METODA PENGAJARAN MANAJEMEN RESIKO TEKNOLOGI INFORMASI DI PERGURUAN TINGGI

Tjahjo Adiprabowo
Prodi Teknik Telekomunikasi,Engineering School, Telkom University
Jl. Telekomunikasi No. 1 Terusan Buah Batu,Bandung, 40257
Telp: (022) 70501961, Fax : (022) 7562721
E-mail : tjahjo.a@gmail.com

Abstrak

Pengajaran Manajemen Resiko Teknologi Informasi di perguruan tinggi memerlukan metoda tersendiri. Mahasiswa diharapkan dapat mengerti dan memahami apa yang dimaksud dengan manajemen resiko beserta komponen-komponennya. Selain itu mahasiswa juga diharapkan dapat menerapkan pengetahuan tentang manajemen resiko ini dalam dunia nyata yaitu di lingkungan kerjanya nanti, baik itu di sektor industri, pemerintahan, pendidikan, perdagangan, kesehatan, dan lain-lain. Oleh karena itu pengajaran Manajemen Resiko sebaiknya tidak hanya berupa teori, tetapi mencakup juga studi kasus. Kemudian untuk meningkatkan pengetahuan sekaligus keterampilan mahasiswa, studi kasus mereka sampaikan di depan kelas dalam bentuk presentasi dan diskusi. Metoda ini berhasil baik dalam pengajaran Manajemen Resiko kepada mahasiswa, terlihat dari nilai akhir yang cukup tinggi yang berhasil dicapai oleh mahasiswa.

Kata kunci: *pengajaran, manajemen resiko, teori, studi kasus, presentasi, diskusi*

Abstract

In a tertiary school, teaching Risk Management for Information Technology System needs special methods. The students are expected to understand and comprehend what Risk Management is and its components are. Furthermore, the students are expected to be able to implement their knowledge about Risk Management to the real world, which is their working environment, either in industry, government, education, commerce, health, or other sectors. That is why teaching Risk Management had better be presented not only as theories but also as case studies. Then to improve students' cognition as well as their skill, they conduct to a presentation and discussion over the case studies. This Risk Management teaching method has been proven highly effective, judging from the students' final scores.

Key words*: teaching, risk management, theories, case studies, presentation, discussion*

1. PENDAHULUAN

Tujuan utama dari institusi yang menyelenggarakan manajemen resiko adalah untuk melindungi institusi dan kemampuannya dalam mencapai visi dan misi institusi. Penerapan manajemen resiko ini sangat luas, dia dapat diterapkan di bidang teknologi informasi, di bidang pendidikan[2], di bidang perdagangan, di bidang hukum, di bidang kesehatan[3], dan lain-lain. Oleh karena itu untuk membatasi permasalahan, dalam makalah ini hanya akan dibahas manajemen resiko yang diterapkan pada sistem teknologi informasi.

Peran Perguruan Tinggi dalam hal ini adalah mempersiapkan sumber daya manusia yang dapat melaksanakan Manajemen Resiko dengan baik. Untuk itu diperlukan metode pengajaran yang tepat supaya mahasiswa dapat memahami dengan baik tentang Manajemen Resiko khususnya di bidang teknologi informasi dan pada gilirannya menerapkan Manajemen Resiko ini di tempat dia bekerja nantinya dengan baik.

Metodologi yang digunakan dalam metode pengajaran ini adalah *Action Research* yang terdiri dari empat langkah yaitu: *plan*, *action*, *observe*, dan *reflect*[6]. *Plan* mencakup kuliah penjelasan teori Manajemen Resiko dan penjelasan tugas studi kasus. *Action* meliputi pembuatan makalah oleh mahasiswa dan mempresentasikannya di depan kelas disertai dengan diskusi. *Observe* meliputi penilaian oleh dosen terhadap presentasi dan diskusi yang dilakukan oleh mahasiswa. *Reflect* meliputi pembandingan hasil yang diperoleh dalam metode pengajaran ini dibandingkan dengan pengajaran tanpa studi kasus.

