MODEL PENILAIAN RISIKO ASET TEKNOLOGI INFORMASI MENGGUNAKAN ISO 31000 DAN ISO/IEC 27001. STUDI KASUS : POLITEKNIK POS INDONESIA (POLTEKPOS)

Roni Habibi [1], Indra Firmansyah [2]

[1] Teknik Informatika Politeknik Pos Indonesia Bandung
[2]Akuntansi Keuangan Politeknik Pos Indonesia Bandung
Jl Sariasih No 54 Bandung, 40151
Email : roni.habibi@poltekpos.ac.id [1], indra_firmansyah@yahoo.com [2]

Abstrak

Risiko merupakan kemungkinan terjadinya keadaan dengan dampak yang merugikan bagi perusahaan, Unit 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. Hasil penelitian ini berupa model penilaian risiko yaitu dengan identifikasi konteks sampai dengan penanganan risiko. Penilaian risiko menghasilkan dampak dan frekuensi kejadian yang menggambarkan tingkat risiko yang termasuk risiko dengan kategori rendah, kategori menengah atau kategori tinggi, sehingga dapat menentukan prioritas untuk penanganan risiko dan dihasilkan bahwa risiko dengan kategori low terdapat 2 (dua), untuk kategori medium terdapat 11 (sebelas) dan terdapat 4 (empat) risiko yang termasuk kategori high atau kritis.

Kata kunci: ISO 31000, ISO/IEC 27001, Model Penilaian Risiko, Penilaian Risiko, 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 [1]. 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 dan untuk identifikasi nya memanfaatkan kerangka kerja ISO/IEC 27001 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). Penelitian ini terinisiasi dari beberapa penelitian sebelumnya yang saling terkait sebagai bahan acuan.

Dalam pengelolaan risiko arsitektur yang dirancang meliputi tiga komponen, mereka adalah prinsip-prinsip manajemen risiko TI, identifikasi risiko dan analisis IT, Pemeriksaan kerangka manajemen risiko TI dihasilkan sesuai dengan kebutuhan perusahaan yang bergerak di industri telekomunikasi dan telah mengintegrasikan risiko TI dengan ERM. Hal utama dalam pengembangan kerangka kerja manajemen risiko TI adalah adanya pengendalian internal sebagai peran kunci dalam Enterprise Risk Management.[2].

Keberhasilan imlementasi manajemen risiko terkait dengan kemampuan sebuah organisasi dalam pengelolaan terhadap risiko TI setelah implementasi proses manajemen risiko sebelumnya. [3]

Evaluasi keberhasilan terhadap manajemen risiko yang sudah dilakukan tentang kematangan kondisi ideal dari manajemen risiko. [4]

Dalam implementasi manajemen risiko disesuaikan dengan kondisi sebuah institusi dengan penggabungan

dua buah kerangka kerja pengukuran risiko enterprise risk management COSO ERM dan ISO 31000 dengan tujuan utama adalah mengetahui kekurangan dan kelebihan dari masing-masing framework yaitu dengan penekanan pada risiko bisnis, penciptaan nilai, serta pengendalian internal dan sebagai kebutuhan partikular dari struktur dan masing-masing organisasi. [5]

Perbedaan dengan penelitian terkait sebelumnya terdapat beberapa kekurangan seperti untuk mengetahui hasil penilaian risiko, evaluasi terhadap risiko-risiko asset TI, tingkat dampak dan frekuensi asset TI, tingkat risiko diurutkan berdasarkan tingkat paling tinggi sampai yang terendah, sehingga dengan mengetahui tangkat risiko tersebut akan mudah dalam penanganan terhadap risiko asset TI tersebut.

2. Metodologi Penelitian

Metodologi yang digunakan dalam melaksanakan penelitian ini adalah mengacu pada metodologi *design science research* sebagaimana dinyatakan oleh Peffers, dkk. [6]. 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. [7].

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.[8]

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.[8]

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.[8]

Menurut ISO 27001 proses penilaian dan evaluasi risiko meliputi kegiatan-kegiatan sebagai berikut: [9]

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.[9].

4. Pembahasan

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

1. Menentukan komponen pemodelan yang akan digunakan dalam model penilaian risiko penelitian telah dijabarkan pada Bab II.
2. Merancang metoda keterkaitan identifikasi risiko aset TI.
3. Merancang langkah identifikasi aset TI
4. Merancang metode penilaian risiko aset TI.

