnya TI yang sangat pesat saat ini, telah menuntut setiap perusahaan untuk terus bergerak mengikutinya. Oleh karena itu, untuk dapat menghadapi ketatnya persaingan, perusahaan dituntut untuk selalu berkembang, dengan melakukan pengambilan keputusan secara cepat, tepat, dan efisien. TI pada perusahaan, selain memberikan keuntungan juga membawa risiko yang beragam seperti timbulnya kesalahan tanpa disengaja. Misalnya adalah kehilangan data akibat *server* yang terserang virus dan kesalahan yang terjadi karena faktor kesengajaan atau kecurangan. Risiko-risiko yang timbul tersebut akan menimbulkan dampak kerugian bagi perusahaan, baik secara finansial ataupun non finansial. Oleh karena itu, diperlukan suatu pengukuran terhadap risiko yang ada dalam penerapan TI. Pengukuran risiko TI berguna untuk mengetahui profil risiko TI, analisis terhadap risiko, dan juga melakukan respon terhadap risiko, sehingga tidak terjadi dampak-dampak yang kemungkinan muncul dari risiko tersebut. Penerapan TI didukung dengan sistem pengamanan yang kuat, prosedur yang baik, otorisasi yang baik, dan pemeliharaan berkala

terhadap sumber daya komputer, sehingga dapat menjamin keamanan asset perusahaan, pemeliharaan integritas data, dan penggunaan sumber daya yang tepat.

Pembahasan

Dalam pengukuran risiko yang dilakukan pada PT. XYZ, kami telah mengumpulkan dan mengolah data berdasarkan kuisioner yang telah dibagikan kepada Bapak Johan selaku manajer TI dan juga para staf-staf TI lainnya. Kuisioner yang dibagikan digunakan untuk mengetahui kelemahan dari hasil pengukuran risiko serta mencari solusi atas risiko-risiko yang terjadi dalam PT. XYZ. Kuisioner yang dibuat dengan menggunakan metode OCTAVE-S terdiri dari 3 tahap, yaitu: membangun aset berbasis profil ancaman, mengidentifikasi kerentanan infrastruktur, serta mengembangkan strategi keamanan dan perencanaan. Dari ketiga tahap ini, dijabarkan menjadi 5 proses yang terdiri dari 16 aktivitas dan 30 langkah. PT. XYZ saat ini memiliki reputasi yang baik. Hal ini dapat dilihat dari kehilangan pelanggan sebesar 3 persen per tahun. Ini membuktikan bahwa terdapat kesetiaan pelanggan dalam menggunakan jasa perusahaan. Angka tersebut berbanding jauh dengan penambahan pelanggan pada perusahaan selama tahun 2008 ini yang mencapai 10 persen. Dari segi finansial perusahaan, biaya operasional perusahaan dikategorikan sedang karena meningkat 10 persen. Dengan demikian kehilangan pendapatan akan berkurang seiring biaya operasional yang meningkat. Kehilangan pendapatan tersebut diperkirakan sekitar 15 persen. Biaya operasional ini dihabiskan hampir 40 persen untuk kebutuhan TI organisasi. Hal ini dikarenakan perombakan total perusahaan pada awal 2008. Pelanggan yang bertambah mengakibatkan meningkatnya jam kerja untuk menunjang produktivitas perusahaaan. Pada 2008, produktivitas perusahaan bertambah sebesar 20 persen, dan diprediksikan akan terus meningkat sepanjang periode 2009.Perlindungan kesehatan setiap karyawan menjadi tanggungan perusahaan. Untuk masalah kesehatan karyawan, perusahaan memberikan kompensasi sesuai dengan kebijakan yang diterapkan. Ancaman keselamatan pada karyawan dikategorikan rendah karena tidak pernah terjadi ancaman yang berakibat fatal. Untuk hukuman denda memang diberlakukan di dalam perusahaan ini, tetapi hal tersebut semata hanya dilakukan dengan tujuan agar para karyawan dapat lebih mengedepankan kedisiplinan serta profesionalitas kerja.PT. XYZ juga memiliki 15 praktek keamanan, yang diantaranya meliputi sebagai berikut. Pertama adalah kesadaran keamanan dan pelatihan. Dalam perusahaan ini sudah terdapat kesadaran anggota staf yang memahami dan mematuhi kebijakan keamanan, dengan menggunakan *password* yang baik dalam menggunakan sistem yang ada di perusahaan dan sudah terdapat dokumentasi dan verifikasi atas peraturan

keamanan dan tanggung jawab yang harus dipatuhi staf. Tetapi dalam perusahaan ini, pelatihan hanya dilakukan untuk karyawan baru saja dan belum ada pelatihan yang dilakukan secara periodik. Hal ini menunjukkan kesadaran keamanan dan pelatihan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya pelatihan yang dilakukan secara periodik; bukan hanya untuk karyawan baru, tetapi untuk semua karyawan. Hal ini dilakukan supaya kesadaran keamanan karyawan menjadi meningkat. Kedua adalah strategi keamanan. Strategi perusahaan telah secara rutin memasukkan pertimbangan keamanan dan kebijakan, serta strategi keamanan mempertimbangkan tujuan dan strategi bisnis perusahaan. Srategi pengamanan perusahaan telah berjalan dengan baik; tetapi dalam perusahaan ini, strategi pengamanan belum didokumentasikan dan dikaji secara rutin. Hal ini menunjukkan bahwa kesadaran keamanan dan pelatihan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah untuk membuat perubahan strategi bisnis perusahaan, harus ada dokumentasi dan dikaji secara rutin, agar karyawan dalam menjalankan strategi keamanannya menjadi lebih terarah. Ketiga adalah manajemen keamanan. Dalam perusahaan ini, peraturan keamanan telah ditetapkan secara baik oleh perusahaan kepada semua karyawan, prosedurprosedur manajemen keamanan telah didokumentasikan untuk mengawasi semua staf yang bekerja. Tetapi perusahaan ini belum mengalokasikan dana untuk pembiayaan aktivitas keamanan informasi, belum adanya proses yang formal dalam menilai dan mengelola risiko, belum terdapat mekanisme yang resmi dalam menyiapkan manajer dengan ringkasan informasi yang berhubungan dengan keamanan yang penting. Hal ini menunjukkan bahwa manajemen keamanan dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah adanya pengalokasian dana dalam menjaga keamanan informasi, agar segala kerusakan yang muncul dapat segera ditangani; menyediakan proses yang formal dalam menilai dan mengelola risiko; serta menyediakan mekanisme resmi dalam menyiapkan manajer,
dengan ringkasan informasi yang berhubungan dengan keamanan yang penting. Keempat adalah kebijakan keamanan dan peraturan. Dalam perusahaan ini, terdapat peraturan dan kebijakan keamanan informasi, dan diterapkan oleh seluruh staf. Kebijakan tersebut secara berkala ditinjau dan diperbaharui. Tetapi, evaluasi yang dilakukan dalam perusahaan tidak didokumentasikan secara menyeluruh, untuk memastikan pemenuhan kebijakan keamanan informasi. Kesimpulannya adalah peraturan dan kebijakan keamanan perusahaan diperlukan sedikit perbaikan, tetapi tidak terlalu berarti (*Stoplight status YELLOW*). Rekomendasinya adalah perlu

adanya proses yang didokumentasi dalam setiap evaluasi yang dilakukan untuk pemenuhan kebijakan keamanan informasi, agar dapat diketahui setiap evaluasi yang dilakukan pada perusahaan. Kelima adalah manajemen keamanan kolaboratif. Perusahaan telah membuat kebijakan dan prosedur untuk melindungi informasi milik perusahaan lain dalam prosedur kolaborasi. Akan tetapi, tidak tersedia dokumentasi ataupun mekanisme formal terhadap setiap prosedur dan hasil yang ada (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya dokumentasi ataupun mekanisme formal terhadap setiap prosedur dan hasil yang ada. Keenam adalah rencana *contingency*. Perusahaan ini telah mempunyai rencana cadangan yang disediakan untuk menangani kemungkinan buruk yang akan terjadi. Analisis, operasi, aplikasi, dan data yang penting telah dilakukan. Tetapi, belum semua staf menyadari perlunya rencana cadangan, rencana pemulihan bencana, dan rencana untuk menghadapi keadaan darurat. Perusahaan juga belum terdapat dokumentasi seluruh rencana cadangan dan rencana cadangan tersebut belum diuji tingkat keberhasilannya. Hal ini menunjukkan rencana cadangan dan pemulihan dari bencana perlu adanya perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah mendokumentasikan seluruh rencana cadangan untuk menganggapi keadaan darurat menjadi jelas dan mudah untuk diikuti oleh karyawan; serta menguji tingkat keberhasilan rencana cadangan agar keberhasilan dari rencana cadangan tersebut lebih akurat. Ketujuh adalah pengendalian akses fisik. Perusahaan telah mempunyai pengendalian akses fisik yang baik. Dapat dilihat dari rencana keamanan fasilitas dan prosedur untuk menjaga lokasi, bangunan, dan area apapun yang dibatasi telah didokumetasi. Terdapat kebijakan untuk mengendalikan akses fisik ke tempat kerja serta *hardware* dan *software*. Contohnya adalah area bangunan dan tempat kerja, serta tempat server hanya dapat dimasuki oleh orang yang berwenang. Kesimpulannya adalah pengendalian akses fisik dalam perusahaan sudah baik (*Stoplight status GREEN*). Kedelapan adalah Pemantauan dan Audit Keamanan Fisik. Perusahaan telah melakukan hal yang baik dalam mengawasi dan mengaudit keamanan secara fisik. Dapat dilihat dari catatan pemeliharaan yang disimpan untuk mendokumentasi perbaikan dan modifikasi dari komponen fasilitas fisik. Tindakan individu atau grup berkaitan dengan media yang dikontrol dan secara fisik dapat dilaporkan. Adanya catatan audit dan pengawasan secara rutin diperiksa kejanggalannya. Kesimpulannya adalah pengendalian akses fisik dalam perusahaan sudah baik (*Stoplight status GREEN*). Kesembilan adalah sistem dan manajemen jaringan. Dalam perusahaan telah terdapat *firewall* yang di-*update* secara rutin untuk menjaga sistem dan jaringan yang ada dalam perusahaan. Informasi sensitif yang ada dalam perusahaan telah di-*back up daily,*

weekly, *monthly*. Semua sistem dalam perusahaan selalu *up to date* dengan direvisi dan di-*patch*. Perubahan terhadap *hardware* dan *software* direncanakan dan dikontrol. Jika dalam perusahaan terdapat sistem yang tidak diperlukan, maka akan segera dihapus. Dengan demikian, manajemen jaringan dan sistem terdapat beberapa kekurangan (*Stoplight status YELLOW*). Rekomendasinya adalah perlunya mendokumentasikan keseluruhan rencana keamanan utnuk menjaga sistem dan jaringan. Kesepuluh adalah pemantauan dan audit keamanan TI. Dalam perusahaan ini, pengawasan sistem dan jaringan telah dilakukan secara rutin oleh perusahaan. *Firewall* dan komponen keamanan lainnya telah diaudit secara periodic untuk memenuhi persyaratan keamanan. Kesimpulannya adalah pengawasan dan pengauditan keamanan TI dalam perusahaan sudah baik (*Stoplight status GREEN*). Kesebelas adalah pengesahan dan otorisasi. Perusahaan ini telah mempunyai akses kontrol sesuai akses dan otentikasi penggunaan, sesuai dengan kebijakan yang ada untuk membatasi akses pengguna. Dokumentasi kebijakan yang terdapat dalam perusahaan berguna untuk membuat dan mengakhiri hak untuk mengakses informasi. Contohnya adalah adanya *id* dan *password* untuk setiap masing-masing *user*. Metode atau mekanisme yang disediakan untuk memastikan bahwa informasi yang sensitif tidak diakses, diubah ataupun dihancurkan secara tidak sah. Metode atau mekanisme secara periodik ditinjau ulang dan diverifikasi. Kesimpulannya adalah otentikasi dan otorisasi dalam perusahaan sudah baik (*Stoplight status GREEN*). Keduabelas adalah manajemen kerentanan. Dalam perusahaan terdapat prosedur keamanan kerentanan yang telah diikuti dan secara periodik ditinjau, serta terdapat penilaian kerentanan teknologi dan kerentanan dihadapi ketika risiko teridentifikasi. Dengan demikian, manajemen kerentanan terdapat beberapa kekurangan yang tidak terlalu signifikan (*Stoplight status YELLOW*). Rekomendasinya adalah mendokumentasikan seluruh dokumentasi untuk mengelola kerentanan. Ketigabelas adalah enkripsi. Perusahaan telah mengontrol keamanan yang sesuai untuk melindungi informasi yang sensitif selama dalam penyimpanan, misalnya enkripsi data. Enkripsi data dalam perusahaan telah dilakukan dengan baik. Kesimpulannya adalah enkripsi dalam perusahaan sudah baik (*Stoplight status GREEN*). Keempatbelas adalah desain dan arsitektur keamanan. Sebelum membuat arsitektur dan desain untuk system yang baru, perusahaan telah mempertimbangkan strategi keamanan, kebijakan dan prosedur, sejarah keamanan, serta hasil dari penilaian risiko keamanan. Akan tetapi, perusahaan tidak mempunyai diagram *up to date* yang menunjukkan keamanan arsitektur dan topologi jaringan dari perusahaan. Dengan menggunakan diagram *up to date*, lebih mudah dilihat bagaimana perkembangan keamanan

perusahaan. Hal ini menunjukkan arsitektur keamanan dan desain dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah adanya diagram *up to date* untuk menunjukkan bagaimana gambaran perusahaan dalam segi perancangan dan arsitektur keamanan. Kelimabelas adalah manajemen insiden. Perusahaan telah mengikuti prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dengan baik. Tetapi perusahaan belum terdapat dokumentasi atas prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dan pelanggaran. Dalam hal ini, manajemen insiden dalam perusahaan hanya perlu sedikit perbaikan (*Stoplight status YELLOW*). Rekomendasinya adalah perlu adanya dokumentasi atas prosedur dalam mengidentifikasi, melaporkan, dan menanggapi dugaan insiden keamanan dan pelanggaran.

Hasil Identifikasi dan Analisis

Dampak ancaman melalui akses jaringan yang dilakukan oleh internal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi bernilai sedang untuk penyingkapan dan interupsi, dan bernilai tinggi untuk modifikasi dan penghancuran; dampak terhadap finansial pada hasil penyingkapan, modifikasi, dan interupsi bernilai sedang, untuk penghancuran bernilai tinggi; dampak terhadap produktifitas bernilai sedang untuk penyingkapan dan modifikasi, dan tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda bernilai sedang untuk semua hasil ancaman, sedangkan untuk dampak terhadap perlindungan bernilai rendah. Dampak ancaman melalui akses jaringan yang dilakukan oleh internal perusahaan secara sengaja adalah: dampak terhadap reputasi bernilai sedang untuk semua hasil ancaman, sedangkan terhadap finansial bernilai tinggi pada keseluruhan hasil ancaman; dampak terhadap produktifitas bernilai rendah untuk penyingkapan, sedang untuk modifikasi, dan tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda bernilai sedang untuk semua hasil ancaman dan dampak terhadap perlindungan bernilai rendah juga untuk semua hasil ancaman. Dampak ancaman melalui akses jaringan yang dilakukan oleh eksternal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi bernilai sedang untuk penyingkapan dan modifikasi, dan bernilai rendah untuk penghancuran dan interupsi; dampak terhadap finansial bernilai sedang untuk hasil interupsi, dan bernilai tinggi untuk hasil penyingkapan, modifikasi dan penghancuran; dampak terhadap produktifitas bernilai rendah untuk hasil penyingkapan, bernilai sedang untuk hasil modifikasi dan bernilai tinggi untuk hasil penghancuran dan interupsi; serta dampak terhadap denda dan perlindungan masing-masing bernilai sedang dan rendah untuk semua hasil ancaman. Dampak

ancaman melalui akses jaringan yang dilakukan oleh eksternal perusahaan secara sengaja adalah: dampak terhadap reputasi dan finansial, masing-masing bernilai rendah dan tinggi untuk semua hasil ancaman; dampak terhadap produktifitas bernilai rendah untuk penyingkapan, bernilai sedang untuk modifikasi dan bernilai tinggi untuk penghancuran dan interupsi; serta dampak terhadap denda dan perlindungan, sama dengan sebelumnya yaitu masing-masing bernilai sedang dan rendah untuk semua hasil ancaman. Dampak ancaman melalui akses fisik yang dilakukan oleh internal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi, finansial dan denda, bernilai sama yaitu sedang untuk semua hasil ancaman, sedangkan dampak terhadap produktifitas dan perlindungan bernilai rendah untuk semua hasil ancaman. Dampak ancaman melalui akses fisik yang dilakukan oleh internal perusahaan secara sengaja adalah: dampak terhadap reputasi, finansial dan denda bernilai sedang pada semua hasil ancaman, sedangkan untuk perlindungan bernilai rendah; serta dampak pada produktifitas bernilai sedang untuk hasil modifikasi dan penyingkapan, dan bernilai tinggi untuk hasil modifikasi dan interupsi. Dampak ancaman melalui akses fisik yang dilakukan oleh eksternal perusahaan secara tidak sengaja adalah: dampak terhadap reputasi, finansial dan denda bernilai sedang untuk semua hasil ancaman, sedangkan dampak terhadap produktifitas dan perlindungan bernilai rendah untuk semua hasil ancaman. Dampak ancaman melalui akses fisik yang dilakukan oleh eksternal perusahaan secara sengaja adalah: dampak terhadap reputasi, finansial, dan produktifitas bernilai sedang untuk semua hasil ancaman sedangkan dampak terhadap denda dan perlindungan bernilai rendah untuk semua hasil ancaman.