Kompetensi yang diharapkan akan dicapai oleh mahasiswa adalah pertama mahasiswa mengerti teori Manajemen Resiko, kemudian dengan adanya studi kasus diharapkan mahasiswa memiliki pengalaman menerapkan teori dalam suatu kasus. Mahasiswa mengerti dan mempraktekkan proses *Risk Assessment* dan *Risk Mitigation*.

2. MENGENAL MANAJEMEN RESIKO

Proses manajemen resiko terdiri dari paling sedikit dua proses kegiatan yaitu Penilaian Resiko (*Risk Assessment*) dan Mitigasi Resiko (*Risk Mitigation*). Kedua proses ini saling ketergantungan dan saling melengkapi demi tercapainya tujuan yaitu memperkecil resiko.

2.1 Penilaian Resiko (*Risk Assessment*)

Proses pertama dalam Manajemen Resiko adalah Penilaian Resiko[1]. Disini dipelajari komponen-komponen yang penting untuk merumuskan suatu resiko, antara lain : karakteristik sistem, ancaman (*threat*), *vulnerability*, *control*, *likelihood*, dan *impact*. Komponen-komponen itu diperlukan untuk memperkirakan besarnya resiko yang dinyatakan dalam level resiko. Untuk mengatasi resiko ini perlu dipasang pengaman atau *control*.

Sistem yang dimaksud dalam karakteristik sistem adalah sistem teknologi informasi yang dinilai resikonya. Ini meliputi baik *hardware*, *software*, maupun lingkungannya. Karakteristik sistem dalam keadaan normal perlu diketahui terlebih dahulu sebagai nilai rujukan atau faktor pembanding, supaya jika terjadi penyimpangan performansi dapat segera diketahui.

Ancaman yang mungkin mengganggu sistem secara garis besar dapat berasal dari tiga sumber yaitu: alam, manusia, dan lingkungan. Gangguan alam misalnya banjir, gempa bumi, tanah longsor dan lain sebagainya. Gangguan dari manusia dapat berupa kejadian yang dapat merusak sistem sebagai akibat dari perbuatan yang disengaja maupun tidak disengaja. Gangguan dari lingkungan dapat berupa padamnya aliran listrik untuk jangka waktu yang lama, atau bisa juga polusi udara atau polusi radio aktif dan lain sebagainya.

Vulnerability adalah kerentanan atau kelemahan sistem, baik dari sisi desain sistem atau implementasinya maupun dari sisi prosedur operasional atau kontrol-internalnya. Kelemahan sistem ini dapat dimanfaatkan oleh sumber ancaman untuk masuk menerobos ke dalam sistem secara tidak sah dan mengganggu sistem.

Control adalah pengaman yang melindungi sistem dari ancaman. Selain itu *control* juga berfungsi sebagai solusi dari *vulnerability* yang ada. Metoda *control* yang dapat digunakan dapat dikelompokkan sebagai *technical control*, *management control*, maupun *operational control*.

Impact adalah akibat dari terjadinya gangguan terhadap sistem. Atau dari sudut pandang manajemen resiko dapat dikatakan sebagai akibat dari resiko yang benar-benar terjadi. *Impact* ini dapat juga dipandang sebagai hilangnya atau terganggunya integritas sistem atau data (*system or data integrity*), terganggunya kesiapan sistem (*systemavailability*), dan bocornya kerahasiaan sistem dan data (*system and data confidentiality*).

Semua komponen resiko tersebut diatas digunakan untuk memperkirakan besarnya resiko yang mungkin dihadapi oleh suatu sistem. Besaran resiko ini dikenal dengan sebutan level resiko.

Dalam Manajemen Resiko, menjadi tugas tim Penilaian Resiko untuk merekomendasikan pengaman atau *control*. Untuk setiap resiko yang ditemukan, perlu direkomendasikan lebih dari satu *control*. Hal ini perlu dilakukan untuk memberi keleluasaan kepada Manajemen Pengambil Keputusan untuk memilih *control* mana yang akan digunakan untuk mengatasi atau mengurangi resiko. Rekomendasi ini dibuat secara utuh berupa Laporan Penilaian Resiko untuk diserahkan kepada Manajemen yang berkepentingan.

