COMPETITIVE, Vol. 9, No.1, Juni 2014
ISSN: 0216-2539

Penilaian Risiko Aset Teknologi Informasi Menggunakan ISO 31000:2009 dan ISO/IEC 27001:2005 Studi Kasus : Politeknik Pos Indonesia (Poltekpos)

Roni Haabibi [1], Ai Rosita [2]
Politeknik Pos Indonesia Bandung, Jalan Sariasih No.54 Bandung, Indonesia
rony@poltekpos.ac.id, airosita@poltekpos.ac.id

Abstrak

Risiko merupakan kemungkinan terjadinya keadaan dengan dampak yang merugikan bagi perusahaan, SIM-Poltekpos merupakan aset penting yang dimiliki oleh Poltekpos yang bertugas memberikan layanan Teknologi Informasi (TI) dan terdapat beberapa permasalahan yang terjadi, terutama terkait dengan risiko terhadap aset TI (hardware, software, sistem informasi dan manusia). Kajian tersebut akan menjadi input untuk melakukan penilaian risiko dengan acuan kerangka kerja ISO 31000 dan identifikasi risiko dengan acuan ISO/IEC 27001:2005. Hasil kajian ini berupa model penilaian risiko secara komprehensif. Tahapan kegiatan penilaian risiko tersebut adalah mengidentifikasi dan mengukur setiap dampak potensi risiko pada aset TI, menilai besaran risiko dan penanganan risiko. Dari model penilaian risiko diketahui risiko yang termasuk kategori rendah, menengah dan kritis, sehingga dapat menentukan prioritas untuk penanganan risiko.

Kata kunci: ISO 31000, ISO/IEC 27001:2005, Model Penilaian Risiko, Penilaian Risiko, SIM-Poltekpos

Abstract

Risk is the possibility of a state with an adverse impact on a company/institution.SIM-Poltekpos is an important asset owned by Poltekpos in charge of service Information Technology (IT) and there are some problems that occur, primarily related to the risks to IT assets (hardware , software, information systems and human).
The review will be an input to perform a risk assessment with the ISO 31000 framework and identification of risk with the ISO / IEC 27001:2005.
The results of this study in the form of a comprehensive risk assessment models. Stages of the risk assessment is to identify and quantify any potential impact on the risk of IT assets, assessing the amount of risk and risk management. Of the risk assessment model known risk is low category, medium and critically, so as to set priorities for risk management.

Keywords*: ISO 31000, ISO/IEC 27001:2005, Risk Assessment Model, Risk Assessment, SIM-Poltekpos*

1. Pendahuluan

Pemanfaatan teknologi informasi (TI) saat ini menjadi suatu kebutuhan yang hampir tidak bisa dilepas dari aktivitas sehari-hari, baik itu kebutuhan personal maupun kebutuhan bagi organisasi atau perusahaan. Institusi Perguruan Tinggi (PT) merupakan sebuah institusi yang memiliki tugas memberikan layanan kepada mahasiswa dan masyarakat untuk menyiapkan

Sumber Daya Manusia (SDM) yang berkualitas, berdaya saing tinggi serta berdaya guna. Penggunaan TI PT merupakan upaya yang sudah seharusnya dilakukan.

Di samping akan kebutuhan TI, PT juga menghadapi beragam risiko yang dapat mempengaruhi secara positif ataupun negatif terhadap pencapaian tujuannya. Risiko yang timbul adalah risiko keamanan terhadap aset TI (hardware, software, sistem informasi dan manusia), dimana aset TI menjadi suatu yang penting yang harus tetap tersedia, dapat digunakan serta selalu terjaga keberadaannya dari pihak yang tidak berwenang yang akan menggunakannya untuk kepentingan tertentu atau akan merusak informasi tersebut. TI merupakan sebuah aset penting bagi organisasi yang perlu dilindungi oleh perusahaan dan organisasinya.[2]. Keamanan aset TI tidak hanya berdasarkan pada *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi untuk menentukan secara tepat solusi yang dapat menangani permasalahan tersebut.

Untuk meminimalisasi risiko tersebut di atas, maka diperlukan penilaian risiko sebagai langkah awal dalam melakukan manajemen risiko. Penilaian risiko ini perlu dilakukan secara komprehensif sehingga kemungkinan terjadinya risiko dapat diketahui.