Kesimpulan

Dari hasil analisis yang dilakukan, maka ada beberapa hal yang dapat disimpulkan, yaitu: secara garis besar manajemen risiko pada PT. XYZ sudah berjalan dengan baik, hanya terdapat beberapa kelemahan yang harus diperbaiki untuk menunjang kinerja perusahaan agar lebih maksimal dan efektif; dalam hal keamanan informasi, PT. XYZ masih memiliki sedikit kekurangan, khususnya risiko-risiko yangmelalui akses jaringan karena pengamanan perusahaan melalui jaringan masih kurang terorganisir dengan baik; praktek keamanan dalam perusahaan telah diterapkan dengan cukup baik karena hanya terdapat beberapa kekurangan dari 15 praktek keamanan yang dievaluasi; serta diperlukan pelatihan karyawan secara menyeluruh pada setiap bagian/ divisi dalam setiap periodik.

DAFTAR PUSTAKA

Alberts, C, et al. (2005). *Introduction to OCTAVE-S*. U.S. Patent & Trademark Office. United State: Carnegie Mellon University.

Bandyopadhyay, K. et al. (1999). *Management Decision*, Vol.37, hlm. 437. London.

Djojosoedarso, S. (2005). *Prinsip-prinsip Manajemen Risiko Asuransi*, Edisi revisi. Jakarta: Salemba Empat. 38 *CommIT, Vol. 2 No. 1 Mei 2008, hlm. 33 - 38*

Febrian, Jack. (2000). *Kamus Komputer dan Istilah TI*.

Gondodiyoto, S., dan Hendarti, H. (2006). *Audit Sistem Informasi*. Jakarta: Mitra Wacana Media.

Haag, Cummings, dan Cuberry, C. (2005). *Management Information Systems for the Information Age*, Edisi kelima. New York: McGraw-Hill.

Hughes, G. (2006). *Five Steps to IT Risk Management Best Practices*. Risk Management, Vol. 53, hlm. 7, 34.

Jordan, E., dan Silcock, L. (2005). *Beating IT Risks*. England:John Wiley and Sons, Inc.

McLeod, R., dan Schell, G. P. (2007). *Management Information Systems,* Edisi kesepuluh. New Jersey: Pearson Prentice Hall.

Peltier, Thomas R. (2001). *Information Security Risk Analysis*. Washington D.C: Auerbach/CRC Press Release.

Turban, Efraim. et.al. (2003). *Introduction to Information Technology*, 2th edition. England: John Wiley and Sons, Inc.

Judul Tugas	Proses Asesmen Resiko
Judul Paper	Asesmen Resiko Bencana Menggunakan Metode Kualitatif Pada Desa Imogiri
Penulis	Imam Trianggoro Saputro
MK	ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEM
Reviewer	M. Riski Qisthiano (182420040)
Tanggal	14 Januari 2020

Abstrak	Bencana alam merupakan suatu ancaman yang dapat menimpa suatu kawasan dimanapun berada. Ini tentunya harus menjadi perhatian yang penting dalam rangka upaya pengurangan resiko bencana. Desa Imogiri merupakan salah satu desa yang berlokasi di Yogyakarta, tepatnya kabupaten Bantul. Seperti yang diketahui, daerah Yogyakarta sering terjadi bencana seperti kekeringan, gempa bumi, letusan gunung berapi, dan lainnya. Pada penelitian ini mengasesmen resiko bencana tersebut. Metode yang digunakan adalah asesmen resiko bencana menggunakan metode kualitatif (Qualitative Risk Hazard Assessment). Parameter dan indikator penilaian yang digunakan mengacu pada British Columbia Provincial Emergency Program. Hasil dari penelitian menunjukkan bahwa resiko yang paling dominan pada daerah ini adalah bencana gempa bumi kemudian disusul oleh letusan/erupsi gunung berapi.
Pendahuluan	Desa Imogiri merupakan salah satu daerah di Bantul yang terkena dampak terhadap gempa Yogyakarta yang terjadi pada tanggal 27 mei 2006. Dan mengalami cukup banyak korban jiwa dan juga kerusakan struktur dan infrastruktur. Selain itu, gunung Merapi yang sering meletus merupakan suatu ancaman tersendiri bagi masyarakat Yogyakarta. Material vulkanik yang terbawa oleh angin dapat mengganggu kesehatan masyarakat dan juga perekonomian sekitar. Bencana lain pun terkadang terjadi seperti kekeringan maupun banjir. Hal ini tentunya diperlukan suatu asesmen dalam rangka mengidentifikasi bencana mana yang memiliki resiko paling tinggi. Standar acuan yang dipakai pada penelitian ini adalah mengacu pada British Columbia Provincial Emergency Program. Terdapat beberapa aspek yang diperhitungkan dalam acuan ini diantaranya adalah kematian (fatality), terluka (injured), fasilitas vital (critical facilities), fasilitas umum pendukung (life-lines), kerusakan harta milik (property damage), lingkungan (environment), dampak

	ekonomi dan sosial (economics and sosial impacts). Berdasarkan datadata tersebut maka dapat disajikan data dalam bentuk matrikulasi resiko/Risk Matrix.
Pembahasan	Penelitian dilakukan pada daerah Desa Imogiri, Kecamatan Imogiri, Bantul, Yogyakarta. Desa ini memiliki luas sekitar 54,49 km². Survei lokasi dilakukan untuk mengetahui kondisi tempat penelitian secara langsung. Selain itu, terdapat beberapa data sekunder yang diperlukan sebagai bahan pertimbangan dalam melakukan proses analisis. Data sekunder yang diperlukan seperti data penduduk daerah imogiri
Kesimpulan	Dari hasil asesmen resiko (risk assessment) dengan menggunakan metode qualitative risk hazard assessment diperoleh hasil bahwa pada desa Imogiri, bencana/hazard yang paling dominan atau terparah itu adalah gempa bumi. Salah satu penyebabnya karena dekat dengan sumber gempa sesar Opak. Gempa bumi pada tahun 2006 banyak menimbulkan korban jiwa dan juga kerusakan terhadap rumah warga maupun fasilitas pemerintahan. Dari pengambilan data diperoleh fakta bahwa korban banyak terjadi pada anak-anak dan juga orang lanjut usia.
Daftar Pustaka	• Columbia, British (2004). Hazard, Risk, and Vurnerability Analysis Tool Kit. Provincial Emergency Program. • Saputro, I. T. (2018). Analisis Perbandingan Kurva Hazard Pada Kota Banda Aceh Dengan Sumber Gempa Sesar Seulimeum Dan Menggunakan Beberapa Fungsi Atenuasi. • Widodo (2013). Natural Hazard Risk Assessment. Bahan Kuliah. Universitas Islam Indonesia. Yogyakarta

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **DITA RAHMAWATI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa orang untuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci: *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada website Hyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

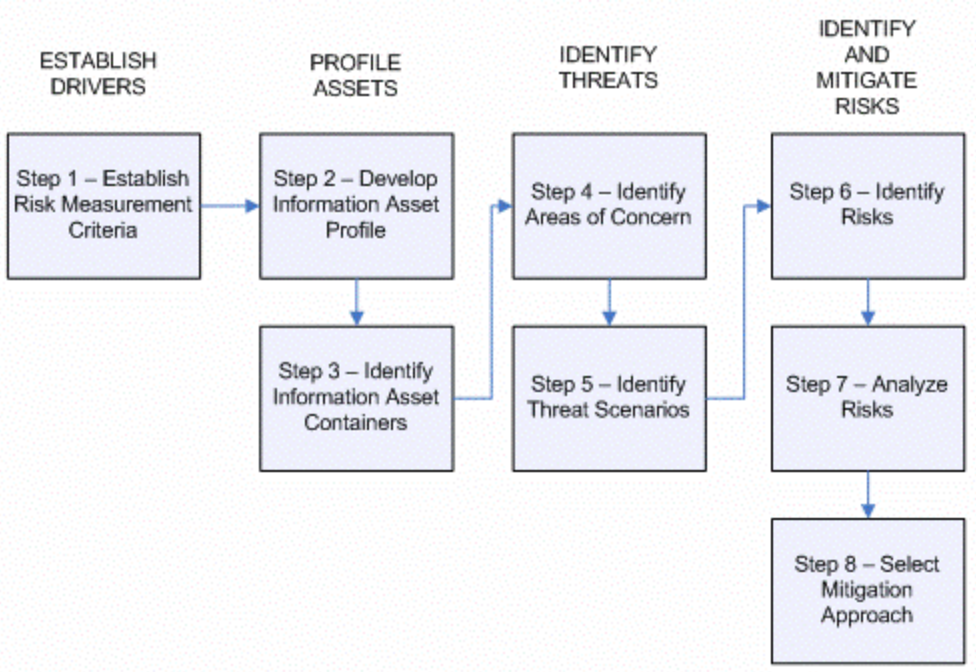
Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi. (Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang mengkontak calon pelamar perusahaan tersebut dan data harus diamankan	

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi

dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	**Area of Concern**
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**
Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	***Risk***			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1), 43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8 November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

Oleh:

Kelompok I:

1. **Muhammad Irvai (182420063)**
2. **M. Apriliansyah**
3. **Pamuji Muhammad Jakak**
4. **Anshori**

Dosen Pengampu: M. Izman Herdiansyah, M.M., Ph.D.

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat pada saat ini mendorong Universitas Bina Insan Lubuklinggau untuk menerapkan sistem *e-learning* sebagai sistem pembelajaran berbasis elektronik yang mempermudah proses transformasi atau pertukaran informasi antara pihak Universitas Bina Insan dengan mahasiswa. Namun dalam pemanfaatan aplikasi *e-learning* itu sendiri, terkadang pihak Universitas kesulitan dalam mengidentifikasikan kemungkinan resiko-resiko yang terjadi. Adapun tujuan dari penelitian ini adalah melakukan suatu analisis resiko yang berkaitan dengan penerapan aplikasi *e-learning* di Universitas Bina Insan Lubuklinggau dengan menggunakan metode *OCTAVE Allegro.* Metode ini terdiri dari 8 tahap yang diklasifikasikan menjadi 4 kategori untuk mendapatkan tindakan pencegahan atau pengendalian pada Universitas Bina Insan. Hasil dari penelitian ini berupa pertimbangan strategi bagi Universitas Bina Insan mengenai penyimpanan aset informasi yang kritis dan pengembangan terhadap fitur aplikasi *e-learning* secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat dan pemanfaatan aplikasi *e-learning* menjadi lebih efektif.

Kata kunci: analisis resiko, manajemen resiko, *OCTAVE Allegro*, *e-learning.*

1. PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan sistem dan teknologi informasi saat ini, banyak organisasi yang memanfaatkan kemajuan tersebut untuk mendorong proses bisnisnya. Organisasi menyusun dan merencanakan strategi bisnis maupun teknologi informasi untuk menghasilkan kinerja yang lebih baik. Dengan adanya pemanfaatan teknologi informasi, informasi yang dihasilkan dapat digunakan lebih lanjut untuk proses pengambilan keputusan yang cepat dan tepat. Selain itu, teknologi informasi ini juga membantu organisasi dalam pengelolaan data-data secara akurat dan *real-time*. Banyak organisasi yang menerapkan teknologi informasi yang *up-to-date* dan terbaru, termasuk

perguruan tinggi. Salah satu perkembangan teknologi informasi yang sering digunakan dalam suatu perguruan tinggi adalah penerapan *e-learning* sebagai sistem pembelajaran berbasis elektronik. Pembelajaran seperti ini lebih praktis dilakukan karena *e-learning* dapat memberikan keuntungan bagi suatu perguruan tinggi dalam memperlancar pengaksesan informasi kepada mahasiswa. Hal ini juga bermanfaat untuk mempermudah proses transformasi atau pertukaran informasi antara kedua pihak.

Aktivitas-aktivitas akademik yang berkaitan dengan sistem *e-learning* dapat memberikan kemudahan pengaksesan materi perkuliahan bagi mahasiswa. Selain itu, mahasiswa dapat melakukan *download* dan *upload* tugas, melakukan *post* terhadap forum diskusi, dan mengakses kuis. *E-learning* Universitas Bina Insan dapat membantu pihak Universitas dalam memberikan informasi berupa pengumuman-pengumuman yang berkaitan dengan proses perkuliahan yang berlangsung. Selain itu, mahasiswa Universitas Bina Insan dapat mendalami penggunaan *e-learning* terkait dengan perkuliahannya. Mahasiswa dapat berfokus pada penguasaan materi perkuliahan yang diberikan oleh dosen secara langsung. Sistem pembelajaran ini dapat memfokuskan mahasiswa pada pengerjaan tugas-tugas secara mandiri dan dapat memberikan pengetahuan tambahan terkait dengan penerapan teknologi informasi yang berkaitan dengan pendidikan.

E-learning ini juga memberikan dampak positif terhadap dosen yang memberikan pengajaran dalam perkuliahan yang berlangsung sesuai dengan penetapan jadwal perkuliahan. Setiap dosen dapat mengetahui seberapa jauh pemahaman mahasiswa terhadap perkuliahan yang diberikan di Universitas Bina Insan Lubuklinggau. Dosen juga dapat menerima *feedback* dari mahasiswa secara langsung dan dosen dapat memberikan tanggapan kepada mahasiswa tanpa terhalang oleh batasan lokasi dan waktu. Selain dampak **positif** yang dihasilkan dari penerapan *e-learning* di Universitas Bina Insan, maka selalu terdapat risiko yang nantinya dapat memberikan dampak **negatif**. Adapun kemungkinan **risiko-risiko** yang dapat terjadi selama proses perkuliahan berlangsung dalam *e-learning*, seperti terjadinya *down server*

karena banyak mahasiswa yang melakukan pengaksesan *e-learning* secara bersamaan dan terdapat keterbatasan sumber daya dalam penanganan dan pemeliharaan *e-learning*. Selain itu, *e-learning* juga terdapat keterbatasan kapasitas terhadap *file* yang bisa di-*upload* dan penyimpanan data mahasiswa dalam sistem *e-learning*. Ada kemungkinan terdapat keterbatasan fitur-fitur dalam *e-learning* yang memiliki tingkat kompleksitas yang berbeda-beda. Hal ini dapat menyebabkan dosen dan mahasiswa bisa kesulitan menggunakan *e-learning*.

Dengan adanya kemungkinan **risiko-risiko** yang muncul selama proses implementasi *e-learning*, maka diperlukan manajemen risiko di Universitas Bina Insan untuk mengelola dan meminimalkan risiko tersebut. Oleh karena itu, diperlukan adanya tindakan pengendalian maupun pengawasan sistem *e-learning* yang dilakukan secara teratur. Proses-proses pengelolaan terhadap kemungkinan risiko di Universitas dapat dilakukan metodologi manajemen risiko. Untuk mengidentifikasikan kemungkinan risiko-risiko secara akurat, maka digunakan metode ***OCTAVE Allegro***. Metode ini menjabarkan identifikasi terhadap penilaian risiko dan dapat memberikan tindakan mitigasi terhadap risiko tersebut. Hal ini dapat membantu Universitas Bina Insan untuk menghadapi permasalahan-permasalahan yang terjadi pada *e-learning*.

1.2 Rumusan Masalah

Adapun rumusan permasalahan yang dilakukan dalam penelitian ini adalah

1. pihak Universitas Bina Insan kesulitan mengidentifikasikan tentang kemungkinan risiko-risiko yang dapat terjadi selama implementasi *elearning* di Universitas dengan metode *OCTAVE Allegro*
2. Evaluasi tindakan pengelolaan risiko sebagai tindakan pencegahan atau pengendalian pada Universitas Bina Insan

1.3 Tujuan Penelitian

Tujuan dilakukan proses penelitian ini adalah untuk melakukan analisis terhadap proses pengelolaan risiko sebagai bentuk manajemen risiko dalam hal implementasi *e-learning* di Universitas Bina Insan Lubuklinggau.

2. Tinjauan Pustaka

2.1 Sistem *E-Learning*

Sistem *E-learning* merupakan pendekatan inovatif dalam hal pengiriman pembelajaran untuk bidang pendidikan yang lebih tinggi dan menyediakan alternatif bagi mahasiswa untuk belajar tanpa adanya keterbatasan waktu dan tempat (Al-Samarraie et al., 2017). *E-learning* yang diterapkan dalam perguruan tinggi merupakan salah satu strategi pembelajaran yang efektif dan efisien yang memanfaatkan sistem dan teknologi informasi sehingga dapat menggantikan pembelajaran *face-to-face*. Penggunaan *e-learning* dalam perguruan tinggi yang digunakan oleh dosen sebagai *workplace tool* memiliki potensi dalam hal transformasi pengajaran dan pengalaman pembelajaran (King & Boyatt, 2014).

2.2 Manajemen Resiko

Setiap penggunaan sistem dan teknologi informasi selalu terdapat risiko yang muncul sebagai bentuk ancaman dan ketidakpastian yang dapat memberikan dampak negatif dalam suatu perusahaan atau perguruan tinggi. Tingkat probabilitas atau peluang terjadinya risiko dalam suatu organisasi berbeda-beda tergantung dari faktor-faktor pemicu munculnya risiko tersebut, seperti pengetahuan para pakar dan data-data histori dari setiap aktivitas yang telah selesai dilakukan (Aqlan & Lam, 2015). Risiko dapat terjadi pada pengelolaan aset dalam suatu organisasi karena aset bisa mengalami kerusakan ataupun kesalahan penggunaan aset tersebut oleh pihak terkait (Tobing & Puspa, 2015). Selain itu, terdapat faktor-faktor internal dalam suatu perguruan tinggi yang dapat memunculkan berbagai risiko sehingga penggunaan *e-learning* yang memengaruhi hubungan antara dosen dengan mahasiswa. Tingkat pengetahuan dan pengalaman yang terdapat masing-masing dosen sebagai pihak pengajar dan penyampaian materi perkuliahan kepada mahasiswa bisa memunculkan kesalahpahaman penyampaian informasi kepada mahasiswa (Mackay & Tymon, 2014).