2.2 Mitigasi Resiko (*Risk Mitigation*)

Mitigasi Resiko adalah proses kedua dalam Manajemen Resiko[1]. Proses ini menindaklanjuti data, temuan, dan rekomendasi dari proses Penilaian Resiko. Secara garis besar mitigasi resiko terdiri dari : proses penyusunan prioritas resiko, pemilihan *control* yang sesuai, dan pengimplementasian *control*.

Penyusunan prioritas resiko dimaksudkan untuk mengetahui urutan resiko yang mungkin akan mengganggu sistem mulai dari yang paling besar sampai dengan yang paling kecil. Resiko paling besar wajib diatasi terlebih dahulu sebelum mengatasi resiko yang lebih kecil.

Tidak semua *control* yang diusulkan untuk dipasang sesuai dengan kebutuhan yang sebenarnya, oleh karena itu perlu dipilih *control* yang benar-benar sesuai kebutuhan dan yang terjangkau harganya.

Setelah diperoleh *control* yang tepat, proses berikutnya adalah mengimplementasikannya dengan terlebih dahulu membuat *planning* yang dituangkan dalam *safeguard implementation plan*[1].

3. STUDI KASUS 1: PENILAIAN RESIKO (*Risk Assessment*)

Studi kasus dilakukan dua kali dalam satu semester, masing-masing mengambil waktu 25% dari keseluruhan pertemuan dalam matakuliah Manajemen Resiko, sehingga dengan sendirinya teori Manajemen Resiko disampaikan dalam waktu 50% dari keseluruhan pertemuan matakuliah ini.

Dalam studi kasus yang pertama ini, mahasiswa diminta untuk membuat penilaian resiko terhadap beberapa sistem teknologi informasi. Satu kelas dibagi dalam beberapa kelompok, satu kelompok beranggotakan 3 atau 4 mahasiswa. Setiap kelompok membuat penilaian resiko terhadap satu sistem teknologi informasi. Sistem yang dikaji misalnya: *e-commerce*, *e-government*, *e-auction*, *e-learning*, sistem komputerisasi data rekam medis di rumah sakit[3], dll.

Dalam studi kasus ini penilaian resiko dibuat secara studi literatur. Data bisa diperoleh dari Internet atau boleh juga diperoleh dari instansi terkait. Mahasiswa mengumpulkan data selengkap mungkin baik *hardware*, *software*, maupun informasi yang lain. Keluaran (*Output*) studi kasus ini berupa simulasi Laporan Penilaian Resiko untuk dipresentasikan di depan kelas. Dalam dunia nyata Laporan Penilaian Resiko ini untuk diserahkan kepada Pimpinan atau Manajemen yang berwenang untuk menindak-lanjutinya.

Simulasi Laporan ini berisi antara lain: pendekatan penilaian resiko, karakteristik sistem, kemungkinan ancaman dan sumbernya, *vulnerability*, *control* yang sudah terpasang (*existing control*), diskusi dan evaluasi tentang *likelihood*, diskusi dan evaluasi tentang *impact*, peringkat resiko yang didasarkan pada matriks level resiko, dan rekomendasi *control* untuk mengurangi resiko.

Berdasarkan data yang diperoleh, mahasiswa mendefinisikan karakteristik sistem yang dapat berupa : *flow chart* proses yang terjadi dalam sistem, *input output* sistem, dan performansi sistem. Informasi ini perlu untuk mengetahui bagaimana seharusnya sistem bekerja.

Demikian juga komponen lain dari penilaian resiko ini dijabarkan dengan rinci di simulasi Laporan. Dengan demikian diharapkan mahasiswa dapat merasakan secara langsung bagaimana melakukan suatu penilaian resiko.