Pada penelitian ini ditujukan untuk membuat model penilaian risiko aset teknologi informasi dengan menggunakan kerangka kerja ISO 31000:2009 dan untuk identifikasi nya memanfaatkan kerangka kerja ISO/IEC 27001:2005 yaitu untuk mengidentifikasi risiko dari beberapa kriteria aset TI, analisis risiko, evaluasi risiko dan penanganan risiko. Model penilaian risiko yang dirancang dalam penelitian ini akan diuji pada studi kasus di Politeknik Pos Indonesia (Poltekpos).

2. Metodologi Penelitian

Metodologi yang digunakan dalam melaksanakan penelitian ini adalah mengacu pada metodologi *design science research* sebagaimana dinyatakan oleh Peffers, dkk.[1]. Dengan mengacu pada metodologi tersebut, kegiatan yang dilakukan pada penelitian ini terbagi dalam beberapa tahapan, antara lain:

1. Identifikasi Masalah dan Motivasi
   Proses ini adalah persiapan dan perencanaan pelaksanaan penelitian.
2. Penentuan Tujuan
   Tujuan penelitian dibuat dengan mengacu pada permasalahan yang telah didefinisikan.
3. Analisis
   Proses ini dimaksudkan untuk memahami pengetahuan dasar yang sudah ada dari hasil studi pustaka dan mengidentifikasi potensi yang ada untuk kepentingan penelitian.
4. Perancangan dan Pengembangan
   Aktivitas-aktivitas dalam proses perancangan model penilaian risiko aset TI.
5. Demonstrasi
   Tahap ini bertujuan untuk melakukan penerapan model yang telah dibuat untuk melihat sejauh mana model tersebut dapat bermanfaat pada tempat studi kasus.
6. Evaluasi
   Hasil dari tahap demonstrasi dievaluasi untuk mendapatkan keterangan mengenai model yang dibuat.
7. Komunikasi
   Tahap komunikasi merupakan tahapan pembuatan laporan hasil analisis, rancangan model serta hasil pengujian model pada sebuah studi kasus.

3. Tinjauan Pustaka

1. Risiko

Risiko merupakan konsep yang digunakan untuk menyatakan perhatian tentang dampak yang mungkin terjadi atas lingkungan yang penuh dengan ketidakpastian. Setiap peristiwa yang terjadi dapat mempunyai dampak yang material atau konsekuensi yang signifikan bagi organisasi dan tujuan organisasi. Akibat yang bersifat negatif disebut dengan risiko dan akibat yang bersifat positif disebut dengan kesempatan. [6].

Risiko akan selalu ditemukan dalam kehidupan dimana apabila dikelola dengan baik dapat menjadi sebuah kesempatan dan sebaliknya, apabila manajemennya buruk maka akan menjadi

sebuah ancaman. Definisi risiko adalah suatu efek dari ketidakpastian dalam pencapaian suatu tujuan. Dan risiko juga menambahkan bahwa efek tersebut bisa bersifat negatif maupun positif.[7]

2. Aset

Aset merupakan sesuatu yang dimiliki oleh perusahaan baik itu yang terlihat atau yang tidak terlihat. Pada tataran perusahaan, aset TI dapat diartikan sesuatu yang dimiliki perusahaan yang sifatnya tidak terlihat, seperti data dan informasi. Seiring dengan perkembangan teknologi dan informasi, maka informasi merupakan aset yang paling penting dalam sebuah perusahaan. Dengan statusnya yang sangat penting, maka perlu adanya pengamanan agar informasi atau data tersebut tidak diambil atau jatuh kepada tangan bukan haknya.[2]

3. Penilaian Risiko

Penilaian risiko adalah keseluruhan proses yang meliputi identifikasi risiko, analisis risiko dan evaluasi risiko. Penilain risiko adalah suatu proses untuk:

a. Mengidentifikasi dan mengukur setiap potensi bahaya dari setiap tahapan pekerjaan yang berdampak pada aset TI.
b. Menilai besaran risiko.
c. Mengendalikan risiko atas dasar prioritas tertentu.