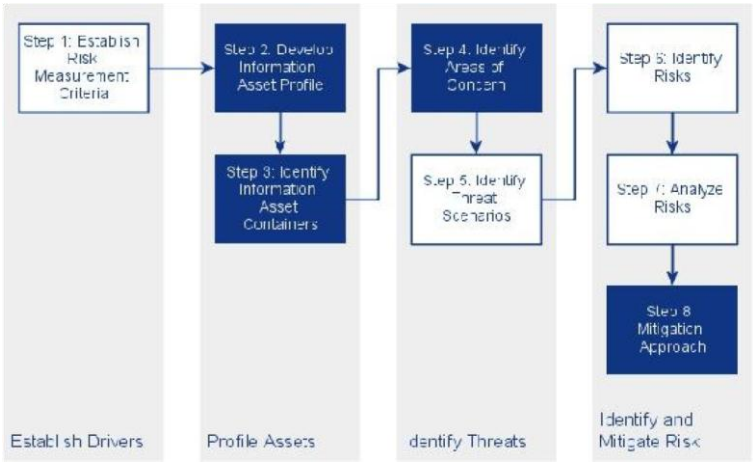
2.3 Metode OCTAVE Allegro

Metode OCTAVE merupakan singkatan dari *the Operationally Critical Threat, Asset, and Vulnerability Evaluation* adalah seperangkat alat, teknik, dan metode untuk menilai strategi keamanan informasi yang berbasis risiko dan perencanaan. Metode OCTAVE terdiri dari tiga prinsip dasar administrasi keamanan, yaitu: *confidentiality, integrity,* dan *availability* (Pandey & Mustafa, 2012). Metode penilaian OCTAVE Allegro yang dilakukan oleh *Carnegie Mellon University Software Engineering Institute (SEI)* yang memiliki kemampuan untuk memberikan hasil penilaian risiko yang kuat, dengan investasi yang relatif kecil dalam waktu dan sumber daya, bahkan untuk organisasi-organisasi yang tidak memiliki keahlian manajemen risiko yang luas (Keating, 2014). Metode OCTAVE Allegro dinilai sesuai untuk digunakan oleh individu yang ingin melakukan penilaian risiko secara komprehensif tanpa keterlibatan organisasi, ahli, atau sumber daya lainnya sehingga metode ini direkomendasikan untuk penilaian risiko *container* informasi (Maček, Magdalenić, & Ivković, 2011).

Metode *OCTAVE Allegro* terdiri dari delapan tahap yang diklasifikasikan menjadi empat kategori yaitu sebagai berikut (Caralli et al., 2007).

a. Menetapkan apa yang menjadi arahan organisasi dan mengembangkan kriteria pengukuran risiko didalamnya
b. Membuat profil aset yang dimiliki organisasi dengan mengidentifikasi persyaratan keamanan, dan mengidentifikasi semua lokasi dimana aset tersebut disimpan, diangkut, atau diproses
c. Mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadah aset tersebut
d. Mengidentifikasi, analisis dan mitigasi risiko terhadap aset informasi dan pengembangan terhadap pendekatan mitigasi

Berikut ini adalah gambar kategori-kategori dalam metode *OCTAVE Allegro* (Caralli et al., 2007).



Gambar 1. Pendekatan Metode *OCTAVE Allegro*

Terdapat delapan langkah-langkah yang terdapat dalam mdetode OCTAVE Allegro (Caralli et al., 2007).

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini terdapat *organizational driver* yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling prioritas. Kriteria pengukuran risiko didokumentasikan dalam bentuk *Risk Measurement Criteria Worksheets* dan pemberian nilai prioritas *impact area* dalam bentuk *Impact Area Ranking Worksheet.*

Langkah 2 – Mengembangkan Profil Aset Informasi

Langkah ini dilakukan dengan identifikasi aset informasi dimana profil tersebut merupakan representasi aset yang menggambarkan fitur, kualitas, karakteristik, dan nilai yang unik. Langkah ini berguna untuk memastikan bahwa deskripsi aset sudah jelas dan konsisten sehingga dapat mempermudah penyusunan kebutuhan keamanan yang paling penting untuk aset informasi.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Langkah ini mengacu pada identifikasi faktor internal dan eksternal yang penting dilakukan terhadap kontainer sebagai tempat penyimpanan, pengiriman, dan pemrosesan aset informasi.

Langkah 4 – Mengidentifikasi Area Masalah yang Diperhatikan

Langkah ini dilakukan dengan proses pengembangan profil risiko dari aset informasi melalui pertukaran pikiran. Pertukaran pikiran/ *brainstorming* mengenai kondisi atau situasi tertentu untuk mengetahui komponen ancaman yang akan dihadapi. Dengan berpedoman pada dokumen *information asset risk environment maps* dan *information asset risk worksheet* maka dilakukan pencatatan *area of concern.* Setelah itu, dilakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Langkah ini dilakukan dengan identifikasi skenario ancaman tambahan yang lebih jauh dari area-area pada langkah sebelumnya berfokus pada properti ancaman. Aktivitas ini dapat menggunakan *Threat Scenario Questionnaries* dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Langkah ini digunakan untuk menentukan *threat scenario* terhadap gambaran risiko secara terperinci. *Threat scenario* didokumentasikan dalam bentuk *information asset risk worksheet* yang dapat memberikan dampak bagi organisasi.

Langkah 7 – Menganalisis Risiko

Langkah ini mengacu pada dokumentasi yang terdapat pada *information asset risk worksheet.* Setelah itu, dilakukan review dan menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis seberapa jauh dampak risiko tersebut dan memutuskan strategi terbaik dalam menghadapi risiko.

Langkah 8 – Memilih Pendekatan Pengurangan

Langkah ini dilakukan dengan mengurutkan setiap risiko yang diidentifikasi berdasarkan nilai risikonya sehingga dapat ditentukan pendekatan mitigasi terhadap risiko tersebut. Hal ini dilakukan dengan memprioritaskan risiko-risiko diikuti dengan pendekatan pengembangan strategi penanganan risiko. Strategi tersebut juga harus mempertimbangkan nilai aset dan kebutuhan keamanan, container aset, serta lingkungan operasional yang unik dalam organisasi.

3. Pembahasan

Adapun pelaksanaan penilaian risiko terhadap implementasi *e-learning* yang dilakukan di Universitas Bina Insan berdasarkan 8 fase atau langkah utama dalam metode OCTAVE Allegro adalah sebagai berikut:

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini, dibangun *organizational drivers* untuk penentuan *impact area* yang paling penting serta memberikan nilai skala prioritas pada *impact area* yang telah ditentukan. Terdapat 5 area dampak dalam OCTAVE Allegro yang menentukan nilai kualitatif dengan ukuran rendah, sedang, dan tinggi. Prioritas *impact area* yang dipilih adalah reputasi dan kepercayaan pelanggan, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan penalti.

Berikut ini adalah tabel *impact area* yang berfokus pada reputasi dan kepercayaan mahasiswa.

Tabel 1. Allegro *Worksheet* 1

Impact Area	*Low*	*Medium*	*High*
Reputasi	Reputasi Universitas Bina Insan tidak terpengaruh dari perubahan *e-learning*	Reputasi Universitas Bina Insan terpengaruh sedikit dari perubahan *e-learning*	Reputasi Universitas Bina Insan terpengaruh banyak dari perubahan *e-learning*
Kepercayaan Mahasiswa	Kurang dari 2% kehilangan kepercayaan	2% -10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*	Lebih dari 10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*

	mahasiswa terhadap fitur *e-learning*		

Berikut ini adalah tabel *impact area* yang berfokus pada keuangan.

Tabel 2. Allegro *Worksheet* 2

Impact Area	*Low*	*Medium*	*High*
Biaya Operasional	Peningkatan biaya operasional saat implementasi *e-learning* kurang dari 2,5%	Peningkatan biaya operasional saat implementasi *e-learning* sebesar 2,5% - 5%	Peningkatan biaya operasional saat implementasi *e-learning* lebih dari 5%
Kerugian	Kurang dari 10jt kerugian tahunan jika *e-learning* ada gangguan	Antara 10jt – 50jt kerugian tahunan jika *e-learning* ada gangguan	Lebih dari 50jt kerugian tahunan jika *e-learning* ada gangguan

Dari tabel-tabel di atas, diuraikan beberapa contoh *allegro worksheet* dari semua area dampak yang berfokus di area reputasi dan kepercayaan mahasiswa dan keuangan. Dari masing-masing area dampak yang diidentifikasikan, maka ditentukan estimasi tingkat prioritas risiko apakah *low*, *medium*, dan *high* dan tingkat kerusakan yang mungkin terjadi saat implementasi *e-learning* Universitas Bina Insan. Berikut ini adalah tabel skala prioritas *impact area*.

Tabel 3. Skala Prioritas *Impact Area*

Priority	*Impact Area*
1	Reputasi & Kepercayaan Mahasiswa
2	Keuangan
3	Produktivitas
4	Keamanan & Kesehatan
5	Denda & Penalti

Dari tabel-tabel identifikasi masing-masing area dampak risiko tersebut, maka didapatkan urutan prioritas area dampak, yaitu bagian reputasi dan kepercayaan mahasiswa sebagai prioritas pertama, bagian keuangan sebagai prioritas kedua, bagian produktivitas sebagai prioritas ketiga, bagian denda dan penalti sebagai prioritas keempat, dan bagian keamanan dan kesehatan sebagai prioritas kelima.

Langkah 2 – Mengembangkan Profil Aset Informasi

Profil aset informasi kritis (*Critical information assets profile*) terdiri dari deskripsi aset informasi kritis, alasan pemilihan, dan pemilik (pengelola). Profil aset informasi kritis dilengkapi dengan persyaratan (*requirements*) keamanan yang harus ada untuk melindungi aset tersebut dengan menyatakan kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan persyaratan keamanan lainnya. Berikut ini adalah tabel *critical information asset*.

Tabel 4. *Critical Information Asset Profile*

Allegro Worksheet	*Critical Information Asset*	
(1) Critical Asset	***(2) Rationale for Selection***	***(3) Description***
Peningkatan proses pembelajaran mahasiswa yang yang semakin bermutu	Penerapan *e-learning* sangat penting dilakukan untuk meningkatkan kinerja mahasiswa dan mempermudah pengaksesan materi perkuliahan, mengerjakan tugas dan kuis secara efektif dan efisien, serta dapat meningkatkan hubungan yang baik antara dosen dengan mahasiswa. Hal ini berpengaruh terhadap nilai mahasiswa.	Informasi ini terdiri dari fiturfitur *e-learning*, program studi, materi dan jadwal kuliah, jumlah kelas, deskripsi tugas dan kuis, jumlah akses fitur *elearning* oleh mahasiswa dan dosen.
(4) Owner		
Bagian Pusat Pembelajaran Elektronik		
(5) Security Requirements		
Confidentiality	Informasi selama proses perkuliahan berlangsung sangat penting untuk didistribusikan bagi mahasiswa, dosen, dan program studi. Bagian program studi menggunakan informasi ini untuk mengolah nilai mahasiswa dan melakukan evaluasi terhadap minat belajar mahasiswa melalui sistem *e-learning*.	

Integrity	Informasi selama proses perkuliahan harus benar dan *up-to-date* sesuai dengan perkembangan zaman serta mahasiswa selalu mendapatkan informasi tersebut jika terdapat perubahan antara dosen dengan mahasiswa. Bagian program studi melakukan distribusi informasi tersebut kepada dosen yang nantinya akan didistribusikan ke mahasiswa secara komprehensif.	
Availability	Informasi selama proses perkuliahan harus tersedia dengan lengkap dan jelas bagi program studi, mahasiswa, dan dosen termasuk instruksi yang diberikan, deskripsi tugas dan kuis, dan proses pengerjaan pelatihan dalam *e-learning*.	
(6) Most Important Secu rity Requirement		
Confidentiality	*Integrity*	√ ***Availability***

Dari tabel tersebut, terdapat identifikasi profil aset informasi yang kritis berupa peningkatan proses pembelajaran mahasiswa yang semakin bermutu di Universitas Bina Insan sehingga dapat diketahui risiko yang dihadapi Universitas Bina Insan.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Identifikasi *information asset container* yang terbagi menjadi tiga yaitu *technical, physical,* dan *people* masing-masing memiliki sisi eksternal dan internal dengan menggunakan *worksheet information asset risk environment map.*

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi teknikal.

Tabel 5. ***Information Asset Risk Environment Map (Technical)***

Container Description	*Owner(s)*
Internal	
E-mail Server, Database Server, Internal Network	Divisi TI
Appliction Server	Divisi TI, Program Studi
Personal Computer	Dosen, Program Studi
External	
Internet, External Network.E-learning Web	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi fisik.

Tabel 6. *Information Asset Risk Environment Map (Physical)*

Container Description	*Owner(s)*
Internal	
Paper copies dari banyaknya akses *e-learning* secara rutin oleh mahasiswa	Program Studi, Bagian Pembelajaran Elektronik
External	
Paper copies dari kehadiran setiap mahasiswa	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi sumber daya manusia.

Tabel 7. *Information Asset Risk Environment Map (People)*

Container Description	*Owner(s)*
Internal	
Dosen, Staf Program Studi	Program Studi
External	
Mahasiswa	Mahasiswa

Langkah 4 – Mengidentifikasi Area Masalah

Identifikasi *areas of concerns* dilakukan untuk meninjau kembali setiap *container* untuk mempertimbangkan dan menentukan *area of concern* yang potensial dilanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. *Areas of concern* diperluas untuk mendapatkan *threat scenarios* dan didokumentasikan untuk melihat apakah memengaruhi *security requirements.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Identifikasi *threat scenario* yang memberikan gambaran mengenai *property* dari *threat,* antara lain *actor, means, motives, outcome* dan *security requirement.* Selain itu, langkah ini dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Identifikasi risiko bertujuan untuk menentukan bagaimana *threat scenario* memberikan dampak bagi organisasi serta menentukan tingkatannya apakah masuk ke kategori *high, medium* atau *low.* Selain itu, dilakukan perhitungan *relative score* untuk membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko.

Berikut ini adalah tabel penentuan nilai prioritas berdasarkan *impact area*.

Tabel 8. *Impact – Priority Score*

Impact Area	*Priority*	*Impact Score*		
		Low (1)	*Medium (2)*	*High (3)*
Reputasi & Kepercayaan Mahasiswa	1	1	2	3
Keuangan	2	2	4	6
Produktivitas	3	3	6	9
Keamanan dan Kesehatan	5	5	10	15
Denda dan Penalti	4	4	8	12

Langkah 7 – Menganalisis Risiko

Analisis risiko dilakukan pada setiap *areas of concern* terhadap *information asset* serta identifikasi konsekuensi yang terjadi berdasarkan *relative risk score.* Nilai risiko relatif diperoleh dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area* dan estimasi kemungkinan terjadi risiko tersebut.

Berikut ini adalah tabel penilaian risiko relatif.

Tabel 9. *Relative Risk Score*

Area of Concern	*Risk*			
Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *elearning* secara bersamaan setiap harinya	Konsekuensi	Diperlukan waktu pemrosesan *e-learning* untuk melakukan *back-up* terlebih dahulu dan perubahan terhadap prosedur perkuliahan		
	Severity	Area Terdampak	Nilai	Skor
		Keuangan	Medium	4
		Reputasi dan Kepercayaan Mahasiswa	High	3
		Produktivitas	High	9
		Denda dan Penalti	Low	4
		Keselamatan dan Kesehatan	Low	5
	Nilai Risiko Relatif			25

Langkah 8 – Memilih Pendekatan Pengurangan

Berdasarkan pengelompokkan risiko yang diidentifikasikan, maka dilakukan pemilihan pendekatan mitigasi. Hal ini dilakukan dengan cara memprioritaskan risiko – risiko berdasarkan nilai risiko relatif, kemudian mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset dan kebutuhan keamanan, kontainer atas aset, serta lingkungan operasional yang unik dari organisasi. Berikut ini adalah tabel matriks penentuan nilai risiko.

Tabel 10. *Relative Risk Matrix*

Risk Score		
30 to 45	16 to 29	0 to 15
POOL 1	POOL 2	POOL 3

Berikut ini adalah tabel pendekatan yang menentukan tindakan dalam penanganan risiko.

Tabel 11. *Mitigation Approach*

POOL	*Mitigation Approach*
POOL 1	*Mitigate*
POOL 2	*Mitigate or Defer*
POOL 3	*Accept*

Dari nilai risiko relatif yang didapatkan sebesar 25, maka nilai risiko tersebut dapat dikategorikan ke dalam POOL 2 yang memiliki pendekatan *mitigate* atau *defer*.

Berikut ini adalah tabel strategi pengendalian risiko terhadap risiko-risiko yang dihadapi Universitas Bina Insan

Tabel 12. *Risk Mitigation*

Risk Mitigation	
Area of Concern	Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *e-learning* secara bersamaan setiap harinya
Action	Mitigasi
Container	Kontroli
Server	Melakukan filter tehadap informasi yang dihasilkan dari setiap fitur *e-learning*
Internet	Memastikan bahwa jaringan internet telah stabil untuk akses *e-learning*
Dosen	Memastikan bahwa semua instruksi sudah diditribusikan secara menyeluruh
Program Studi	Melakukan *back-up* terhadap materi perkuliahan/ informasi terbaru dari *e-learning*
Bagian Pembelajaran Elektronik	Memastikan bahwa akses fitur *e-learning* dapat dilakukan dosen dan mahasiswa sesuai dengan prosedur perkuliahan dan melakukan *report* terkait dengan akses *e-learning* dan perubahan fitur-fitur *e-learning*

4. Kesimpulan

Analisis manajemen risiko yang dapat mengidentifikasikan *area of concern* yang berdampak pada Universitas Bina Insan. Penilaian risiko dari masing-masing *area of concern* tersebut dapat dilakukan dengan metode OCTAVE Allegro. Selain itu, Universitas Bina Insan dapat melakukan penilaian risiko berdasarkan tingkat prioritas dan besarnya dampak *e-learning* terhadap proses pembelajaran mahasiswa. Setelah mengidentifikasi adanya risiko yang akan berpengaruh terhadap keberlangsungan implementasi *e-learning*, maka Universitas Bina Insan melakukan identifikasi pendekatan strategi atau mitigasi yang berfokus dari aspek lingkungan internal dan eksternal organisasi.