Simulasi Laporan ini diakhiri dengan resume atau kesimpulan dimana di dalamnya direkomendasikan alternatif-alternatif *control* untuk tiap-tiap resiko yang ditemui.

Keseluruhan hasil simulasi Laporan penilaian resiko ini akan digunakan sebagai masukan (*input*) untuk studi kasus kedua, yaitu tentang mitigasi resiko yang disampaikan dalam bentuk tabel rencana pengimplementasian pengaman (*safeguard implementation plan table*).

4. STUDI KASUS 2: MITIGASI RESIKO (*Risk Mitigation*)

Sasaran studi kasus yang kedua ini adalah mengajak mahasiswa untuk memahami mitigasi resiko dengan bantuan tabel *safeguard implementation plan*[1]. Contoh tabel ini adalah seperti yang tertera di bawah ini :

Tabel 1. *Safeguard Implementation Plan Table*

(1) Resiko	(2) Level Resiko	(3) Rekomendasi *Control*	(4) Prioritas	(5) *Control* yang dipilih	(6) Prasarana yang diperlukan	(7) Tim	(8) Waktu	(9) Komentar

(1) Resiko adalah *output* dari proses penilaian resiko. Semua resiko yang sudah disampaikan di Laporan di tulis di kolom ini.
(2) Level Resiko adalah *output* dari proses penilaian resiko untuk tiap-tiap resiko.
(3) Rekomendasi *Control* adalah *output* dari proses penilaian resiko. Diharapkan untuk tiap-tiap resiko direkomendasikan lebih dari satu *control* sebagai alternatif solusi.
(4) Prioritas ditentukan berdasarkan level resiko dan prasarana yang tersedia, baik tenaga ahli, dana, maupun teknologi.
(5) *Control* dipilih dari rekomendasi *control* hasil proses penilaian resiko. Bisa dipilih lebih dari satu.
(6) Prasarana yang diperlukan untuk mengimplementasikan *control* yang dipilih.

(7) Tim adalah daftar orang yang ditunjuk untuk mengimplementasikan *control*
(8) Waktu adalah tanggal dimulai dan diakhirinya pengimplementasian *control*
(9) Komentar adalah catatan yang diperlukan untuk melengkapi informasi.

Mahasiswa diharapkan dapat mengisi tabel ini berdasarkan hasil Laporan penilaian resiko terdahulu (studi kasus yang sebelumnya). Dengan demikian semakin lengkap pemahaman mahasiswa tentang mitigasi resiko beserta persiapannya.

5. PRESENTASI DAN DISKUSI

Presentasi sangat baik dilaksanakan karena dengan presentasi ini mahasiswa dipacu untuk memahami secara utuh tulisannya sendiri tentang manajemen resiko dan disajikan di depan publik. Presentasi ini juga bermanfaat bagi peserta lain karena akan mendapatkan pemahaman baru tentang penerapan manajemen resiko di bidang-bidang tertentu. Diskusi sangat perlu dalam presentasi ini untuk pendalaman pemahaman permasalahan[5] dan alternatif solusinya.

Dalam presentasi yang pertama, yaitu tentang simulasi penilaian resiko, pendengar (*audience*) berperan sebagai pimpinan yang mencermati isi Laporan Penilaian Resiko yang dipresentasikan. Diskusi dimaksudkan untuk memperjelas isi Laporan dan menguji seberapa bahayanya resiko yang ditemukan dan seberapa penting dan perlunya penambahan *control* yang direkomendasikan.

Dalam studi kasus 1, hal-hal yang dinilai adalah kemampuan mahasiswa menerapkan teori Manajemen Resiko dalam kasus yang ditugaskan, termasuk diantaranya adalah adanya rekomendasi *control* terhadap resiko yang dihadapi di studi kasus 1. Juga dinilai kemampuan mahasiswa dalam menjawab pertanyaan dalam diskusi.

Dalam presentasi yang kedua, yaitu tentang simulasi mitigasi resiko dengan bantuan *safeguard implementation plan*, pendengar (*audience*) berperan sebagai pemilik proyek yang menjustifikasi rencana implementasi yang dibuat oleh tim manajemen resiko.