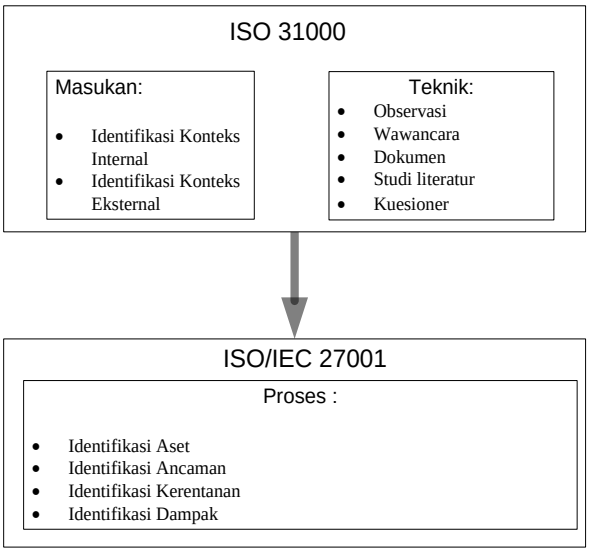
1. Keterkaitan ISO 31000 dan ISO 27001

Panduan manajemen risiko ISO 31000 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.

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

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 dan ISO 27001 seperti gambar 1 adalah hubungan kedua standar tersebut dengan tempat studi kasus.



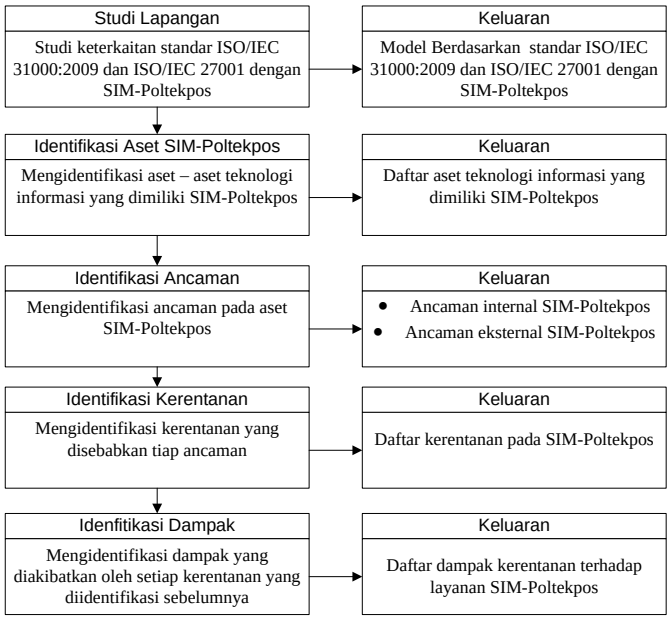
Gambar 1. *Keterkaitan identifikasi risiko. [9]*

Penjelasan gambar 1 adalah sebagai berikut:

1. Masukan identifikasi dalam indentifikasi risiko SIM-Poltekpos adalah proses bisnis SIM-Poltekpos itu sendiri, yaitu terkait layanan yang diberikan.
2. Teknik identifikasi yang digunakan untuk menggali proses bisnis SIM-Poltekpos adalah dengan melakukan:
   a. Wawancara kepada penanggung jawab SIM-Poltekpos. Untuk proses identifikasi aset TI SIM-Poltekpos yaitu untuk mengetahui risiko yang pernah muncul terhadap aset TI.
   b. Observasi adalah teknik dengan mengamati secara langsung objek data pada SIM-Poltekpos.
   c. Dokumen yang mendukung dalam identifikasi ini.
   d. *Brainstorming* dalam satu kelompok dan juga studi literatur mengenai jenis-jenis ancaman, kerentanan, serta dampaknya yang kemudian disesuaikan dengan SIM-Poltekpos.
3. Proses identifikasi risiko mengadaptasi ISO 27001.

2. Langkah Identifikasi Risiko

Gambar 2 berikut adalah langkah identifikasi risiko aset TI SIM-Poltekpos.



Gambar 2. *Langkah identifikasi risiko aset TI*

Penjelasan gambar 2 adalah sebagai berikut:

1. Studi literatur dilakukan untuk menjawab permasalahan yang pertama, yaitu terkait bagaimana melakukan identifikasi risiko berdasarkan ISO/IEC 27001. Keluaran dari

studi literatur ini adalah penjelasan aktivitas-aktivitas yang dilakukan untuk identifikasi risiko.