Berdasarkan hasil analisis manajemen risiko yang dilakukan, maka terdapat area perhatian mengenai perubahan fitur-fitur *e-learning* untuk akses material kuliah, tugas, dan kuis serta mengetahui hasil terhadap banyaknya akses *e-learning* yang dilakukan oleh mahasiswa dan dosen. Dari area perhatian tersebut, maka didapatkan konsekuensi berupa waktu pemrosesan *e-learning* untuk melakukan *back-up* dan memantau perubahan prosedur perkuliahan dengan mempertimbangkan kelima area dampak yang sudah diidentifikasi nilai prioritas risikonya. Dari hasil penelitian ini, Universitas Bina Insan juga harus mempertimbangkan strategi mana yang diutamakan untuk penyimpanan aset informasi yang kritis dan fitur-fitur *e-learning* yang perlu dikembangkan secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat. Untuk penelitian berikutnya, diharapkan dapat melakukan identifikasi risiko yang mendalam dan menyeluruh. Tidak hanya melihat sisi dari penggunaan fitur-fitur *e-learning*, tetapi juga mempertimbangkan pengembangan sistem *e-learning* dengan memperhatikan lingkungan eksternal perkuliahan dalam Universitas Bina Insan.

5. Daftar Pustaka

Al-Samarraie, H., Teng, B. K., Alzahrani, A. I., & Alalwan, N. 2017. E-learning continuance satisfaction in higher education: a unified perspective from instructors and students. *Studies in Higher Education*, 1–17.

Aqlan, F., & Lam, S. S. 2015. Supply chain risk modelling and mitigation. *International Journal of Production Research*, 1–17.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

Dewi, N. A. N., & Yudana, I. G. P. H. 2016. Analisa Manajemen Risiko Pada Sistem Akademik Di STMIK STIKOM Bali. In *Seminar Nasional Teknologi Informasi dan Multimedia*, 7–12.

Ekelhart, A., Fenz, S., & Neubauer, T. 2009. AURUM: A framework for information security risk management. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*: 1–10. https://doi.org/10.1109/HICSS.2009.82

Jakaria, D. A., Dirgahayu, R. T., & Hendrik. 2013. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. In *Seminar Nasional Aplikasi Teknologi Informasi. (SNATI)* (pp. 37–42).

Keating, C. G. 2014. *Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study*. *NSUWorks*. Nova Southeastern University.

King, E., & Boyatt, R. 2014. Exploring factors that influence adoption of e-learning within higher education. *British Journal of Educational Technology*, 1–9.

Matondang, N., Isnainiyah, I. N., & Muliawati, A. 2018. Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Rekayasa Sistem Dan Teknologi Informasi*, *2*(1), 282–287.

Tobing, J. J. L., & Puspa, A. K. 2015. Analisis Manajemen Resiko Untuk Evaluasi Aset Menggunakan Metode Octave Allegro. *Jurnal Manajemen Sistem Informasi Dan Teknologi*, *5*(1), 28–30.

MANAJEMEN RISIKO WEBSITE PENCARIAN INFORMASI PEKERJAAN HYPERLOKAL.ID

KELOMPOK III:

1. **DITA RAHMAWATI**
2. **ILSA PALINGGA NINDITAMA**
3. **MUHAMMAD DIAH MAULIDIN**
4. **NURHACHITA**
5. **RAHMA FITRIYANI**

KELAS : **REGULER A R1**
MATA KULIAH : **ETHICAL ISSUES IN ELECTRONIC INFORMATION SYSTEMS**

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA S2

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ABSTRAK

Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Sifat teknologi web yang mudah diakses dan digunakan menjadi alasan utama beberapa orang untuk mendapatkan informasi lowongan pekerjaan. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data. Dengan manajemen risiko teknologi informasi diharapkan dapat mengurangi dampak kerusakan yang bisa berupa dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Pada saat ini banyak yang memanfaatkan teknologi web sebagai sarana untuk mencari pekerjaan sesuai bidang yang dimiliki. Salah satu website yang menyediakan informasi lowongan pekerjaan yaitu bernama Lokal (www.hyperlokal.id). Untuk melindungi website serta menjaga keberlangsungan proses bisnis, maka paper ini akan menggunakan metode OCTAVE Allegro.

Kata kunci: *risk assessment*, website, manajemen risiko, OCTAVE Allegro

PENDAHULUAN

Manajemen risiko memegang peranan penting dalam pengambilan keputusan terhadap berbagai risiko yang sedang terjadi. Diantaranya ialah mengatur risiko teknologi informasi, membantu perkembangan proses bisnis yang akan memberikan keuntungan, serta sebagai manajemen sumber daya yang efektif. Keamanan sistem dibuat sebagai upaya untuk mengamankan kinerja, fungsi atau proses dan sedini mungkin mendeteksi adanya penyusup yang mencoba untuk melakukan pencurian data ataupun memanipulasi data. Inti masalah dari keamanan sistem umumnya disebabkan karena sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data.

Informasi sekarang ini sudah menjadi sebuah kondisi yang sangat penting, dengan seiring berkembangnya teknologi informasi (TI) dikalangan masyarakat luas, berkembang juga sistem infromasi (SI) yang dapat memudahkan masyarakat untuk mengakses dan mencari informasi dari media webserver. Segala bentuk organisasi pemerintah atau swasta baik yang menghasilkan profit maupun non-profit pasti akan menghadapi masalah internal dan eksternal dalam sistem yang mereka jalankan. Informasi merupakan aset yang sangat penting dan dijaga kerahasiaannya baik bagi sebuah organisasi seperti perusahaan, perguruan tinggi, lembaga pemerintahan maupun individual. Namun, kadang kala kemudahan akses informasi berbanding terbalik dengan tingkat keamanan website itu sendiri.

Di satu sisi website telah menjadi bagian yang sulit dipisahkan pada hampir setiap proses bisnis di perusahaan tersebut. Dengan demikian jika terdapat gangguan pada website maka dapat mengganggu keberlangsungan proses bisnis perusahaan yang bersangkutan. Teknologi web memberikan kemudahan untuk mengakses informasi dengan cepat. Saat ini belum banyak perusahaan yang melakukan *risk assessment* pada website yang digunakan. Website beserta asetnya rentan terhadap risiko kerusakan fisik dan logik. Risiko kerusakan fisik berkaitan dengan perangkat keras seperti bencana alam (natural disaster), pencurian (theft), kebakaran (fires), lonjakan listrik (power surge) dan perusakan (vandalism). Risiko kerusakan logik mengacu kepada akses tidak sah (unauthorized access), kerusakan secara sengaja maupun tidak disengaja pada website dan data (A. M. Suduc, M. Bîzoi dan F. G. Filip, 2010).

Untuk menjamin keamanan website yang sudah di buat, mengevaluasi adalah cara yang tepat untuk mengetahui sejauh mana keamanan website yang telah dibuat. Paper ini dibuat dalam rangka memperdalam pemahaman tentang keamanan website dan menerapkan metode OCTAVE Allegro pada website yang menyediakan informasi lowongan pekerjaan yaitu bernama Hyperlokal (www.hyperlokal.id) serta mengidentifikasi potensi gangguan dan permasalahan yang ada pada website Hyperlokal. Agar pembahasan pada penelitian ini tidak terlalu luas, maka akan dibatasi pembahasan penelitian yakni evaluasi terhadap analisis manajemen resiko keamanan informasi menggunakan metode OCTAVE Allegro yang dilakukan pada website Hyperlokal.id. Tujuan dari evaluasi ini adalah menjamin integritas informasi, pengamanan kerahasiaan data dan memastikan website tidak digunakan ataupun dimodifikasi oleh pihak yang tidak memiliki otoritas.

PEMBAHASAN

A. Sekilas tentang Hyperlokal.id

Hyperlokal.id merupakan perusahaan yang bergerak di bidang informasi lowongan pekerjaan yang berbasis di kota Palembang. Perusahaan tersebut memiliki portal yaitu website yang berisi tentang daftar lowongan pekerjaan dan informasi perusahaan yang membutuhkan karyawan. Hyperlokal.id dapat diakses melalui aplikasi toko digital yaitu Android Play Store.

B. Manajemen Risiko

Manajemen risiko secara umum merupakan proses dengan tujuan untuk mendapatkan keseimbangan antara efisiensi dan merealisasikan peluang untuk mendapatkan keuntungan dan meminimalkan kerentanan dan kerugian. Manajemen risiko harus menjadi proses tanpa henti dan berulang yang terdiri dari beberapa fase, ketika diterapkan dengan benar, memungkinkan terjadinya perbaikan terus-menerus dalam pengambilan keputusan dan peningkatan kinerja (Joint Task Force Transformation Initiative, 2011). Manajemen risiko merupakan proses yang memungkinkan manajer TI untuk menyeimbangkan biaya operasional dan biaya ekonomi untuk tindakan pengamanan dalam upaya melindungi sistem IT dan data yang mendukung misi organisasi. (G. Stoneburner, A. Goguen dan A. Feringa, 2002)

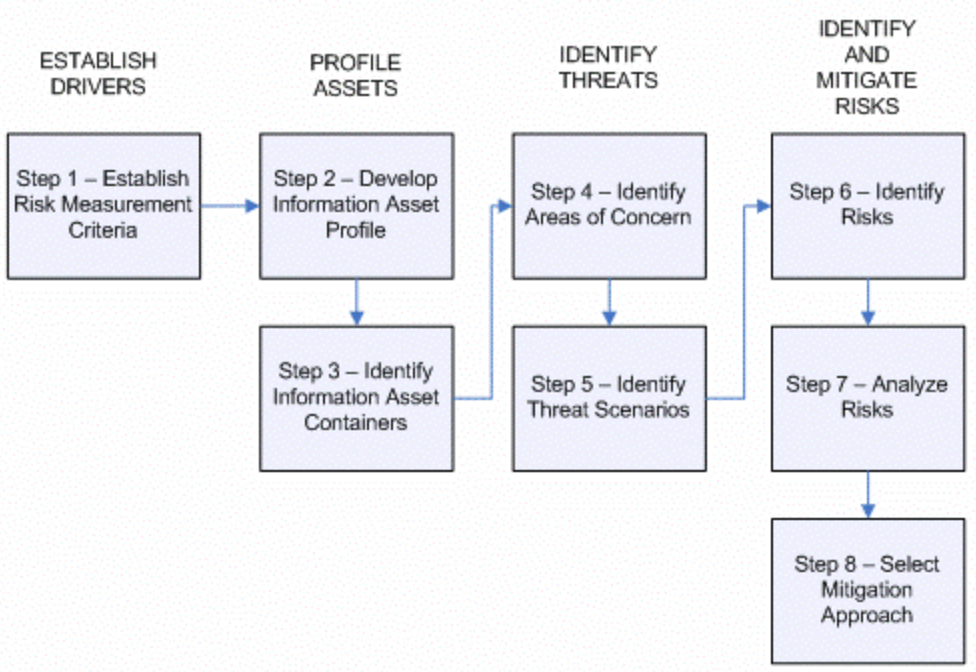
Suatu upaya dari perencanaan, pengorganisasian, memimpin dan mengendalikan sumber daya dan kegiatan untuk meminimalkan dampak dari kerugian akibat kecelakan pada biaya yang paling dapat diterima. Untuk memenuhi kebutuhan spesifik organisasi, keberhasilan manajemen risiko harus menyeimbangkan pengendalian risiko dan teknik risiko pembiayaan dengan mempertimbangkan visi, misi, nilai-nilai dan tujuan organisasi (G. Blokdijk, C. Engle, J. Brewster, 2008)

C. Metode OCTAVE

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) mendefinisikan komponen-komponen penting secara komprehensif, sistematis, berbasis konteks (context-driven) evaluasi risiko keamanan informasi. Dengan menggunakan metode OCTAVE, organisasi dapat membuat perlindungan terhadap informasi berbasis pengambilan keputusan risiko berdasarkan CIA (Confidentiality, Integrity, Authentication) untuk aset teknologi informasi kritis (S. K. Pandey dan K. Mustafa., 2012).

OCTAVE merupakan metodologi untuk mengidentifikasi dan mengevaluasi risiko keamanan sistem informasi. Penggunaan OCTAVE ditujukan untuk membantu organisasi dalam hal: (a) Mengembangkan kriteria evaluasi risiko kualitatif yang menggambarkan toleransi risiko operasional organisasi; (b) Mengidentifikasi aset – aset penting untuk mencapai misi organisasi; (c) Mengidentifikasi kerentanan dan ancaman terhadap aset tersebut; (d) Menentukan dan melakukan evaluasi untuk menghadapi konsekuensi yang terjadi pada organisasi jika ancaman tersebut terjadi. (Caralli et al., 2007)

Metoda OCTAVE memiliki tiga varian yaitu OCTAVE, OCTAVE-S dan OCTAVE Allegro. OCTAVE merupakan seperangkat peralatan, teknik dan metode untuk penilaian dan perencanaan keamananan sistem informasi berbasis risiko. OCTAVE Allegro merupakan metoda yang disederhanakan dengan fokus pada aset informasi. OCTAVE Allegro dapat dilakukan dengan metoda workshop-style dan kolaboratif. OCTAVE Allegro terdiri dari delapan langkah dibagi dalam empat fase.



Gambar 1. Langkah – langkah OCTAVE Allegro (Richard. A. Caralli., 2007).

D. Penilaian Risiko

Penilaian risiko (*risk assessment*) merupakan bagian dari manajemen risiko, penilaian risiko adalah proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko (M. M. Maulana dan S. H. Supangkat, 2006).

Manfaat melakukan analisis risiko antara lain menciptakan rasio cost-to-value yang jelas untuk perlindungan keamanan. Hal ini juga mempengaruhi proses pengambilan keputusan yang berhubungan dengan konfigurasi hardware dan desain sistem software (R. L. Krutz dan D. R. Vines, 2006).

Tujuan dari penilaian risiko adalah untuk melakukan identifikasi: (i) ancaman terhadap organisasi (contoh: operasional, aset atau individu) atau ancamana yang dialamatkan melalui organisasi kepada organisasi lain atau negara; (ii) kerentanan pada organisasi baik dari internal maupun eksternal; (iii) Bahaya terhadap organisasi yang mungkin terjadi yang diakibatkan oleh eksploitasi kerentanan; (iv) kemungkinan terjadinya bahaya atau kerusakan (Joint Task Force Transformation Initiative, 2011).

E. Tahapan Penilaian Risiko

1. Membangun Kriteria Pengukuran Risiko

Langkah ini terdapat dua aktivitas, diawali dengan membangun organizational drivers digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali impact area yang paling penting. Aktivitas 1 yaitu membuat definisi ukuran kualitatif yang didokumentasikan pada *Risk Measurement Criteria Worksheets*. Aktivitas dua melakukan pemberian nilai prioritas impact area *menggunakan Impact Area Ranking Worksheet*.

TABEL I. IMPACT AREA – REPUTASI DAN KEPERCAYAAN PELANGGAN

Impact Area	Low	Medium	High
Reputation	Reputasi sedikit terpengaruh; tidak ada usaha atau dibutuhkan usaha kecil untuk perbaikan	Reputasi terkena dampak buruk, dan dibutuhkan usaha dan biaya untuk perbaikan	Reputasi terkena dampak sangat buruk hingga hampir tidak dapat diperbaiki
Customer Loss	Kurang dari 2% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	2% hingga 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan	Lebih dari 10% pengurangan pelanggan yang diakibatkan hilangnya kepercayaan

TABEL II. SKALA PRIORITAS IMPACT AREA

Priority	Impact Areas
5	Reputasi dan kepercayaan pelanggan
4	Finansial
3	Produktivitas
1	Keamanan dan Kesehatan
2	Denda dan Penalti

2. Mengembangkan Profil Aset Informasi

Terdiri dari delapan aktivitas, diawali dengan identifikasi aset informasi selanjutnya dilakukan penilaian risiko terstruktur pada aset yang kritis. Aktivitas tiga dan empat mengumpulkan informasi mengenai information aset yang penting dilanjutkan dengan membuat dokumentasi alasan pemilihan aset informasi kritis. Aktivitas lima dan enam membuat deskripsi aset informasi kritis kemudian mengidentifikasi kepemilikan dari aset informasi kritis tersebut. Aktivitas tujuh mengisi kebutuhan keamanan untuk *confidentiality, integrity dan availaibility*. Aktivitas delapan mengidentifikasi kebutuhan keamanan yang paling penting untuk aset informasi.

Aset informasi yang dipilih harus mempertimbangkan hal – hal berikut:

- Aset informasi yang penting dan digunakan dalam kegiatan sehari – hari.
- Aset informasi yang jika hilang dapat mengganggu tujuan dan misi organisasi.

Dari hasil pertimbangan di atas maka informasi yang dikategorikan sebagai aset informasi penting diantaranya yaitu profil pengguna (user), profil perusahaan (company) dan profil pekerjaan (job). Tabel 3 berisi contoh *information asset profiling* untuk profil pengguna (user).