Dalam studi kasus 2, hal-hal yang dinilai adalah kemampuan mahasiswa menganalisis alternatif *control* yang direkomendasikan di studi kasus 1. Juga kemampuan mahasiswa dalam menjawab pertanyaan dalam diskusi.

Dengan memperhatikan presentasi dan diskusi yang terjadi, dosen dapat melakukan penilaian baik untuk pemakalah (*presenter*) maupun juga untuk *audience* yang aktif yaitu yang bertanya atau memberikan pendapat ataupun komentar. Terhadap *presenter* juga dapat dilakukan penilaian saat dia presentasi atau menjawab pertanyaan yang diajukan oleh *audience*. Komponen penilaian untuk mahasiswa ada dua yaitu nilai makalah yang dibuat dan nilai presentasi dan diskusi.

6. CONTOH HASIL PENILAIAN TERHADAP MAHASISWA

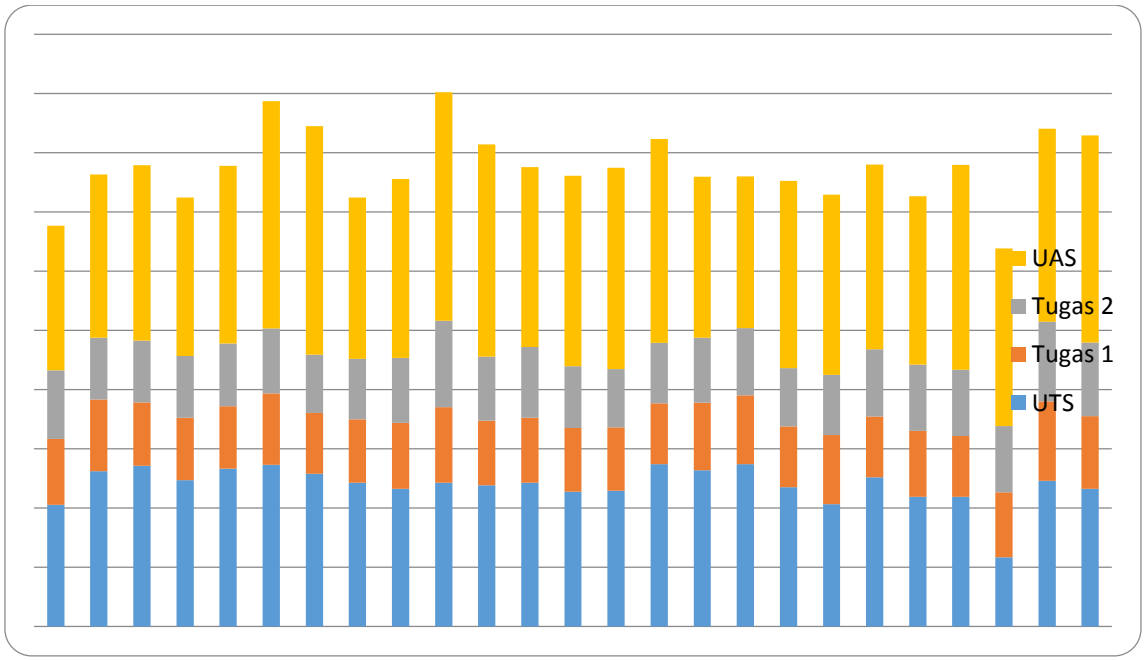
Berikut ini disajikan contoh penilaian terhadap mahasiswa yang dilakukan pada semester satu 2013 di Bandung. Contoh penilaian ini menggunakan metoda yang sama dengan yang dijelaskan di atas, yaitu menggunakan dua kali tugas presentasi dan diskusi, tetapi materinya sedikit berbeda.

UTS adalah Ujian Tengah Semester dengan nilai maksimum 30 karena bobot UTS terhadap nilai keseluruhan adalah 30%.