Sumber risiko adalah :

a. Keadaan atau tindakan yang berpotensi menciderai badan atau mengganggu kesehatan manusia.
b. Elemen yang dapat berdiri sendiri atau merupakan kombinasi yang berpotensi untuk terjadinya risiko.[4]

Menurut ISO 27001 proses penilaian dan evaluasi risiko meliputi kegiatan-kegiatan sebagai berikut: [5]

a. Menentukan kriteria aset berdasarkan data aset TI yang telah diidentifikasi.
b. Menentukan kriteria penilaian risiko yang terdiri dari kriteria dampak dan kecenderungan yang dituangkan dalam metodologi penilaian risiko.
c. Melaksanakan penilaian risiko yang terdiri dari kegiatan identifikasi, evaluasi, dan analisis risiko.
d. Menentukan rencana penanganan risiko sebagai bagian dari proses penerapan aset TI dan meminimasi dampak dari risiko tersebut.

Penilaian risiko merupakan proses untuk menilai seberapa sering risiko terjadi atau seberapa besar dampak dari risiko. Dampak risiko terhadap bisnis dapat berupa: dampak terhadap finansial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data) dan penundaan proses pengambilan keputusan. Sedangkan kecenderungan terjadinya risiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya.[2].

4. Hasil dan Pembahasan

Aktivitas-aktivitas dalam proses perancangan model penilaian risiko aset TI ini adalah sebagai berikut :

a. Menentukan komponen pemodelan.
b. Merancang metoda keterkaitan identifikasi risiko aset TI.
c. Merancang langkah identifikasi aset TI
d. Merancang metode penilaian risiko aset TI.

1. Keterkaitan ISO 31000:2009, ISO 27001:2005

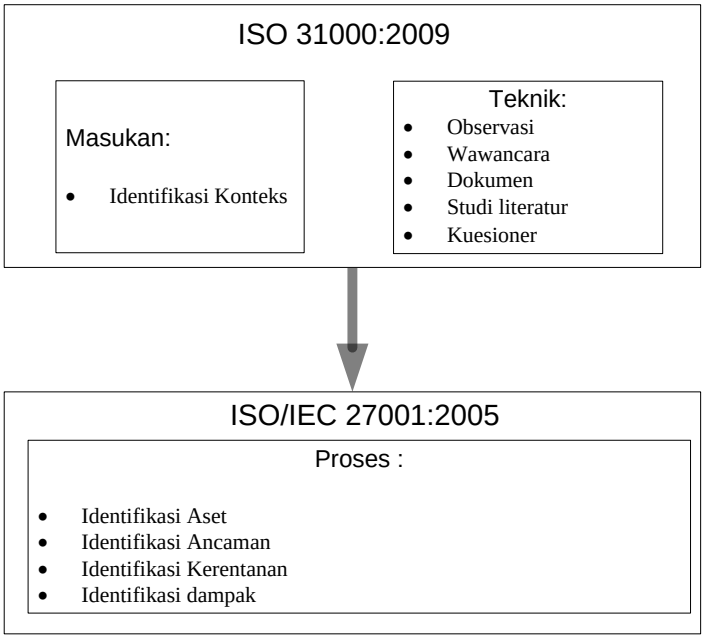
Panduan manajemen risiko ISO 31000:2009 menjelaskan masukan dan teknik dari identifikasi risiko, namun belum dapat menjelaskan proses identifikasi risiko itu sendiri. Oleh karena itu dibutuhkan standar lain yang dapat menjelaskan bagaimana proses identifikasi risiko yang komprehensif yaitu dengan menggunakan kerangka ISO/IEC 27001:2005.

Berikut ini adalah proses identifikasi risiko berdasarkan ISO/IEC 27001:2005 :

1. Identifikasi aset-aset teknologi informasi yang dimiliki oleh organisasi.
2. Identifikasi ancaman pada setiap aset-aset teknologi informasi tersebut.
3. Identifikasi kerentanan yang diakibatkan oleh ancaman.

4. Identifikasi frekuensi dan dampak.

Keterkaitan untuk identifikasi risiko menggunakan ISO 31000:2009 dan ISO 27001 seperti gambar 1 adalah hubungan kedua standar tersebut dengan tempat studi kasus.