TABEL III. INFORMATION ASSET PROFILLING – PROFIL PENGGUNA

Critical Asset	Profil Pengguna	
Rationale for Selection	Digunakan untuk menentukan Nama pengguna hyperlokal.id	
Description	Terdiri dari nama, alamat email, nomor telepon	
Owner	Administrator, Pengguna	
Security Requirements	**Confidentiality**	Informasi profil pengguna sangat penting bagi perusahaan yang mencari calon pelamar yang ingin masuk ke dalam perusahaan.
	Integrity	Informasi harus benar dan akurat, hanya operator di bagian administrator dan pengguna yang dapat memasukan atau memodifikasi data tersebut
	Availability	Informasi harus selalu tersedia bagi perusahaan.
Most Important Security Requirement	**Integrity** **Alasan:** Nama profil pengguna sangat penting bagi perusahaan yang mengkontak calon pelamar perusahaan tersebut dan data harus diamankan	

3. Mengidentifikasi Kontainer dari Aset Informasi

Hanya ada satu aktivitas pada langkah tiga, perhatikan tiga poin penting terkait dengan keamanan dan konsep dari kontainer aset informasi yaitu cara aset informasi

dilindung, tingkat perlindungan atau pengaman aset informasi dan kerentanan serta ancaman terhadap kontainer dari aset informasi.

TABEL IV. INFORMATION ASSET RISK ENVIRONMENT (TECHNICAL) – PROFIL PENGGUNA

Data Profil Pengguna	
Information Asset Risk Environment Map (Technical)	
Internal	
Container Description	**Owner(s)**
Modul: Transaksi Input Data Profil Pengguna Input transaksi data profil pengguna untuk diproses oleh perusahaan pembuka lowongan kerja.	Adminstrator, User Perusahaan
External	**Owner(s)**
Container Description	Pengguna (User)
Aplikasi: Web Data Profil Pengguna	
Pengguna dapat melihat profil	

4. Mengidentifikasi Area Masalah

Aktivitas pada langkah empat yaitu diawali dengan pengembangan profil risiko dari aset informasi dengan cara bertukar pikiran untuk mencari komponen ancaman dari situasi yang mungkin mengancam aset informasi. Dengan berpedoman pada dokumen *Information Asset Risk Environment Maps* dan *Information Asset Risk Worksheet* maka dapat dicatat area of concern. Berpedoman pada dokumen *Information Asset Risk Worksheet* lakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern*.

TABEL V. AREA OF CONCERN – TRANSAKSI DATA PROFIL PENGGUNA

No	**Area of Concern**
1	Jumlah data profil pengguna yang banyak dapat menyebabkan kesalahan input data oleh user perusahaan
2	Penyebaran akses password transaksi data profil pengguna oleh user perusahaan yang memiliki akses
3	Celah keamanan pada aplikasi web data profil pengguna yang dapat dieksploitasi oleh pihak dalam/luar
4	Error yang terjadi pada saat proses insert/update/delete modul data profil pengguna dilakukan secara bersama-sama

5. Mengidentifikasi Skenario Ancaman

Aktivitas satu pada langkah lima yaitu melakukan identifikasi skenario ancaman tambahan pada aktivitas ini dapat menggunakan *Appendix C – Threat Scenarios Questionnaries*. Aktivitas dua melengkapi *Information Asset Risk Worksheets* untuk setiap threat scenario yang umum.

TABEL VI. PROPERTIES OF THREAT – TRANSAKSI DATA PROFIL PENGGUNA

1	**Area of Concern**	**Threat of Properties**
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan	**1. Actors**	User perusahaan
2. Means		User perusahaan menggunakan modul aplikasi data profil pengguna
3. Motives		*Human error (accidental)*
4. Outcome		*Modification, interruption*
5. Security Requirements		- Validasi input data nilai pada field - Administrator melakukan verifikasi data profil pengguna yang telah diinput oleh user perusahaan

6. Mengidentifikasi Risiko

Aktivitas satu pada langkah 6 menentukan threat scenario yang telah didokumentasikan di *Information Asset Risk Worksheet* dapat memberikan dampak bagi organisasi.

TABEL VII. MENGHITUNG SCORE IMPACT AREA

Impact areas	**Priority**	**Low (1)**	**Medium (2)**	**High (3)**
Reputasi dan kepercayaan pelanggan	**7**	**7**	**9**	**12**
Finansial	**4**	**4**	**8**	**14**
Produktivitas	**2**	**2**	**7**	**10**
Keamanan dan Kesehatan	**2**	**2**	**4**	**5**
Denda dan Penalti	**1**	**1**	**6**	**8**

7. Menganalisis Risiko

Aktivitas harus dilakukan mengacu pada dokumentasi yang terdapat pada *Information Asset Risk Worksheet*. Aktivitas satu dimulai dengan melakukan *review risk measurement criteria* dilanjutkan dengan aktivitas kedua menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis risiko dan memutuskan strategi terbaik dalam menghadapi risiko.

TABEL VIII. ANALISIS RESIKO – TRANSAKSI DATA PROFIL PENGGUNA

Area of concern	***Risk***			
Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data oleh user perusahaan	**Consequences**	Diperlukan waktu tambahan untuk memperbaiki kesalahan input data profil pengguna		
	Severity	**Impact Area**	**Value**	**Score**
		Reputasi dan kepercayaan pelanggan	Med	7
		Finansial	Low	5
		Produktivitas	High	8
		Keamanan dan Kesehatan	Low	2
		Denda dan Penalti	Low	3
		Relative Risk Score		25

8. Memilih Pendekatan Pengurangan

Aktivitas satu pada langkah delapan yaitu mengurutkan setiap risiko yang telah diidentifikasi berdasarkan nilai risikonya. Hal ini dilakukan untuk membantu dalam pengambilan keputusan status mitigasi risiko tersebut. Aktivitas dua melakukan pendekatan mitigasi untuk setiap risiko dengan berpedoman pada kondisi yang unik di organisasi tersebut.

TABEL IX. RELATIVE RISK MATRIX

RISK SCORE		
30 TO 45	**16 TO 29**	**0 TO 15**
POOL 1	POOL 2	POOL 3

TABEL X. MITIGATION APPROACH

Pool	**Mitigation Approach**
Pool 1	Mitigate
Pool 2	Mitigate or Defer
Pool 3	Accept

TABEL XI. CONTOH MITIGASI RISIKO BERDASARKAN AREA OF CONCERN

Risk Mitigation	
Area of Concern	Jumlah data profil pengguna yang banyak menyebabkan kesalahan input data profil pengguna oleh user perusahaan
Action	Mitigate
Container	Control
Modul data profil pengguna	Dibuat validasi input pada field tertentu
Administrator	Administrator dapat melakukan verifikasi nilai yang telah diinputkan oleh user perusahaan

KESIMPULAN

OCTAVE Allegro merupakan salah satu metode manajemen risiko sistem informasi yang dapat diterapkan pada perusahaan tanpa memerlukan keterlibatan yang ekstensif di dalam organisasi dan difokuskan pada aset informasi yang kritis bagi keberlangsungan organisasi dalam mencapai misi dan tujuannya. Penilaian risiko dapat memberikan gambaran mengenai kemungkinan adanya ancaman pada aset kritikal dan mengambil langkah – langkah pencegahan yang tepat untuk meminimalkan kemungkinan ancaman tersebut terjadi.

Dari hasil penilaian risiko maka pembuat kebijakan dapat membuat perencanaan strategis untuk menjaga aset informasi kritikal secara tepat serta langkah-langkah pemulihan jika skenario ancaman benar terjadi.

DAFTAR PUSTAKA

A. M. Suduc, M. Bîzoi dan F. G. Filip. 2010. Audit for Information Systems Security. *Journal Informatica Economică*, 14(1), 43-48.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

G. Blokdijk, C. Engle, J. Brewster. 2008. *IT Risk Management Guide: Risk Management Implementation Guide, Presentations, Blueprints, Templates*. AU: Emereo Pty Limited.

G. Stoneburner, A. Goguen dan A. Feringa. 2002. Risk Management Guide for Information Technology Systems. *Recommendation of National Institute of Standards and Technology Special Publication* 800-30.

Joint Task Force Transformation Initiative. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View*. NIST Special Publication 800-39.

M. M. Maulana dan S. H. Supangkat. 2006. Pemodelan Framework Manajemen Risiko Teknologi Informasi Untuk Perusahaan di Negara Berkembang. *Prosiding Konferensi Nasional Teknologi Informasi & Komunikasi untuk Indonesia*, 121-126.

Richard. A. Caralli. 2007. *Introducing OCTAVE Allegro: Improving the Information Securiy Risk Assessment Process*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419. Diakses 8 November 2019.

R. L. Krutz dan D. R. Vines. 2006. *The CISSP Prep Guide - Mastering the Ten Domains of Computer Security*. CA: Wiley Computer Publishing John Wiley & Sons, Inc

S. K. Pandey dan K. Mustafa. 2012. *A Comparative Study of Risk Assessment Methodologies for Information Systems*. Buletin Teknik Elektro dan Informatika, 1(2),111-122.

RISK ASSESSMENT PADA PENERAPAN TEKNOLOGI CLOUD COMPUTING BAGI PEMERINTAH DAERAH

Abstrak

Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus bermunculan. Adanya teknologi *Cloud Computing* memberikan harapan untuk mengoptimalkan layanan TI, infrastruktur TI, dan biaya. Berdasarkan Inpres No. 3/2003 tentang Kebijakan dan Strategi Nasional tentang Pengembangan e-Government, ada ketertarikan dari pemerintah untuk mengadopsi teknologi *Cloud Computing* ini. Dengan beragamnya infrastruktur dan sumber daya TI di daerah, perlu dilakukan analisis menyeluruh, misalnya analisis terhadap manajemen resiko sebelum pemerintah benar-benar akan mengadopsi dan menerapkan teknologi baru ini. Penilaian resiko atau *Risk Assessment* adalah salah satu langkah awal yang bisa dilakukan. Tujuannya adalah untuk mengidentifikasi resiko-resiko yang mungkin muncul dalam penerapan teknologi *Cloud* ini. Dengan mengacu pada *Risk Management Guide for Information Technology Systems* yang dikembangkan oleh *The National Institute of Standards and Technology* (NIST), diharapkan dalam makalah ini menghasilkan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud*.

Kata kunci : Teknologi *Cloud Computing*, Manajemen Resiko, *Risk Assessment*, NIST

1. Pendahuluan

Peran Teknologi Informasi (TI) dalam organisasi saat ini sangat penting sekali, dimana tingkat ketergantungan dunia usaha, badan-badan pemerintahan, dan organisasi, terhadap TI semakin tinggi. TI digunakan sebagai sarana untuk meningkatkan keunggulan kompetitif suatu organisasi melalui efektifitas dan efisiensi dalam otomasi, pengolahan, dan manipulasi data. Seiring dengan meningkatnya frekuensi kebutuhan layanan komputasi dalam organisasi yang semakin komplek, inovasi-inovasi untuk mempermudah penataan dan pengelolaan sumber daya TI di organisasi terus

bermunculan. Hal ini dibuktikan dengan munculnya berbagai alternatif teknologi yang bisa di adopsi untuk mencapai tujuan organisasi yaitu mempercepat dan mempermudah pekerjaan, misalnya di bidang pemerintahan telah mengadopsi aplikasi *e-Government* yang memanfaatkan jaringan internet dalam mendukung proses bisnis pemerintahan dan layanan publik.

Adanya Inpres No. 3/2003 tentang "Kebijakan dan Strategi Nasional tentang Pengembangan e-Government" yang bertujuan : Pengembangan e-government merupakan upaya untuk mengembangkan penyelenggaraankepemerintahan yang berbasis (menggunakan) elektronik dalam rangka meningkatkan kualitas layanan publik secara efektif dan efisien. Melalui pengembangan e-government dilakukan penataan sistem manajemen dan proses kerja di lingkungan pemerintah dengan mengoptimasikan pemanfaatan teknologi informasi. Pemanfaatan teknologi informasi tersebut mencakup 2 (dua) aktivitas yang berkaitan yaitu: 1) pengolahan data, pengelolaan informasi, sistem manajemen dan proses kerja secara elektronis; 2) pemanfaatan kemajuan teknologi informasi agar pelayanan publik dapat diakses secara mudah dan murah oleh masyarakat di seluruh wilayah negara [1].

Cloud Computing adalah teknologi bidang TI yang memanfaatkan jaringan internet berupa model komputasi dimana sumberdaya-sumberdaya seperti *storage*, *processor*, *network*, dan *software* menjadi abstrak dan dijadikan sebagai layanan di jaringan menggunakan pola *remote access*. Konten yang ditawarkan seperti *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS) menjadi solusi TI yang praktis dan ekonomis. Sifat jangkauan layanan terbagi menjadi *Public Cloud*, *Private Cloud*, dan *Hybrid Cloud*. Ini adalah salah satu inovasi bidang TI terkini yang sejak tahun 2005 di tingkatkan kemampuannya sehingga bisa mendukung aplikasi e-Government dan diharapkan dengan mengadopsi teknologi ini untuk bidang pemerintahan dapat mengurangi biaya investasi TI, meningkatkan produktivitas pegawai, dan meningkatkan pelayanan pemerintah kepada masyarakat sekaligus mampu menyelaraskan proses bisnis dengan unit pemerintahan lainnya sehingga tercipta efektifitas dan efisiensi operasional pemerintahan. Keuntungan yang dapat diperoleh bagi pemerintah dalam mengadopsi *Cloud Computing* adalah ***A clean government with no corruption*** dimana Sistem SOA (*Service Oriented Architecture*) pada *cloud computing* yang memungkinkan kolaborasi otomatis di antara *software* yang dimiliki

dunia bisnis dengan *software* yang dimiliki pemerintah memungkinkan semua transaksi yang berhubungan dengan pemerintah dilakukan tanpa campur tangan manusia seperti perhitungan dan pembayaran pajak. Hal ini akan menghilangkan korupsi yang biasanya bisa terjadi karena terlibatnya begitu banyak manusia atau petugas didalam proses tersebut, selain itu keuntungan lainnya bagi pemerintah adalah ***A more responsive government services*** dimana setiap warga negara bisa mengakses pelayanan secara *online* dari mana dan kapan saja sehingga dapat meningkatkan kualitas pelayaran pemerintah.

Dengan adanya Inpres tersebut diatas semakin menguatkan alasan perusahaan layanan *Information Communication Technology* (ICT) tanah air untuk menggarap dan memberikan layanan *Cloud Computing* untuk pemerintahan, salah satunya adalah Telkom, perusahaan BUMN yang bergerak di bidang telekomunikasi. Melalui layanan G-Cloud, Telkom berharap dapat membantu efektifitas dan efisiensi operasional pemerintahan. G-Cloud merupakan sebuah layanan ICT yang bersifat *complete*, *affordable* dan *simple* yang menyediakan media untuk mengkolaborasikan melalui Telkom Collaboration antara modul aplikasi e-Government dan Portal Pemerintahan dalam model *Cloud Computing*. G-Cloud dilengkapi dengan 12 aplikasi e-Goverment penyelenggaraan pemerintahan di daerah yang telah memenuhi kriteria yang ditetapkan Menkominfo. Telkom menargetkan layanan G-Cloud meliputi 87 kota, 348 kabupaten, 5.224 kecamatan dan 6.890 kelurahan di Indonesia [2]. Berdasarkan informasi dalam Konferensi e-Indonesia Initiatives (e-II) Forum VII 2011 yang bertempat di kampus ITB tanggal 14-15 Juni 2011, pemerintah Jawa Barat adalah salah satu provinsi di Indonesia yang akan ikut mengadopsi layanan ini.

2. Permasalahan

Meskipun pemerintah daerah sudah menetapkan tujuannya untuk mengadopsi teknologi *cloud*, perlu disadari bahwa adopsi yang dilakukan tidak semudah yang dibayangkan. Perlu pertimbangan dan analisis menyeluruh mengenai adopsi ini karena adopsi teknologi *cloud* akan melibatkan pihak ketiga (*outsourcing*) sebagai penyedia layananan. Sifat dari layanan yang diberikan yaitu *multi-tenant* maka akan ada banyak pelanggan dalam satu *platform* sehingga kemampuan untuk kustomisasi akan menjadi terbatas.

Implementasi *Cloud Computing* memiliki keuntungan dan juga memiliki resiko yang harus dihadapi saat implementasi. Pihak yang terkait dan terlibat implementasi *cloud* perlu melakukan serangkaian tindakan yang mendukung keberhasilan penerapan *cloud computing* di organisasi. Aspek-aspek resiko yang mungkin timbul saat implementasi *cloud* seperti *Service Level*, *Privacy*, *Compliance*, *Data Ownership*, *Data Mobility* perlu dikelola dengan baik melalui manajemen resiko.