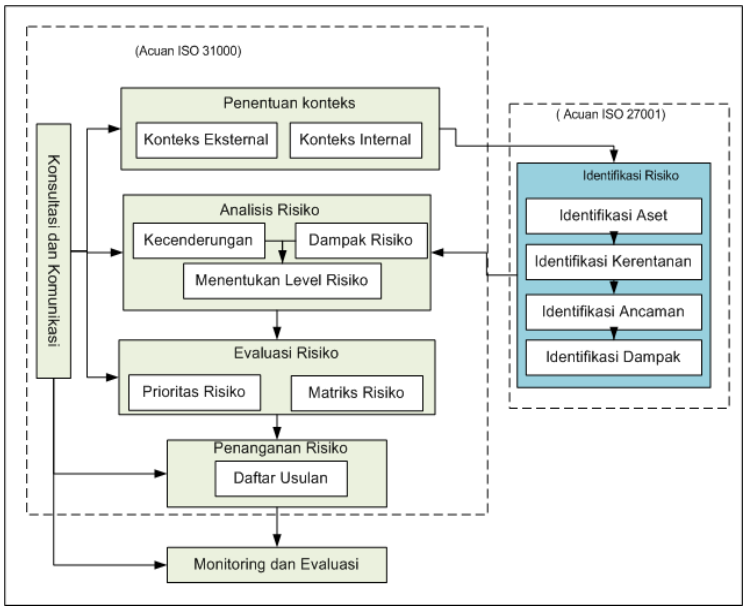
2. Identifikasi aset SIM-Poltekpos berikutnya adalah mengidentifikasi aset-aset TI yang dimiliki oleh SIM-Poltekpos berdasarkan komponen sistem informasi, yaitu: data, perangkat lunak, perangkat keras, sumber daya manusia, dan prosedur. Keluaran dari tahap ini adalah daftar aset TI yang dimiliki SIM-Poltekpos.
3. 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.
4. 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.
5. 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. Berikut ini adalah beberapa hal yang ingin dihasilkan dari model penilaian risiko aset TI untuk Poltekpos yang akan dirancang:

1. Model penilaian risiko aset TI dirancang dengan memanfaatkan kerangka kerja ISO 31000.
2. Model penilaian risiko ini dirancang untuk mengidentifikasi dan menangani ancaman-ancaman terhadap aset TI dengan memanfaatkan kerangka kerja ISO/IEC 27001.
3. Model penilaian risiko ini harus memenuhi kriteria pemilihan tindakan risiko dengan memaksimalkan aset TI yang telah ada.
4. Model penilaian risiko ini terdokumentasi dengan baik dan mudah dipahami.
5. Model penilaian risiko ini mudah direvisi dan disesuaikan dengan perubahan yang akan dan mungkin terjadi.

Gambar 3 adalah usulan model penilaian risiko aset TI yang dirancang dalam penelitian ini.



Gambar 3. *Model penilaian risiko aset TI*

Posisi TI pada SIM-Poltekpos adalah sebagai enabler operasional (transaksi) layanan tersebut. Hal ini sesuai dengan nilai TI yang telah dibahas pada bagian sebelumnya yaitu TI digunakan untuk menciptakan nilai agar meningkatkan pertumbuhan pelayanan dan kepuasan pengguna.

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:

1. Prosedur penggunaan perangkat komputer.
2. Prosedur peminjaman perangkat TI.
3. Prosedur backup data.
4. 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 TI 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

4. Analisis Aset TI

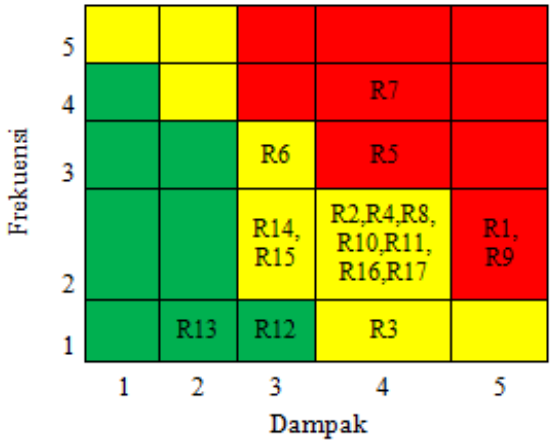
Hasil analisis risiko aset TI tercantum dalam tabel 2. Dari hasil analisis tersebut diketahui bahwa tingkat risiko frekuensi tertinggi 4 (empat) dan tingkat risiko terendah adalah 1 (satu) serta dampak tertinggi 5 (lima) dan dampak terendah 2 (dua).

Tabel 2. *Hasil Analisis Risiko Aset TI*

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

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 3. Dari penjelasan tabel 3 yang termasuk risiko-risiko *high* atau kritis tersebut selanjutnya diberikan prioritas untuk dilakukan penanganan terlebih dahulu.