Gambar 1 Keterkaitan Identifikasi Risiko.[3]

Penjelasan gambar 1 adalah sebagai berikut:

a. Masukan identifikasi dalam indentifikasi risiko SIM-Poltekpos adalah proses bisnis SIM-Poltekpos itu sendiri, yaitu terkait layanan yang diberikan.
b. Teknik identifikasi yang digunakan untuk menggali proses bisnis SIM-Poltekpos adalah dengan melakukan wawancara, observasi, dokumen pendukung dan brainstorming.
c. Proses identifikasi risiko mengadaptasi ISO 27001.

2. Langkah Identifikasi Risiko

Berikut adalah langkah identifikasi risiko aset TI SIM-Poltekpos.

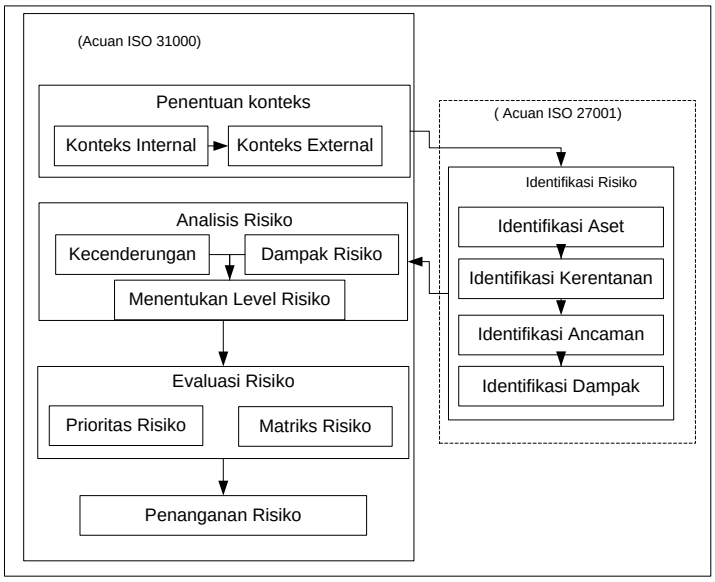
a. Studi literatur dilakukan untuk menjawab permasalahan yang pertama, yaitu terkait bagaimana melakukan identifikasi risiko berdasarkan ISO/IEC 27001:2005. Keluaran dari studi literatur ini adalah penjelasan aktivitas-aktivitas yang dilakukan untuk identifikasi risiko.
b. Identifikasi aset SIM-Poltekpos berikutnya adalah mengidentifikasi aset-aset TI yang dimiliki oleh SIM-Poltekpos berdasarkan komponen sistem informasi, yaitu: data, perangkat lunak, perangkat keras, sumber daya manusia, dan prosedur. Keluaran dari tahap ini adalah daftar aset TI yang dimiliki SIM-Poltekpos.
c. Identifikasi ancaman SIM-Poltekpos masing-masing aset yang telah teridentifikasi sebelumnya diidentifikasi ancamannya pada tahap ini. Sehingga keluarannya adalah berupa ancaman-ancaman dari internal dan eksternal organisasi SIM-Poltekpos.
d. Identifikasi kerentanan SIM-Poltekpos memiliki dampak terhadap kerentanan. Identifikasi kerentanan pada setiap ancaman tersebut akan diidentifikasi pada tahap ini, sehingga keluarannya adalah daftar kerentanan aset TI SIM-Poltekpos.
e. Identifikasi dampak kerentanan SIM-Poltekpos yang ada memiliki dampak terhadap layanan yang diberikan oleh SIM-Poltekpos kepada civitas akademika. Dampak-dampak tersebut akan diidentifikasi pada tahap ini, sehingga keluarannya adalah daftar dampak kerentanan terhadap layanan SIM-Poltekpos.

3. Model Penilaian Risiko

ISO 31000 memberikan prinsip-prinsip dan pedoman generik pada manajemen risiko. Pembuatan model ini diperoleh berdasarkan dari hasil identifikasi risiko aset TI. Model ini berfungsi sebagai acuan penilaian risiko aset TI dan sebagai acuan penanganan risiko aset TI untuk memastikan keberlangsungan kegiatan di Poltekpos. Selain itu, model ini digunakan sebagai bahan pertimbangan pada pembuatan *feasibility study* mengenai faktor risiko aset TI yang terjadi saat implementasi. Dengan penilaian risiko aset TI yang baik, maka kerugian yang dapat ditimbulkan dapan ditekan seminimal mungkin.[4]. Berikut ini adalah beberapa hal yang ingin dihasilkan dari model penilaian risiko aset TI untuk Poltekpos yang akan dirancang:

a. Model penilaian risiko aset TI dirancang dengan memanfaatkan kerangka kerja ISO 31000:2009.
b. Model penilaian risiko ini dirancang untuk mengidentifikasi dan menangani ancaman-ancaman terhadap aset TI dengan memanfaatkan kerangka kerja ISO/IEC 27001:2005.
c. Model penilaian risiko ini harus memenuhi kriteria pemilihan tindakan risiko dengan memaksimalkan aset TI yang telah ada.
d. Model penilaian risiko ini terdokumentasi dengan baik dan mudah dipahami.
e. Model penilaian risiko ini mudah direvisi dan disesuaikan dengan perubahan yang akan dan mungkin terjadi.

Gambar 2 adalah model penilaian risiko aset TI Poltekpos.



Gambar 2 Model Penilaian Risiko Aset TI

Posisi TI pada SIM-Poltekpos adalah sebagai *enabler* operasional (transaksi) layanan TI. TI digunakan untuk menciptakan nilai agar meningkatkan pelayanan dan kepuasan terhadap pengguna. Penjelasan dari gambar 2 adalah sebagai berikut:

1. Penentuan Konteks Eksternal

Penentuan konteks eksternal perlu dilakukan untuk memastikan sasaran dan kepentingan stakeholder eksternal organisasi dipertimbangkan ketika melakukan penilaian terhadap risiko aset TI. Beberapa konteks eksternal di SIM-Poltekpos adalah sebagai berikut:

a. Prosedur penggunaan perangkat komputer.
b. Prosedur peminjaman perangkat TI.
c. Prosedur backup data.
d. Prosedur penanganan masalah.

Kebijakan dan prosedur tersebut mencakup keseluruhan operasi komputer yang ada dilingkungan Poltekpos. Belum terdapat prosedur khusus yang membahas tentang pengelolaan risiko aset TI. Prosedur dan kebijakan tertulis terkait operasi komputer yang ada adalah prosedur penggunaan perangkat komputer pada laboratorium komputer. Prosedur penanganan permasalahan dan prosedur data *backup* dan *restore.*

2. Penentuan Konteks Internal

Proses pengelolaan risiko harus selaras dengan budaya, proses bisnis, struktur serta strategi organisasi dalam mencapai tujuannya. Konteks internal berpengaruh langsung terhadap cara organisasi dalam penilaian terhadap risiko aset TI.

3. Identifikasi Aset TI SIM-Poltekpos

Tabel 1 merupakan daftar risiko aset TI.

Tabel 1 Daftar Aset T SIM-Poltekpos

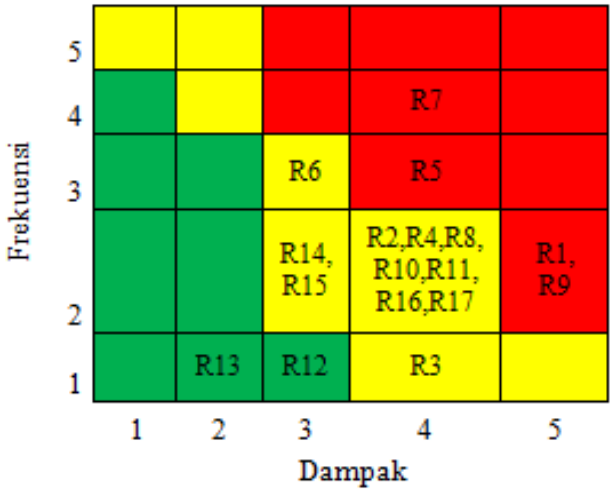
Aset TI	**Aset SIM-Poltekpos**
Data	1. Data tugas mahasiswa 2. Data Nilai
Perangkat Lunak	3. Website Poltekpos 4. Website PMB 5. Elearning 6. Installer aplikasi 7. Sistem Informasi Akademik
Perangkat Keras	8. Personal Computer (PC) 9. LAN Connector 10. Server 11. Kabel jaringan 12. Wi fi 13. Router 14. Switch 15. Access point 16. Finger print 17. Topologi jaringan
Sumberdaya Manusia	18. Kepala Unit SIM 19. Koordinator SIM-Poltekpos 20. Administrator 21. Operator 22. Maintenance
Prosedur	23. Tata kelola server

4. Analisis Aset TI

Hasil analisis risiko aset TI tercantum dalam tabel 2. Dari hasil analisis tersebut diketahui bahwa tingkat risiko frekuensi tertinggi 4 (empat) dan tingkat risiko terendah adalah 1 (satu) serta dampak tertinggi 5 (lima) dan dampak terendah 2 (dua) .