Oleh karena itu dalam makalah ini akan dibahas mengenai :

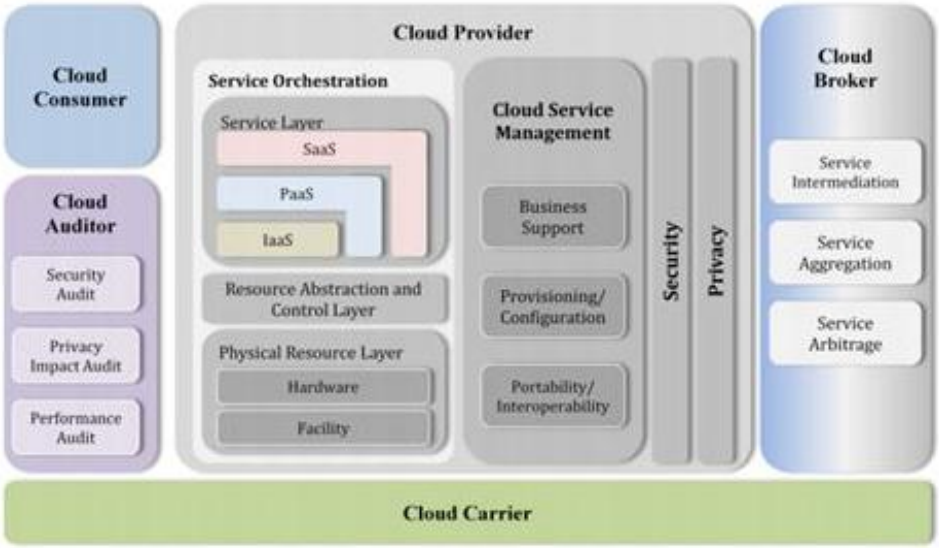
- Melakukan *Risk Assessment* atau penilaian resiko terhadap penerapan teknologi *Cloud Computing* bagi pemerintahan daerah menggunakan rekomendasi penilaian resiko yang disarankan oleh *National Institue of Standards and Technology* (NIST).
- Mendefinisikan karakteristik sistem pada teknologi *Cloud*.
- Melakukan identifikasi ancaman yang mungkin muncul saat implementasi teknologi *Cloud*.
- Melakukan identifikasi kelemahan dari teknologi *Cloud*.
- Memberikan usulan manajemen resiko yang bisa dilakukan terhadap implementasi teknologi *Cloud*.

3. Landasan Teori

Dalam landasan teori pada makalah ini akan dijelaskan secara ringkas mengenai materi yang terkait dengan topik makalah yaitu *Cloud Computing*, *Manajemen Resiko*, dan *Risk Assessment*.

3.1 *Cloud Computing*

Cloud Computing di definisikan sebagai sebuah model yang memungkinkan kenyamanan, akses on-demand terhadap sekumpulan sumber daya komputasi (seperti jaringan, server, media penyimpanan, aplikasi, dan layanan komputasi) yang konfigurasinya dapat dilakukan dengan cepat dan hanya memerlukan sedikit usaha untuk mengelola dan berhubungan dengan penyedia layanan [3].

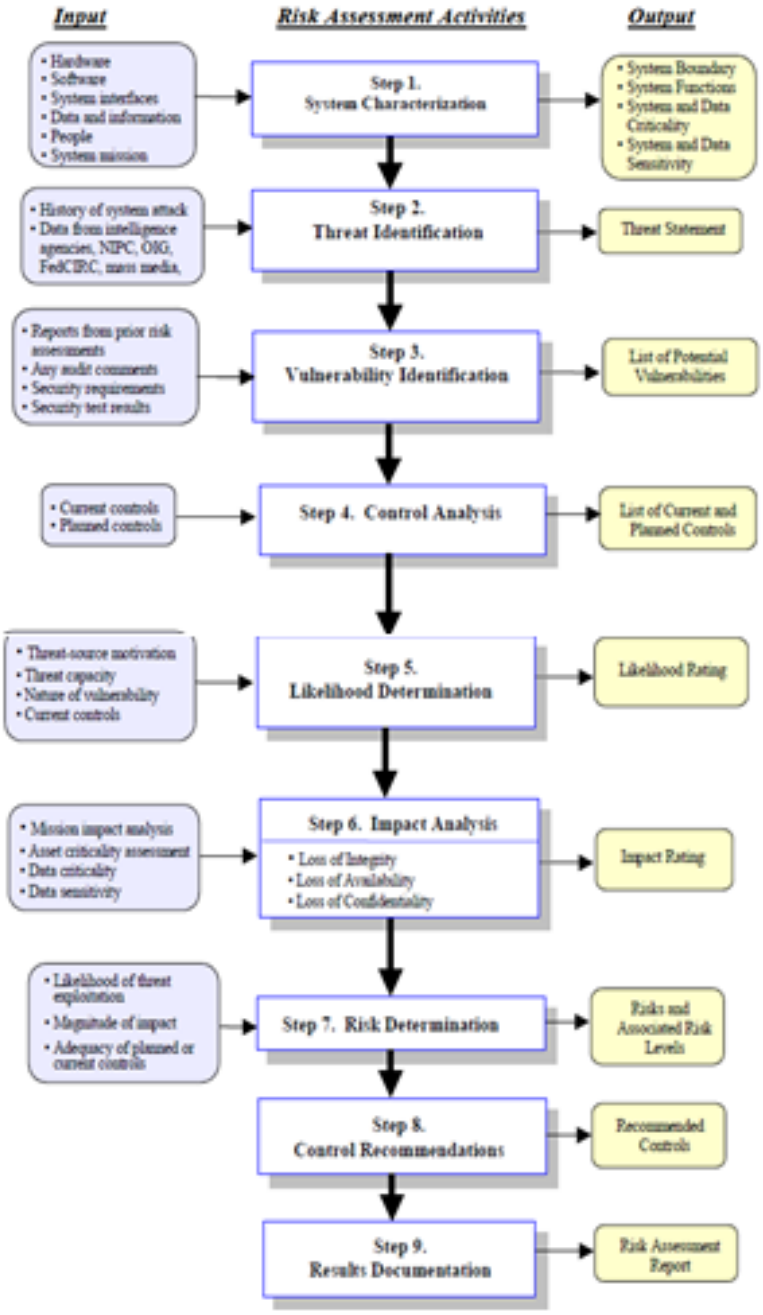


Gambar 1. Arsitektur Cloud Computing

3.2 Manajemen Resiko

Secara umum risiko dapat diartikan sebagai suatu keadaan yang dihadapi seseorang atau perusahaan dimana terdapat kemungkinan yang merugikan. Resiko adalah suatu umpan balik negatif yang timbul dari suatu kegiatan dengan tingkat probabilitas berbeda untuk setiap kegiatan. Pada dasarnya resiko dari suatu kegiatan tidak dapat dihilangkan akan tetapi dapat diperkecil dampaknya terhadap hasil suatu kegiatan. Proses menganalisa serta memperkirakan timbulnya suatu resiko dalam suatu kegiatan disebut sebagai manajemen resiko [4].

Manajemen Resiko terdiri dari 3 proses yaitu, 1) *Risk Assessment*, 2) *Risk Mitigation*, 3) *Evaluation And Assessment*. Manajemen resiko adalah proses yang dilakukan para Manajer TI untuk menyeimbangkan kegiatan operasional dan pengeluaran biaya keuangan, dalam mencapai keuntungan dengan melindungi sistemIT dan data yang mendukung misi organisasinya [5].



Gambar 2. Aktifitas Risk Assessment

3.3 *Risk Assessment*

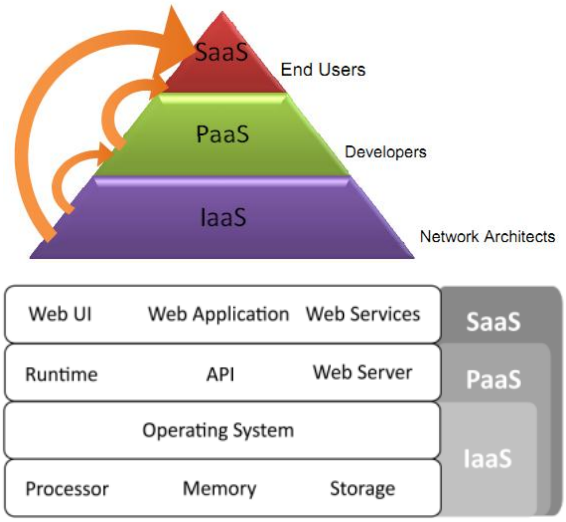
Risk Assessment atau Penilaian Resiko adalah proses pertama yang harus dilakukan dalam metodologi manajemen resiko. Risk Assessment digunakan untuk menentukan ancaman potensial dan resiko. Hasilnya adalah identifikasi kendali yang sesuai untuk mengurangi atau menghilangkan resiko. Proses ini terdiri dari 9 langkah, seperti yang diperlihatkan pada gambar 2 [5].

4. Pembahasan

Dalam pembahasan makalah ini, sebagaimana yang dijelaskan sebelumnya yaitu penilaian resiko akan mengikuti langkah-langkah yang disarankan oleh NIST, dengan pembahasan sebagai berikut :

4.1 *System Characterization*

Untuk menetapkan karakteristik sistem *Cloud Computing*, maka perlu dilihat terlebih dahulu dari layanan yang diberikannya yaitu *software as a service* (SaaS), *platform as a service* (PaaS), dan *infrastructure as a service* (IaaS). IaaS berisi perangkat keras (Processor, memory, storage) dan sistem operasi yang merupakan antarmuka antara CPU dengan perangkat menjadi sebuah paket layanan. Layanan ini digunakan oleh konsumen melalui jaringan internet secara remote. PaaS memungkinkan developer untuk membangun suatu aplikasi diatas suatu platform yang dapat dikostumisasi sehingga spesifikasi perangkat Client tidak menjadi masalah untuk membangun dan menjalankan aplikasi dengan performansi apapun. SaaS merupakan layanan dimana pengguna dapat mengeksekusi suatu aplikasi tanpa perlu menginstal aplikasi tersebut, aplikasi yang dibutuhkan telah tersedia di vendor dan dapat diakses melalui jaringan internet [6].



Gambar 3. Services Model dan Layer

Dari layanan yang dapat diberikan oleh *Cloud* maka dapat diketahui karakteristik dari sistem yaitu [5] :

1. *On-demand Self Service*, pengguna dapat menambah dan mengatur layanan tanpa intervensi siapapun.
2. *Ubiquitous Network Access*, layanan *cloud* diakses dengan bantuan internet menggunakan mekanisme dan protokol standar dan dapat diakses setiap waktu.
3. *Resource Pooling*, sumberdaya *cloud* yang digunakan untuk layanan cloud menggunakan infrastruktur yang homogen dan layanan digunakan bersama dengan pengguna lain.
4. *Rapidly Elasticity*, sumber daya harus dapat ditingkatkan dengan cepat dan elastis.
5. *Measures Services*, sumberdaya dan layanan harus diukur, dukungan optimasi penggunaan sumber daya, memberikan laporan penggunaan dan harus memiliki model bisnis *pay-as-you-go* atau dibayar saat digunakan.

4.2 Threat Identification

Cloud Security Alliance [7] mendefinisikan beberapa ancaman dalam teknologi *Cloud* yaitu :

1. *Abuse and Nefarious Use of Cloud Computing*, penyalahgunaan teknologi *cloud* dimana ada kemungkinan terjadinya penyusupan terhadap layanan melalui kegiatan Hacking. Ini bisa terjadi karena layanan IaaS yang ditawarkan tanpa batas terhadap jaringan dan *storage* sering bersinggungan dimana siapapun yang membayar dengan cara legal ataupun illegal dapat memanfaatkan layanan. Beberapa vendor *cloud* bahkan menyediakan layanan percobaan secara gratis untuk periode waku tertentu. Celah ini dapat dimanfaatkan oleh orang dengan anonimitas yang tidak berkepentingan terhadap layanan untuk melakukan penyalahgunaan layanan *cloud*.
2. *Insecure Interface and APIs*, ketidakamanan antarmuka dan API karena layanan *cloud* tergantung pada keamanan dan ketersediaan layanan umum dari API dasar. Proses otentikasi, akses kontrol, dan log harus dirancang sedemikian rupa sehingga setiap proses selalu melalui *policy* yang ditetapkan.
3. *Malicious Insiders*, ancaman dari orang dalam dimana vendor sebagai penyedia layanan bisa diakatakan sebagai outsourcing dari perusahaan yang menyewa layanan. Adanya konvergensi layanan TI dan tidak adanya transparansi akan

menyulitkan bagi perusahaan memonitor kegiatan yang dilakukan vendor terhadap asset fisik dan virtual.

4. *Shared Technology Issues*, isu penggunaan teknologi bersama dimana vendor IaaS memberikan layanan mereka dengan cara berbagi infrastruktur. Seringkali, komponen dasaryang membentuk infrastruktur ini (misalnya, CPU cache, GPU) tidak dirancang dengan sifatisolasi yang kuat untuk arsitektur multi-penyewa. Kompartementalisasi yang kuat harus digunakan untuk memastikan bahwa pelanggan individu tidak mempengaruhi operasi penyewa lain yang berjalan pada vendor *cloud* yang sama. Pelanggan tidak memiliki akses ke data penyewa lain.
5. *Data Loss or Leakage*, kehilangan dan kebocoran data dimana ada banyak cara untuk mengelola data. Contohnya adalah penghapusan atau perubahan data tanpa backup data dari konten asli. Diperlukan adanya pencegahan untuk mengakses data-data sensitif oleh orang yang tidak berkompeten terhadap data tersebut.
6. *Account or Service Hijacking*, pembajakan *account* dan layananbukan hal baru. Aktifitas ini sudah ada sejak layanan internet ada. Maka aktifitas yang samapun dapat terjadii di layanan *cloud*.
7. *Unknown Risk Profile*, profil resiko yang tidak diketahui dimana salah satu prinsip dari kepemilikan perangkat *Cloud Computing* adalah pengurangan penggunaan perangkat lunak dan perangkat keras, sehingga perusahaan lebih fokus ke kekuatan usaha bisnis mereka tanpa harus mengelola infrastruktur IT dan proses pemeliharaannya. Faktor keamanan tetap menjadi hal utama yang harus diperhatikan dalam layanan *Cloud*.

Dari definisi diatas, maka dapat diidentifikasi ancaman yang mungkin timbul pada teknologi Cloud sebagaimana ditunjukkan oleh tabel 1, sebagai berikut :

Tabel 1. Threat Identification

Threat	Source Motivation	Threat Action
Hacker	*Data burglary, Data hijacking, Data destruction*	*Information bribery, Spoofing System Intrusion, Fraud, Computer crime, DDOS, Launching dynamic attack points, Botnet command and control, Building rainbow tables*

Threat	Source Motivation	Threat Action
User anonymity	*Thef of data*	*Spoofing, Hosting malicious data, Botnet command and control, Backdoor Trap, Sniffing*
Internal outsourcing	*Hacking hobies, Organized Crime, Corporate Espionage, Sponsored Intrusion*	*Hacking, Monitoring, Accessing asset, Data Modification*

4.3 *Vulnerability Identification*

Dari hasil identifikasi ancaman, selanjutnya dilakukan *vulnerability identification* atau mengidentifikasi kelemahan dari teknologi *Cloud*. Dalam pembahasan ini materi yang diuji diambil dari hasil identifikasi ancaman dimana ancaman yang teridentifikasi merupakan kelemahan dari sistem pada layanan *Cloud* sebagai berikut :

Tabel 2. *Vulnerability Identification*

Vulnerability	Threat Action
Abuse and Nefarious Use of Cloud Computing	Pendaftaran dan proses validasi yang ketat, Meningkatkan pemantauan dan koordinasi terhadap penipuan kartu kredit, Instropeksi komprehensif lalu lintas jaringan pelanggan, Pemantauan publik blacklist.
Insecure Interface and APIs	Menganalisa kelayakan model keamanan antarmuka layanan, Otentikasi dan kontrol akses dalam transmisi yang terenkripsi
Malicious Insiders	Supply chain management yang ketat, Melakukan kontrak secara hukum terhadap outsourcing sebagai penyelenggara layanan dalam hal ini vendor penyedia layanan, Transparansi dalam keamanan informasi secara keseluruhan, Memberikan dan meminta pelaporan pelanggaran keamanan.
Shared Technology Issues	Melakukan instalasi dan konfigurasi secara aman, Pemantauan lingkungan terhadap perubahan yang tidak sah, Audit konfigurasi
Data Loss or Leakage	Menerapkan control akses API yang ketat, Menjaga integritas data dalam jalur dengan enkripsi.
Account or Service Hijacking	Memperkerjakan pemantauan proaktif untuk mendeteksi aktivitas yang tidak sah.

Vulnerability	Threat Action
Unknown Risk Profile	Disahkannya pengungkapan log aktifitas dan data, pemantauan informasi.

4.4 *Risk Management Option*

Berdasarkan hasil pencarian yang dibahas sebelumnya, dengan melihat karakteristik sistem, hasil identifikasi ancaman, dan identifikasi kelemahan, maka dapat dibuat suatu rekomendasi yang dapat dijadikan bahan pertimbangan oleh Pemerintah Daerah dalam mengadopsi teknologi *Cloud*, sebagai berikut [8] :

1. Tidak menempatkan data-data yang bersifat sensitif dalam layanan *cloud*.
2. Untuk data-data yang bersifat kritis, harus dilakukan pengamanan ekstra pada saat data dikirimkan, saat data berada dalam jaringan, dan pada saat data berada dalam layanan *cloud* dengan cara otentikasi, validasi, dan enkripsi.
3. Setiap dokumen dalam layanan *cloud* sebaiknya disertai Digital Signature, untuk memberikan keyakinan bahwa dokumen tersebut aman.
4. Pengguna layanan *cloud* harus memahami secara jelas dan mendalam tentang kemampuan dan stabilitas dari vendor penyedia layanan *cloud*.
5. Memiliki alternatif kesiapan untuk menangani gangguan layanan melalui layanan backup data pada layanan *cloud* yang lain.
6. Memahami pasal-pasal yang relevan dalam kontrak perjanjian penggunaan layanan *cloud*.
7. Jika pelanggan tidak puas dengan layanan *cloud* dari vendor atau jika vendor menghentikan layanannya, maka biaya dan waktu peralihan harus dibicarakan dalam SLA (*Service Level Agreement*)
8. Adanya jaminan kemanan untuk transisi data, langkah-langkah keamanan, dan protokol yang dibicarakan dan dicantumkan dalam SLA (*Service level Agreement*).

5. Simpulan dan Saran

Pembahasan dalam makalah ini menitikberatkan pada tiga langkah dalam *Risk Assesment* yaitu *: System Characterization*, *Threat Identification*, dan *Vulnerability Identification*. Hasilnya adalah adanya gambaran mengenai bagaimana karakteristik dari sistem cloud, apa saja ancaman yang ada dalam teknologi *cloud*, dan kelemahan apa yang ada dalam teknologi ini.