Tugas 1 adalah tugas presentasi dan diskusi tentang *Security*[4] dengan nilai maksimum 15 karena bobot tugas 1 terhadap nilai keseluruhan adalah 15%.

Tugas 2 adalah tugas presentasi dan diskusi tentang Penilaian Resiko (*Risk Assessment*) dengan nilai maksimum 15 karena bobot tugas 2 terhadap nilai keseluruhan adalah 15%.

UAS adalah Ujian Akhir Semester dengan nilai maksimum 40 karena bobot UAS terhadap nilai keseluruhan adalah 40%.



Gambar 1. Hasil Penilaian Akhir terhadap mahasiswa

Sumbu horizontal adalah mahasiswa, dan sumbu vertikal adalah nilai yang dicapai oleh mahasiswa tersebut. Tampak dari gambar di atas bahwa kedua presentasi dan diskusi dari tugas 1 dan tugas 2 berjalan dengan baik dan menghasilkan nilai rata-rata lebih dari 60%. Ini menunjukkan bahwa metoda presentasi dan diskusi ini cukup efektif. Terlihat juga satu orang mahasiswa dengan nilai UTS sangat rendah, setelah melakukan presentasi dan diskusi dari tugas 1 dan tugas 2 memperoleh hasil UAS yang cukup bagus. Demikian pula hasil akhir penilaian keseluruhan cukup baik yaitu rata-rata di atas 70% bahkan ada beberapa yang di atas 80% dari nilai maksimum 100%.

7. KESIMPULAN DAN SARAN

7.1 Kesimpulan

a. Mengajarkan teori manajemen resiko teknologi informasi di perguruan tinggi sangat perlu sebagai titik awal pengetahuan tentang manajemen resiko bagi mahasiswa.
b. Dalam teori ini mahasiswa dikenalkan tentang konsep penilaian resiko (*risk assessment*) dan mitigasi resiko (*risk mitigation*).
c. Mengajarkan manajemen resiko teknologi informasi di perguruan tinggi tidak cukup hanya tentang teori saja, tetapi perlu dilengkapi dengan latihan studi kasus baik dalam hal penilaian resiko (*risk assessment*) maupun mitigasi resiko (*risk mitigation*).
d. Latihan studi kasus ini dilanjutkan dengan presentasi dan diskusi untuk memperdalam pemahaman dan untuk penilaian.
e. Metoda ini berhasil baik dalam pengajaran manajemen resiko kepada mahasiswa, terlihat dari nilai akhir yang cukup tinggi yang berhasil dicapai oleh mahasiswa.

7.2 Saran

Untuk memperoleh hasil yang maksimal dari pengajaran manajemen resiko di perguruan tinggi dengan menggunakan metoda ini perlu disediakan SKS (Sistem Kredit Semester) yang cukup untuk mata kuliah Manajemen Resiko, misal 4 SKS atau lebih.

8. DAFTAR RUJUKAN

[1] Stoneburner, G., Goguen, A., Feringa, A., 2002. *Risk Management Guide for Information Technology System*. Falls Church: National Institute of Standards and Technology.

[2] Moertini, V.S., 2012. Managing Risks at the Project Initiation Stage of Large IS Development for HEI: A Case Study in Indonesia. *The Electronic Journal on Information Systems in Developing Countries*, 51 (7), pp.1-23.

[3] Walsh, T., 2011. *Health Information Security Risk Analysis Handbook For Kansas Hospitals and Health Care Providers*. Tom Walsh Consulting, LLC.

[4] Swanson, M., Guttman, B., 1996. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. National Institute of Standards and Technology.

[5] Faldo Maldini's Blog, 2010. *Diskusi dan Pentingnya Pemahaman* Available at: http://faldomaldini.wordpress.com/2010/05/28/diskusi-dan-pentingnya-pemahaman/ [Accessed 3 Agustus 2013]

[6] O'Brien, R., 1998. *An Overview of the Methodological Approach of Action Research* Available at: http://www.web.net/robrien/papers/arfinal.html [Accessed 6 September 2013