Gambar 4. *Matriks penilaian risiko aset TI*

Tabel 3. *Hasil Penilaian Risiko Aset TI*

Aset IT	Id	Risiko	F	D	TR
Data	R1	Hilangnya data	2	5	H
	R2	Database rusak/error	2	4	M
	R3	Penyalahgunaan/pencurian data	1	4	M
Perangkat lunak	R4	Peretasan Aplikasi	2	4	M
	R5	Aplikasi crash (down)	3	4	H

Aset IT	Id	Risiko	F	D	TR
	R6	Aplikasi diserang virus	3	3	M
	R7	Lemahnya maintenance aplikasi	4	4	H
Perangkat keras	R8	Kerusakan hardware	2	4	M
	R9	Server diserang virus	2	5	H
	R10	Koneksi jaringan putus/rusak	2	4	M
	R11	Kegagalan sistem operasi	2	4	M
	R12	Bencana Alam	1	3	L
Sumber daya manusia	R13	Penyalahgunaan kedudukan	1	2	L
	R14	Melemahnya loyalitas SDM	2	3	M
	R15	Pembeberan data dan informasi rahasia	2	3	M
Prosedur	R16	Internet tidak dapat diakses	2	4	M
	R17	Menghambat proses perkuliahan	2	4	M

Keterangan :

F = Frekuensi
D = Dampak
TR = Tingkat risiko

L : Risiko rendah
M : Risiko sedang
H : Risiko tinggi

Tabel 4. *Hasil Pengujian Penilaian Terhadap Penilaian Risiko Aset TI*

No	Komponen Penilaian Risiko	Distribusi Jawaban	
		Nilai	Rata-rata
1	Identifikasi risiko	180	5.00
2	Kriteria pemilihan tindakan risiko	144	4.00
3	Strategi tindakan risiko	180	5.00
4	Prioritas strategi tindakan risiko	180	5.00
5	Rencana tindakan risiko	180	5.00

5. Kesimpulan

Risiko-risiko aset TI yang terjadi di Poltekpos telah berhasil diidentifikasi secara komprehensif. Dari hasil identifikasi risiko aset TI, diketahui terdapat 17 (tujuh belas) jenis risiko aset TI.
Model penilaian risiko dalam penelitian ini telah berhasil dibuat dan sesuai dengan kebutuhan studi kasus yaitu dengan mengukur tingkat risiko berdasarkan dampak dan kecenderungan, dari hasil penelitian dihasilkan bahwa risiko dengan kategori low terdapat 2 (dua), untuk kategori medium terdapat 11 (sebelas) dan terdapat 4 (empat) risiko yang termasuk kategori *high* atau kritis.
Pengujian model penilaian risiko ISO 31000 dan 27001 dan usulan penilaian risiko aset TI di SIM-Poltekpos telah berhasil sesuai dengan kondisi studi kasus. Penilaian hasil pengujian memiliki nilai terendah 144 dan nilai tertinggi 180.

Daftar Pustaka

[1] G. Purdy, "ISO 31000:2009--Setting a new standard for risk management.," *Risk Anal.*, vol. 30, no. 6, pp. 881–6, 2010.
[2] T. Ernawati, Suhardi, and D. R. Nugroho, "IT risk management framework based on ISO 31000:2009," *Syst. Eng. Technol. (ICSET), 2012 Int. Conf.* , pp. 1–8, 2012.
[3] Gery Lusanjaya (2011), Perancangan Model Penilaian Kemampuan Proses Pengelolaan Risiko Teknologi Informasi.
[4] Nazruddin Safaat Harahap (2012), Manajemen Risiko Teknologi Informasi Menggunakan ISO-31000.
[5] Marsyita Zoraya Hanindra (2012), Integrasi Model COSO dan ISO 31000 untuk Mengukur Teknologi Informasi.
[6] 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.
[7] Harold, P. (2010). Risk Management Guideline. Panorama Resource.
[8] 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.
[9] M. Bachtyar Rosyadi, "Identifikasi Resiko is net Berdasarkan iso/iec 31000:2009 dan iso/iec 27001," 2012.

Biodata Penulis

Roni Habibi, memperoleh gelar Sarjana Komputer (S.Kom), Jurusan Teknik Informatika Universitas Nasional Pasim Bandung, lulus tahun 2010. Memperoleh gelar Magister Teknik (M.T.) Program Pasca Sarjana Sekolah Teknik Elektro dan Informatika (STEI) Institut Teknologi Bandung, lulus tahun 2014. Saat ini menjadi Dosen di Politeknik Pos Indonesia Bandung.

Indra Firmansyah, memperoleh gelar Sarjana Akuntansi (S.E), Jurusan Akuntansi Universitas Padjadjaran Bandung, lulus tahun 2002. Memperoleh gelar Magister Manajemen (M.M) Program Pasca Sarjana Magister Manajemen Universitas Padjadjaran Bandung, lulus tahun 2005. Saat ini menjadi Dosen di Politeknik Pos Indonesia Bandung.