Layanan yang diberikan dalam *cloud* sebenarnya sama saja seperti layanan yang ada di internet, yang membedakannya adalah dalam layanan cloud semua infrastruktur dan aplikasi yang seharusnya ada di sisi *Client*, kini semuanya berada di sisi *Server*. Artinya, pengguna cukup menyediakan infrastruktur untuk mengakses internet agar bisa terhubung dalam layanan *cloud* untuk menggunakan berbagai aplikasi yang ditawarkan. Karena sifatnya yang Multi-Tenant atau penggunaan beragam layanan secara bersama dalam satu platform, maka teknologi ini memiliki beberapa kelemahan.

Kelemahan yang paling penting untuk diperhatikan adalah masalah keamanan. Oleh karena itu, ada beberapa hal yang harus diperhatikan oleh pemerintah daerah apabila ingin mengadopsi teknologi untuk layanan publik, yaitu :

1. Menentukan layanan apa saja yang akan digunakan di *cloud* yang dapat mendukung proses bisnis dan layanan publik yang optimal.
2. Menentukan data apa saja yang layak dan aman untuk disimpan dan digunakan dalam layanan *cloud*.
3. Memiliki sumber daya manusia yang mengerti teknologi cloud dan layanannya.
4. Memiliki alternatif penanganan masalah apabila sewaktu-waktu ada gangguan dalam layanan dan mempersiapkan opsi apabila vendor menghentikan layanannya.

Daftar Pustaka :

[1] http://www.bappenas.go.id/node/133/2173/inpres-no3-tahun-2003-tentang-kebijakan-danstrategi-nasional-pengembangan-e-governmet/.

[2] http://www.wartaegov.com/berita-1365-cloudcomputing-untuk-pemerintahan-yangefektif.html.

[3] Mell, P., Grance, T., (2009). The NIST Definition of Cloud Computing. from NIST Information Technology Laboratory: http://www.nist.gov/itl/cloud/upload/clouddefv15.pdf.

[4] Bonham, Stephen S., (2005), IT Project Portfolio Management, Artech House, Boston.

[5] Stoneburner, G., Alice Goguen and Alexis Feringa, Risk Management Guide for Information Technology Systems, Recommendation of The National Institute of Standards and Technology Special Publication 800-30, July, 2002.

[6] Fardani, A., Surendro, K., (2011), Strategi Adopsi Teknologi Informasi Berbasis Cloud Computing Untuk Usaha Kecil dan menengah di Indonesia, Seminar Nasional Aplikasi Teknologi Informasi (SNATI 2011)

[7] Cloud Security Alliance, (2010), Top Threat to Cloud Computing V1.0, csathreat.v1.0.pdf http://www.cloudsecurityalliance.org/topthreats.

[8] Cloud Computing: Benefits, Risks and Recommendations for Information Security, (2009), http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment.

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

Oleh:

Kelompok I:

1. **Pamuji Muhammad Jakak**
2. **Muhammad Irvai (182420063)**
3. **M. Apriliansyah**
4. **Anshori**

Dosen Pengampu: M. Izman Herdiansyah, M.M., Ph.D.

PROGRAM STUDI MAGISTER TEKNIK INFORMATIKA

UNIVERSITAS BINA DARMA

TAHUN AKADEMIK 2019/2020

ANALISIS MANAJEMEN RESIKO SISTEM *E-LEARNING* PADA UNIVERSITAS BINA INSAN LUBUKLINGGAU

ABSTRAK

Perkembangan teknologi informasi yang semakin pesat pada saat ini mendorong Universitas Bina Insan Lubuklinggau untuk menerapkan sistem *e-learning* sebagai sistem pembelajaran berbasis elektronik yang mempermudah proses transformasi atau pertukaran informasi antara pihak Universitas Bina Insan dengan mahasiswa. Namun dalam pemanfaatan aplikasi *e-learning* itu sendiri, terkadang pihak Universitas kesulitan dalam mengidentifikasikan kemungkinan resiko-resiko yang terjadi. Adapun tujuan dari penelitian ini adalah melakukan suatu analisis resiko yang berkaitan dengan penerapan aplikasi *e-learning* di Universitas Bina Insan Lubuklinggau dengan menggunakan metode *OCTAVE Allegro.* Metode ini terdiri dari 8 tahap yang diklasifikasikan menjadi 4 kategori untuk mendapatkan tindakan pencegahan atau pengendalian pada Universitas Bina Insan. Hasil dari penelitian ini berupa pertimbangan strategi bagi Universitas Bina Insan mengenai penyimpanan aset informasi yang kritis dan pengembangan terhadap fitur aplikasi *e-learning* secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat dan pemanfaatan aplikasi *e-learning* menjadi lebih efektif.

Kata kunci: analisis resiko, manajemen resiko, *OCTAVE Allegro, e-learning.*

1. PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan sistem dan teknologi informasi saat ini, banyak organisasi yang memanfaatkan kemajuan tersebut untuk mendorong proses bisnisnya. Organisasi menyusun dan merencanakan strategi bisnis maupun teknologi informasi untuk menghasilkan kinerja yang lebih baik. Dengan adanya pemanfaatan teknologi informasi, informasi yang dihasilkan dapat digunakan lebih lanjut untuk proses pengambilan keputusan yang cepat dan tepat. Selain itu, teknologi informasi ini juga membantu organisasi dalam pengelolaan data-data secara akurat dan *real-time*. Banyak organisasi yang

menerapkan teknologi informasi yang *up-to-date* dan terbaru, termasuk perguruan tinggi. Salah satu perkembangan teknologi informasi yang sering digunakan dalam suatu perguruan tinggi adalah penerapan *e-learning* sebagai sistem pembelajaran berbasis elektronik. Pembelajaran seperti ini lebih praktis dilakukan karena *e-learning* dapat memberikan keuntungan bagi suatu perguruan tinggi dalam memperlancar pengaksesan informasi kepada mahasiswa. Hal ini juga bermanfaat untuk mempermudah proses transformasi atau pertukaran informasi antara kedua pihak.

Aktivitas-aktivitas akademik yang berkaitan dengan sistem *e-learning* dapat memberikan kemudahan pengaksesan materi perkuliahan bagi mahasiswa. Selain itu, mahasiswa dapat melakukan *download* dan *upload* tugas, melakukan *post* terhadap forum diskusi, dan mengakses kuis. *E-learning* Universitas Bina Insan dapat membantu pihak Universitas dalam memberikan informasi berupa pengumuman-pengumuman yang berkaitan dengan proses perkuliahan yang berlangsung. Selain itu, mahasiswa Universitas Bina Insan dapat mendalami penggunaan *e-learning* terkait dengan perkuliahannya. Mahasiswa dapat berfokus pada penguasaan materi perkuliahan yang diberikan oleh dosen secara langsung. Sistem pembelajaran ini dapat memfokuskan mahasiswa pada pengerjaan tugas-tugas secara mandiri dan dapat memberikan pengetahuan tambahan terkait dengan penerapan teknologi informasi yang berkaitan dengan pendidikan.

E-learning ini juga memberikan dampak positif terhadap dosen yang memberikan pengajaran dalam perkuliahan yang berlangsung sesuai dengan penetapan jadwal perkuliahan. Setiap dosen dapat mengetahui seberapa jauh pemahaman mahasiswa terhadap perkuliahan yang diberikan di Universitas Bina Insan Lubuklinggau. Dosen juga dapat menerima *feedback* dari mahasiswa secara langsung dan dosen dapat memberikan tanggapan kepada mahasiswa tanpa terhalang oleh batasan lokasi dan waktu. Selain dampak **positif** yang dihasilkan dari penerapan *e-learning* di Universitas Bina Insan, maka selalu terdapat risiko yang nantinya dapat memberikan dampak **negatif**. Adapun kemungkinan **risiko-risiko** yang dapat terjadi selama proses

perkuliahan berlangsung dalam *e-learning*, seperti terjadinya *down server* karena banyak mahasiswa yang melakukan pengaksesan *e-learning* secara bersamaan dan terdapat keterbatasan sumber daya dalam penanganan dan pemeliharaan *e-learning*. Selain itu, *e-learning* juga terdapat keterbatasan kapasitas terhadap *file* yang bisa di-*upload* dan penyimpanan data mahasiswa dalam sistem *e-learning*. Ada kemungkinan terdapat keterbatasan fitur-fitur dalam *e-learning* yang memiliki tingkat kompleksitas yang berbeda-beda. Hal ini dapat menyebabkan dosen dan mahasiswa bisa kesulitan menggunakan *e-learning*.

Dengan adanya kemungkinan **risiko-risiko** yang muncul selama proses implementasi *e-learning*, maka diperlukan manajemen risiko di Universitas Bina Insan untuk mengelola dan meminimalkan risiko tersebut. Oleh karena itu, diperlukan adanya tindakan pengendalian maupun pengawasan sistem *e-learning* yang dilakukan secara teratur. Proses-proses pengelolaan terhadap kemungkinan risiko di Universitas dapat dilakukan metodologi manajemen risiko. Untuk mengidentifikasikan kemungkinan risiko-risiko secara akurat, maka digunakan metode ***OCTAVE Allegro***. Metode ini menjabarkan identifikasi terhadap penilaian risiko dan dapat memberikan tindakan mitigasi terhadap risiko tersebut. Hal ini dapat membantu Universitas Bina Insan untuk menghadapi permasalahan-permasalahan yang terjadi pada *e-learning*.

1.2 Rumusan Masalah

Adapun rumusan permasalahan yang dilakukan dalam penelitian ini adalah

1. pihak Universitas Bina Insan kesulitan mengidentifikasikan tentang kemungkinan risiko-risiko yang dapat terjadi selama implementasi *elearning* di Universitas dengan metode *OCTAVE Allegro*
2. Evaluasi tindakan pengelolaan risiko sebagai tindakan pencegahan atau pengendalian pada Universitas Bina Insan

1.3 Tujuan Penelitian

Tujuan dilakukan proses penelitian ini adalah untuk melakukan analisis terhadap proses pengelolaan risiko sebagai bentuk manajemen risiko dalam hal implementasi *e-learning* di Universitas Bina Insan Lubuklinggau.

2. Tinjauan Pustaka

2.1 Sistem *E-Learning*

Sistem *E-learning* merupakan pendekatan inovatif dalam hal pengiriman pembelajaran untuk bidang pendidikan yang lebih tinggi dan menyediakan alternatif bagi mahasiswa untuk belajar tanpa adanya keterbatasan waktu dan tempat (Al-Samarraie et al., 2017). *E-learning* yang diterapkan dalam perguruan tinggi merupakan salah satu strategi pembelajaran yang efektif dan efisien yang memanfaatkan sistem dan teknologi informasi sehingga dapat menggantikan pembelajaran *face-to-face*. Penggunaan *e-learning* dalam perguruan tinggi yang digunakan oleh dosen sebagai *workplace tool* memiliki potensi dalam hal transformasi pengajaran dan pengalaman pembelajaran (King & Boyatt, 2014).

2.2 Manajemen Resiko

Setiap penggunaan sistem dan teknologi informasi selalu terdapat risiko yang muncul sebagai bentuk ancaman dan ketidakpastian yang dapat memberikan dampak negatif dalam suatu perusahaan atau perguruan tinggi. Tingkat probabilitas atau peluang terjadinya risiko dalam suatu organisasi berbeda-beda tergantung dari faktor-faktor pemicu munculnya risiko tersebut, seperti pengetahuan para pakar dan data-data histori dari setiap aktivitas yang telah selesai dilakukan (Aqlan & Lam, 2015). Risiko dapat terjadi pada pengelolaan aset dalam suatu organisasi karena aset bisa mengalami kerusakan ataupun kesalahan penggunaan aset tersebut oleh pihak terkait (Tobing & Puspa, 2015). Selain itu, terdapat faktor-faktor internal dalam suatu perguruan tinggi yang dapat memunculkan berbagai risiko sehingga penggunaan *e-learning* yang memengaruhi hubungan antara dosen dengan mahasiswa. Tingkat

pengetahuan dan pengalaman yang terdapat masing-masing dosen sebagai pihak pengajar dan penyampaian materi perkuliahan kepada mahasiswa bisa memunculkan kesalahpahaman penyampaian informasi kepada mahasiswa (Mackay & Tymon, 2014).

2.3 Metode OCTAVE Allegro

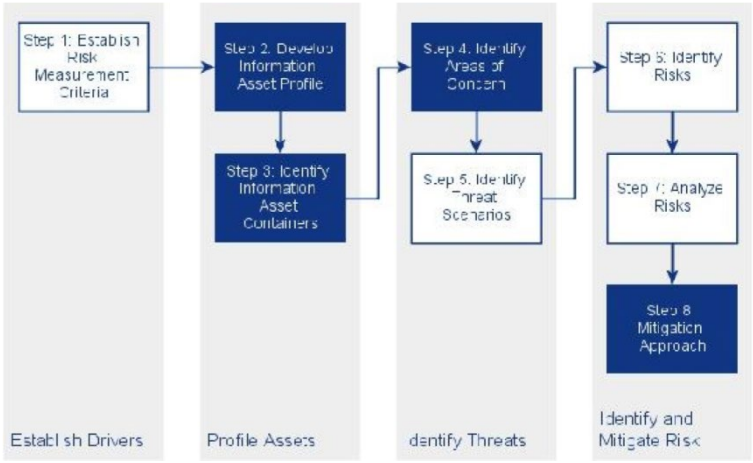
Metode OCTAVE merupakan singkatan dari *the Operationally Critical Threat, Asset, and Vulnerability Evaluation* adalah seperangkat alat, teknik, dan metode untuk menilai strategi keamanan informasi yang berbasis risiko dan perencanaan. Metode OCTAVE terdiri dari tiga prinsip dasar administrasi keamanan, yaitu: *confidentiality, integrity,* dan *availability* (Pandey & Mustafa, 2012). Metode penilaian OCTAVE Allegro yang dilakukan oleh *Carnegie Mellon University Software Engineering Institute (SEI)* yang memiliki kemampuan untuk memberikan hasil penilaian risiko yang kuat, dengan investasi yang relatif kecil dalam waktu dan sumber daya, bahkan untuk organisasi-organisasi yang tidak memiliki keahlian manajemen risiko yang luas (Keating, 2014). Metode OCTAVE Allegro dinilai sesuai untuk digunakan oleh individu yang ingin melakukan penilaian risiko secara komprehensif tanpa keterlibatan organisasi, ahli, atau sumber daya lainnya sehingga metode ini direkomendasikan untuk penilaian risiko *container* informasi (Maček, Magdalenić, & Ivković, 2011).

Metode *OCTAVE Allegro* terdiri dari delapan tahap yang diklasifikasikan menjadi empat kategori yaitu sebagai berikut (Caralli et al., 2007).

a. Menetapkan apa yang menjadi arahan organisasi dan mengembangkan kriteria pengukuran risiko didalamnya
b. Membuat profil aset yang dimiliki organisasi dengan mengidentifikasi persyaratan keamanan, dan mengidentifikasi semua lokasi dimana aset tersebut disimpan, diangkut, atau diproses
c. Mengidentifikasi ancaman untuk setiap aset informasi dalam konteks wadah aset tersebut

d. Mengidentifikasi, analisis dan mitigasi risiko terhadap aset informasi dan pengembangan terhadap pendekatan mitigasi

Berikut ini adalah gambar kategori-kategori dalam metode *OCTAVE Allegro* (Caralli et al., 2007).



Gambar 1. Pendekatan Metode *OCTAVE Allegro*

Terdapat delapan langkah-langkah yang terdapat dalam mdetode OCTAVE Allegro (Caralli et al., 2007).

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini terdapat *organizational driver* yang digunakan untuk mengevaluasi dampak risiko pada misi dan tujuan bisnis, serta mengenali *impact area* yang paling prioritas. Kriteria pengukuran risiko didokumentasikan dalam bentuk *Risk Measurement Criteria Worksheets* dan pemberian nilai prioritas *impact area* dalam bentuk *Impact Area Ranking Worksheet.*

Langkah 2 – Mengembangkan Profil Aset Informasi

Langkah ini dilakukan dengan identifikasi aset informasi dimana profil tersebut merupakan representasi aset yang menggambarkan fitur, kualitas, karakteristik, dan nilai yang unik. Langkah ini berguna untuk memastikan bahwa deskripsi

aset sudah jelas dan konsisten sehingga dapat mempermudah penyusunan kebutuhan keamanan yang paling penting untuk aset informasi.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Langkah ini mengacu pada identifikasi faktor internal dan eksternal yang penting dilakukan terhadap kontainer sebagai tempat penyimpanan, pengiriman, dan pemrosesan aset informasi.

Langkah 4 – Mengidentifikasi Area Masalah yang Diperhatikan

Langkah ini dilakukan dengan proses pengembangan profil risiko dari aset informasi melalui pertukaran pikiran. Pertukaran pikiran/ *brainstorming* mengenai kondisi atau situasi tertentu untuk mengetahui komponen ancaman yang akan dihadapi. Dengan berpedoman pada dokumen *information asset risk environment maps* dan *information asset risk worksheet* maka dilakukan pencatatan *area of concern.* Setelah itu, dilakukan review dari kontainer untuk membuat *Area of Concern* dan mendokumentasikan setiap *Area of Concern.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Langkah ini dilakukan dengan identifikasi skenario ancaman tambahan yang lebih jauh dari area-area pada langkah sebelumnya berfokus pada properti ancaman. Aktivitas ini dapat menggunakan *Threat Scenario Questionnaries* dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Langkah ini digunakan untuk menentukan *threat scenario* terhadap gambaran risiko secara terperinci. *Threat scenario* didokumentasikan dalam bentuk *information asset risk worksheet* yang dapat memberikan dampak bagi organisasi.