5. Evaluasi Risiko

Evaluasi risiko dilakukan dengan memetakan hasil penilaian terhadap matriks penilaian risiko. Dari hasil evaluasi risiko tersebut diketahui 2 (dua) risiko kategori *low*, 11 (sebelas) kategori *medium* dan 4 (empat) risiko kategori *high* atau kritis. Hasil evaluasi terlihat pada gambar 4 dan rincian penjelasan terdapat pada tabel 2. Dari penjelasan tabel 2 yang termasuk risiko-risiko high atau kritis tersebut selanjutnya diberikan prioritas untuk dilakukan penanganan terlebih dahulu.



Gambar 2 Matriks Penilaian Risiko Aset TI

Tabel 2 Hasil Penilaian Risiko Aset TI

Aset IT	Id	Risiko	Frekuensi	Dampak	Tingkat Ririsko
Data	R1	Hilangnya data	2	5	High
	R2	Database rusak/error	2	4	Medium
	R3	Penyalahgunaan/pencurian data	1	4	Medium
Perangkat lunak	R4	Peretasan Aplikasi	2	4	Medium
	R5	Aplikasi crash (down)	3	4	High
	R6	Aplikasi diserang virus	3	3	Medium
	R7	Lemahnya maintenance aplikasi	4	4	High
Perangkat keras	R8	Kerusakan hardware	2	4	Medium
	R9	Server diserang virus	2	5	High
	R10	Koneksi jaringan putus/rusak	2	4	Medium
	R11	Kegagalan sistem operasi	2	4	Medium
	R12	Bencana Alam	1	3	Low
Sumber daya manusia	R13	Penyalahgunaan kedudukan	1	2	Low
	R14	Melemahnya loyalitas SDM	2	3	Medium
	R15	Pembeberan data dan informasi rahasia	2	3	Medium
Prosedur	R16	Internet tidak dapat diakses	2	4	Medium
	R17	Menghambat proses perkuliahan	2	4	Medium

Keterangan :

L : Risiko rendah

M : Risiko sedang

H : Risiko tinggi

5. Kesimpulan

Model penilaian risiko dalam penelitian ini telah berhasil dilaksanakan dan sesuai dengan kebutuhan proses bisnis dengan mengukur tingkat risiko berdasarkan dampak dan kecenderungan, dari hasil penelitian dihasilkan bahwa risiko dengan kategori rendah terdapat 2 (dua), untuk kategori menengah terdapat 11 (sebelas) dan terdapat 4 (dua) risiko yang termasuk kategori tinggi atau kritis.

Pengujian model penilaian risiko ISO 31000 di SIM-Poltekpos berhasil dan sesuai dengan kondisi studi kasus.

Referensi

[1] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). *A Design Science Research Methodology for Information System Research*. Journal of Management Information Systems, 45-78.
[2] Purdi, G., ISO 31000:2009. (2010) *Setting a New Standar for Risk Assessment*, Risk Analysis, 30,6.
[3] M. Bachtyar Rosyadi, "Identifikasi Resiko is net Berdasarkan iso/iec 31000:2009 dan iso/iec 27001," 2012.
[4] AS/NZS ISO 31000, *Risk Management – Principles and Guidelines*, 1st ed. New Zealand: International Standard, 2009.
[5] ISO/IEC 27001-2005 (2005): *Information standard - Information technology - Security techniques - Information security management systems - Requirements*, Switzerland.
[6] Harold, P. (2010). *Risk Management Guideline.* Panorama Resource.
[7] W, K., & AM, K. (2009). *ISO 31000:2009;ISO/IEC 31010 & ISO Guide 73:2009 International Standards for the Management of Risk.* NUNDAH Qld 4012, Australia.