Langkah 7 – Menganalisis Risiko

Langkah ini mengacu pada dokumentasi yang terdapat pada *information asset risk worksheet.* Setelah itu, dilakukan review dan menghitung nilai risiko relatif yang dapat digunakan untuk menganalisis seberapa jauh dampak risiko tersebut dan memutuskan strategi terbaik dalam menghadapi risiko.

Langkah 8 – Memilih Pendekatan Pengurangan

Langkah ini dilakukan dengan mengurutkan setiap risiko yang diidentifikasi berdasarkan nilai risikonya sehingga dapat ditentukan pendekatan mitigasi terhadap risiko tersebut. Hal ini dilakukan dengan memprioritaskan risiko-risiko diikuti dengan pendekatan pengembangan strategi penanganan risiko. Strategi tersebut juga harus mempertimbangkan nilai aset dan kebutuhan keamanan, container aset, serta lingkungan operasional yang unik dalam organisasi.

3. Pembahasan

Adapun pelaksanaan penilaian risiko terhadap implementasi *e-learning* yang dilakukan di Universitas Bina Insan berdasarkan 8 fase atau langkah utama dalam metode OCTAVE Allegro adalah sebagai berikut:

Langkah 1 – Membangun Kriteria Pengukuran Risiko

Pada langkah ini, dibangun *organizational drivers* untuk penentuan *impact area* yang paling penting serta memberikan nilai skala prioritas pada *impact area* yang telah ditentukan. Terdapat 5 area dampak dalam OCTAVE Allegro yang menentukan nilai kualitatif dengan ukuran rendah, sedang, dan tinggi. Prioritas *impact area* yang dipilih adalah reputasi dan kepercayaan pelanggan, keuangan, produktivitas, keamanan dan kesehatan, serta denda dan penalti.

Berikut ini adalah tabel *impact area* yang berfokus pada reputasi dan kepercayaan mahasiswa.

Tabel 1. Allegro *Worksheet* 1

Impact Area	*Low*	*Medium*	*High*
Reputasi	Reputasi Universitas	Reputasi Universitas	Reputasi Universitas

	Bina Insan tidak terpengaruh dari perubahan *e-learning*	Bina Insan terpengaruh sedikit dari perubahan *e-learning*	Bina Insan terpengaruh banyak dari perubahan *e-learning*
Kepercayaan Mahasiswa	Kurang dari 2% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*	2% -10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*	Lebih dari 10% kehilangan kepercayaan mahasiswa terhadap fitur *e-learning*

Berikut ini adalah tabel *impact area* yang berfokus pada keuangan.

Tabel 2. Allegro *Worksheet* 2

Impact Area	*Low*	*Medium*	*High*
Biaya Operasional	Peningkatan biaya operasional saat implementasi *e-learning* kurang dari 2,5%	Peningkatan biaya operasional saat implementasi *e-learning* sebesar 2,5% - 5%	Peningkatan biaya operasional saat implementasi *e-learning* lebih dari 5%
Kerugian	Kurang dari 10jt kerugian tahunan jika *e-learning* ada gangguan	Antara 10jt – 50jt kerugian tahunan jika *e-learning* ada gangguan	Lebih dari 50jt kerugian tahunan jika *e-learning* ada gangguan

Dari tabel-tabel di atas, diuraikan beberapa contoh *allegro worksheet* dari semua area dampak yang berfokus di area reputasi dan kepercayaan mahasiswa dan keuangan. Dari masing-masing area dampak yang diidentifikasikan, maka ditentukan estimasi tingkat prioritas risiko apakah *low, medium*, dan *high* dan tingkat kerusakan yang mungkin terjadi saat implementasi *e-learning* Universitas Bina Insan. Berikut ini adalah tabel skala prioritas *impact area*.

Tabel 3. Skala Prioritas *Impact Area*

Priority	*Impact Area*
1	Reputasi & Kepercayaan Mahasiswa
2	Keuangan
3	Produktivitas
4	Keamanan & Kesehatan
5	Denda & Penalti

Dari tabel-tabel identifikasi masing-masing area dampak risiko tersebut, maka didapatkan urutan prioritas area dampak, yaitu bagian reputasi dan kepercayaan mahasiswa sebagai prioritas pertama, bagian keuangan sebagai prioritas kedua, bagian produktivitas sebagai prioritas ketiga, bagian denda dan penalti sebagai prioritas keempat, dan bagian keamanan dan kesehatan sebagai prioritas kelima.

Langkah 2 – Mengembangkan Profil Aset Informasi

Profil aset informasi kritis (*Critical information assets profile*) terdiri dari deskripsi aset informasi kritis, alasan pemilihan, dan pemilik (pengelola). Profil aset informasi kritis dilengkapi dengan persyaratan (*requirements*) keamanan yang harus ada untuk melindungi aset tersebut dengan menyatakan kerahasiaan (*confidentiality*), integritas (*integrity*), ketersediaan (*availability*), dan persyaratan keamanan lainnya. Berikut ini adalah tabel *critical information asset*.

Tabel 4. *Critical Information Asset Profile*

Allegro Worksheet	*Critical Information Asset*	
(1) Critical Asset	***(2) Rationale for Selection***	***(3) Description***
Peningkatan proses pembelajaran mahasiswa yang yang semakin bermutu	Penerapan *e-learning* sangat penting dilakukan untuk meningkatkan kinerja mahasiswa dan mempermudah pengaksesan materi perkuliahan, mengerjakan tugas dan kuis secara efektif dan efisien, serta dapat meningkatkan hubungan yang baik antara dosen dengan mahasiswa. Hal ini berpengaruh terhadap nilai mahasiswa.	Informasi ini terdiri dari fiturfitur *e-learning*, program studi, materi dan jadwal kuliah, jumlah kelas, deskripsi tugas dan kuis, jumlah akses fitur *elearning* oleh mahasiswa dan dosen.
(4) Owner		

Bagian Pusat Pembelajaran Elektronik		
(5) Security Requirements		
Confidentiality	Informasi selama proses perkuliahan berlangsung sangat penting untuk didistribusikan bagi mahasiswa, dosen, dan program studi. Bagian program studi menggunakan informasi ini untuk mengolah nilai mahasiswa dan melakukan evaluasi terhadap minat belajar mahasiswa melalui sistem *e-learning*.	
Integrity	Informasi selama proses perkuliahan harus benar dan *up-to-date* sesuai dengan perkembangan zaman serta mahasiswa selalu mendapatkan informasi tersebut jika terdapat perubahan antara dosen dengan mahasiswa. Bagian program studi melakukan distribusi informasi tersebut kepada dosen yang nantinya akan didistribusikan ke mahasiswa secara komprehensif.	
Availability	Informasi selama proses perkuliahan harus tersedia dengan lengkap dan jelas bagi program studi, mahasiswa, dan dosen termasuk instruksi yang diberikan, deskripsi tugas dan kuis, dan proses pengerjaan pelatihan dalam *e-learning*.	
(6) Most Important Secu rity Requirement		
Confidentiality	*Integrity*	√ ***Availability***

Dari tabel tersebut, terdapat identifikasi profil aset informasi yang kritis berupa peningkatan proses pembelajaran mahasiswa yang semakin bermutu di Universitas Bina Insan sehingga dapat diketahui risiko yang dihadapi Universitas Bina Insan.

Langkah 3 – Mengidentifikasi Kontainer dari Aset Informasi

Identifikasi *information asset container* yang terbagi menjadi tiga yaitu *technical, physical,* dan *people* masing-masing memiliki sisi eksternal dan internal dengan menggunakan *worksheet information asset risk environment map.*

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi teknikal.

Tabel 5. ***Information Asset Risk Environment Map (Technical)***

Container Description	*Owner(s)*
Internal	
E-mail Server, Database Server, Internal Network	Divisi TI
Appliction Server	Divisi TI, Program Studi
Personal Computer	Dosen, Program Studi

External	
Internet, External Network.E-learning Web	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi fisik.

Tabel 6. *Information Asset Risk Environment Map (Physical)*

Container Description	*Owner(s)*
Internal	
Paper copies dari banyaknya akses *e-learning* secara rutin oleh mahasiswa	Program Studi, Bagian Pembelajaran Elektronik
External	
Paper copies dari kehadiran setiap mahasiswa	Mahasiswa

Berikut ini adalah tabel *information asset risk environment map* yang dilihat dari segi sumber daya manusia.

Tabel 7. *Information Asset Risk Environment Map (People)*

Container Description	*Owner(s)*
Internal	
Dosen, Staf Program Studi	Program Studi
External	
Mahasiswa	Mahasiswa

Langkah 4 – Mengidentifikasi Area Masalah

Identifikasi *areas of concerns* dilakukan untuk meninjau kembali setiap *container* untuk mempertimbangkan dan menentukan *area of concern* yang potensial dilanjutkan dengan melakukan dokumentasi setiap *areas of concern* yang telah diidentifikasi. *Areas of concern* diperluas untuk mendapatkan *threat scenarios* dan didokumentasikan untuk melihat apakah memengaruhi *security requirements.*

Langkah 5 – Mengidentifikasi Skenario Ancaman

Identifikasi *threat scenario* yang memberikan gambaran mengenai *property* dari *threat,* antara lain *actor, means, motives, outcome* dan *security requirement.* Selain itu, langkah ini dilengkapi dengan *Information Asset Risk Worksheets* untuk setiap *threat scenario* yang umum.

Langkah 6 – Mengidentifikasi Risiko

Identifikasi risiko bertujuan untuk menentukan bagaimana *threat scenario* memberikan dampak bagi organisasi serta menentukan tingkatannya apakah masuk ke kategori *high, medium* atau *low.* Selain itu, dilakukan perhitungan *relative score* untuk membantu organisasi dalam menganalisis risiko serta menentukan strategi yang tepat untuk menghadapi risiko.

Berikut ini adalah tabel penentuan nilai prioritas berdasarkan *impact area*.

Tabel 8. *Impact – Priority Score*

Impact Area	*Priority*	*Impact Score*		
		Low (1)	*Medium (2)*	*High (3)*
Reputasi & Kepercayaan Mahasiswa	1	1	2	3
Keuangan	2	2	4	6
Produktivitas	3	3	6	9
Keamanan dan Kesehatan	5	5	10	15
Denda dan Penalti	4	4	8	12

Langkah 7 – Menganalisis Risiko

Analisis risiko dilakukan pada setiap *areas of concern* terhadap *information asset* serta identifikasi konsekuensi yang terjadi berdasarkan *relative risk score.* Nilai risiko relatif diperoleh dengan cara mempertimbangkan sejauh mana konsekuensi atas dampak risiko terhadap berbagai *impact area* dan estimasi kemungkinan terjadi risiko tersebut.

Berikut ini adalah tabel penilaian risiko relatif.

Tabel 9. *Relative Risk Score*

Area of Concern	*Risk*			
Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *elearning* secara bersamaan setiap harinya	Konsekuensi	Diperlukan waktu pemrosesan *e-learning* untuk melakukan *back-up* terlebih dahulu dan perubahan terhadap prosedur perkuliahan		
	Severity	Area Terdampak	Nilai	Skor
		Keuangan	Medium	4
		Reputasi dan Kepercayaan Mahasiswa	High	3
		Produktivitas	High	9
		Denda dan Penalti	Low	4

		Keselamatan dan Kesehatan	Low	5
	Nilai Risiko Relatif			25

Langkah 8 – Memilih Pendekatan Pengurangan

Berdasarkan pengelompokkan risiko yang diidentifikasikan, maka dilakukan pemilihan pendekatan mitigasi. Hal ini dilakukan dengan cara memprioritaskan risiko – risiko berdasarkan nilai risiko relatif, kemudian mengembangkan strategi mitigasi dengan mempertimbangkan nilai dari aset dan kebutuhan keamanan, kontainer atas aset, serta lingkungan operasional yang unik dari organisasi. Berikut ini adalah tabel matriks penentuan nilai risiko.

Tabel 10. *Relative Risk Matrix*

Risk Score		
30 to 45	16 to 29	0 to 15
POOL 1	POOL 2	POOL 3

Berikut ini adalah tabel pendekatan yang menentukan tindakan dalam penanganan risiko.

Tabel 11. *Mitigation Approach*

POOL	*Mitigation Approach*
POOL 1	*Mitigate*
POOL 2	*Mitigate or Defer*
POOL 3	*Accept*

Dari nilai risiko relatif yang didapatkan sebesar 25, maka nilai risiko tersebut dapat dikategorikan ke dalam POOL 2 yang memiliki pendekatan *mitigate* atau *defer*.

Berikut ini adalah tabel strategi pengendalian risiko terhadap risiko-risiko yang dihadapi Universitas Bina Insan

Tabel 12. *Risk Mitigation*

Risk Mitigation	
Area of Concern	Perubahan fitur-fitur *e-learning* untuk pengaksesan keseluruhan materi kuliah, tugas, dan kuis serta banyaknya mahasiswa akses *e-learning* secara bersamaan setiap harinya
Action	Mitigasi
Container	Kontroli
Server	Melakukan filter tehadap informasi yang dihasilkan dari setiap fitur *e-learning*

Internet	Memastikan bahwa jaringan internet telah stabil untuk akses *e-learning*
Dosen	Memastikan bahwa semua instruksi sudah diditribusikan secara menyeluruh
Program Studi	Melakukan *back-up* terhadap materi perkuliahan/ informasi terbaru dari *e-learning*
Bagian Pembelajaran Elektronik	Memastikan bahwa akses fitur *e-learning* dapat dilakukan dosen dan mahasiswa sesuai dengan prosedur perkuliahan dan melakukan *report* terkait dengan akses *e-learning* dan perubahan fitur-fitur *e-learning*

4. Kesimpulan

Analisis manajemen risiko yang dapat mengidentifikasikan *area of concern* yang berdampak pada Universitas Bina Insan. Penilaian risiko dari masing-masing *area of concern* tersebut dapat dilakukan dengan metode OCTAVE Allegro. Selain itu, Universitas Bina Insan dapat melakukan penilaian risiko berdasarkan tingkat prioritas dan besarnya dampak *e-learning* terhadap proses pembelajaran mahasiswa. Setelah mengidentifikasi adanya risiko yang akan berpengaruh terhadap keberlangsungan implementasi *e-learning*, maka Universitas Bina Insan melakukan identifikasi pendekatan strategi atau mitigasi yang berfokus dari aspek lingkungan internal dan eksternal organisasi.

Berdasarkan hasil analisis manajemen risiko yang dilakukan, maka terdapat area perhatian mengenai perubahan fitur-fitur *e-learning* untuk akses material kuliah, tugas, dan kuis serta mengetahui hasil terhadap banyaknya akses *e-learning* yang dilakukan oleh mahasiswa dan dosen. Dari area perhatian tersebut, maka didapatkan konsekuensi berupa waktu pemrosesan *e-learning* untuk melakukan *back-up* dan memantau perubahan prosedur perkuliahan dengan mempertimbangkan kelima area dampak yang sudah diidentifikasi nilai prioritas risikonya. Dari hasil penelitian ini, Universitas Bina Insan juga harus mempertimbangkan strategi mana yang diutamakan untuk penyimpanan aset informasi yang kritis dan fitur-fitur *e-learning* yang perlu dikembangkan secara detail sehingga kinerja dosen dan mahasiswa semakin meningkat. Untuk penelitian berikutnya, diharapkan dapat melakukan identifikasi risiko yang mendalam dan menyeluruh. Tidak hanya melihat sisi dari penggunaan fitur-fitur *e-learning*, tetapi juga mempertimbangkan

pengembangan sistem *e-learning* dengan memperhatikan lingkungan eksternal perkuliahan dalam Universitas Bina Insan.

5. Daftar Pustaka

Al-Samarraie, H., Teng, B. K., Alzahrani, A. I., & Alalwan, N. 2017. E-learning continuance satisfaction in higher education: a unified perspective from instructors and students. *Studies in Higher Education*, 1–17.

Aqlan, F., & Lam, S. S. 2015. Supply chain risk modelling and mitigation. *International Journal of Production Research*, 1–17.

Caralli, R., Stevens, J. F., Young, L. R., & Wilson, W. R. 2007. *Introducing OCTAVE Allegro : Improving the Information Security Risk Assessment Process*. *Young*.

Dewi, N. A. N., & Yudana, I. G. P. H. 2016. Analisa Manajemen Risiko Pada Sistem Akademik Di STMIK STIKOM Bali. In *Seminar Nasional Teknologi Informasi dan Multimedia*, 7–12.

Ekelhart, A., Fenz, S., & Neubauer, T. 2009. AURUM: A framework for information security risk management. In *Proceedings of the 42nd Annual Hawaii International Conference on System Sciences, HICSS*: 1–10. https://doi.org/10.1109/HICSS.2009.82

Jakaria, D. A., Dirgahayu, R. T., & Hendrik. 2013. Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro. In *Seminar Nasional Aplikasi Teknologi Informasi. (SNATI)* (pp. 37–42).

Keating, C. G. 2014. *Validating the OCTAVE Allegro Information Systems Risk Assessment Methodology: A Case Study. NSUWorks*. Nova Southeastern University.

King, E., & Boyatt, R. 2014. Exploring factors that influence adoption of e-learning within higher education. *British Journal of Educational Technology*, 1–9.

Matondang, N., Isnainiyah, I. N., & Muliawati, A. 2018. Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). *Rekayasa Sistem Dan Teknologi Informasi*, *2*(1), 282–287.

Tobing, J. J. L., & Puspa, A. K. 2015. Analisis Manajemen Resiko Untuk Evaluasi Aset Menggunakan Metode Octave Allegro. *Jurnal Manajemen Sistem Informasi Dan Teknologi*, *5*(1), 28–30.