IMPLEMENTASI MANAJEMEN RISIKO SISTEM INFORMASI MENGGUNAKAN COBIT 5

Rini Astuti

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda Bandung 40132

riniastuti@likmi.ac.id

ABSTRAK

Risiko merupakan kehilangan atau kerugian yang disebabkan karena adanya kelalaian, kesalahan manusia atau mesin, gangguan lingkungan, ancaman bahkan bencana alam di suatu lingkungan. Sistem informasi yang banyak dimanfaatkan organisasi dapat dipastikan memiliki risiko. Sehingga untuk mencapai tingkat keamanan dan kenyamanan pemakaian sistem dan tekno;ogi informasi yang memadai diperlukan manajemen risiko. Bermacam kerangka kerja untuk melakukan manajemen risiko dapat dipilih, diantaranya adalah yang dikeluarkan oleh Asosiasi ISACA (*Information System Auditor and Control Association)* yaitu framework COBIT (*Control Objectives for Information and Technology*).

COBIT 5 versi tahun 2013, menyediakan proses yang terstruktur dan memisahkan kegiatan manajemen dan tata kelola ke dalam model referensi proses yang tersedia.

Penelitian ini dibuat untuk mengimplementasikan salah satu kerangka kerja manajemen risiko system informasi dari COBIT 5 pada domain APO (*Align, Plan, Organize*) 12 dengan studi kasus Sitem Informasi Perpustakaan Digital/ *Digital Library* suatu Perguruan Tinggi di Bandung.

Hasil penelitian ini dapat digunakan sebagai referensi untuk melakukan manajemen risiko dengan salah satu kerangka kerja yang tersedia.

Katakunci : resiko, manajemen risiko, sistem informasi, COBIT 5, APO 12

1. PENDAHULUAN

Sistem informasi Perpustakaan Digital secara umum sangat dibutuhkan oleh masyarakat dari berbagai bidang, terutama di bidang pendidikan. Sistem ini sangat penting bagi lingkungan kampus di era informasi ini, salah satu andalan dari sistem informasi perpustakaan digital adalah tersedianya fungsi pencarian yang lengkap, informasi yang mudah diakses, selalu tersedia dan aman. Selain dari manfaat sistem informasi yang banyak, sistem ini pun tidak luput dari berbagai risiko yang mungkin terjadi.

Salah satu aspek yang menjadi bagian penting dalam sistem informasi dan pengembangannya adalah aspek keamanandan manajemen risiko. Seiring dengan berkembangnya sistem informasi pada saatini beberapa hal penting yang menjadi faktor penentu agar sistem yang berjalandapat befungsi dengan baik dan benar, karena selain efek positif yang munculakibat berkembangnya sistem informasi maka permasalahan keamanan sistem informasi danpengelolaan sumber daya teknologi informasi juga dapat terjadi. Sebuah institusi atau lembaga yangmenggantungkan sebagian besar proses bisnisnya pada sistem informasi akanmengalami kendala yang serius ketika sistem yang diterapkan tidak berjalandengan

semestinya. Pada penelitian kali ini penulis akan melakukan sebuah kajian danstudi ilmiah tentang implementasi manajemen risiko pada implementasi sistem informasi Perpustakaan Digital di sebuah Perguruan Tinggi Swasta di Bandungmenggunakan COBIT 5 khususnya proses APO (*Align, Plan, and Organise*) 12 yang merupakan sebuah metode yang cukup popular di lingkungan auditor sistem informasi.

1.1 RUANG LIGKUP

Ruang lingkup dari manajemen resiko yang akan dilakukan adalah pedoman COBIT 5 untuk refernsi proses APO 12 tentang Mengelola Risiko yang mengidentifikasi, menilai dan mengurangi resiko sistem informasi Perpustakaan Digital dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Ruang lingkup proses manajemen risiko tersebut adalah sebagai berikut :

1. Mengumpulkan data
2. Menganalisis risiko
3. Menjaga sebuah profil risiko
4. Mengartikulasikan risiko
5. Menentukan suatu protofolio aksi manajemen risiko
6. Menanggapi risiko

1.3 TUJUAN PENELITIAN

Tujuan dilaksanakannya penilaian resiko Sistem Informasi Perpustakaan Digital di suatu Perguruan Tinggi Swasta (PTS) di Bandung adalah :

a. Memenuhi kebutuhan manajemen risiko enterprise lembaga secara luas.
b. Menginformasikan kepada pembuat keputusandan mendukung penanganan risikodengan mengidentifikasi:
   (i) Ancamanyang terkait denganorganisasiatau ancaman yang diarahkan organisasi lain.
   (ii) Faktor kerentananbaik internaldaneksternaluntukorganisasi.
   (iii) Dampak(bahaya) yangmungkinterjaditerkaitpotensiancaman terhadap organisasi.
   (iv) Kemungkinan bahaya yang akan terjadi.

2. LANDASAN TEORI

2.1 RISIKO

Risiko menurut Stoneburner, sepertidikutip oleh Yaumi, menyebutkan bahwa risiko adalah dampak negatif yang diakibatkan denganadanya kerentanan (vulnerability), berdasarkanpertimbangan dari probabilitas maupun dampakkejadian. Dari beberapa pengertian yang telahdisebutkan, risiko dapat diartikan sebagai dampaknegatif dari suatu ancaman yang mengeksploitasikerentanan yang apabila terjadi, akan merugikan (Yaumi dan Surendro, 2012).

2.2 APO (*Align, Plan, Organize*)

COBIT 5 sebuah kerangka kerja generasi terbaru dari panduan ISACA yang memebahas mengenai tata kelola dan manajemen TI. COBIT 5 menyediakan kerangka kerja yang membantu perusahaan dalam mencapai tujuan mereka dengan tata kelola dan manajemen teknologi informasi (ISACA,2012). Kerangka kerja COBIT 5 terbagi dalam 5domain, salah satunya adalah APO (Align, Plan, Organize) yang merupakan domain yang

digunakan untuk mengidentifikasi cara terbaikbagi tata kelola Teknologi Informasi (TI) untuk berkontribusi dalam pencapaian tujuan perusahaan (ISACA, 2013).

Dalam penelitian ini digunakan proses APO 12 yang merupakan pedoman proses mengelola risiko yang secara terus menerus mengidentifikasi, menilai dan mengurangi risiko terkait TI dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Proses ini mendukung tercapainya serangkaian tujuan yang berhubungan dengan TI, yang mendukung tercapainya serangkaian tujuan perusahaan.

Manajemen risiko perusahaanm yang berkaitan dengan TI harus terintegrasi dengan *enterprise risk management* (ERM) secara keseluruhan. Domain APO12 memiliki 6 subdomain yaitu sebagai berikut:

a. APO12.01 *Collect Data* / mengumpulkan data
b. APO12.02 *Analyse Risk* / menganalisis risiko
c. APO12.03 *Maintain A Risk Profile*
d. APO12.04 *Articulate Risk*
e. APO12.05 *Define a Risk Management Action Portofolio*
f. APO12.06 *Respond to Risk*

Dari domain tersebut dilakukan penilaian capability level yang bertujuan untuk memberikan penilaian yang berbeda dari satu level ke level yang lebih tinggi dan *risk assessment*, yaitu suatu proses untuk mengidentifikasi potensial risiko yang terjadi baik yang berasal dari dalam maupun dari luar yang dihadapi oleh perusahaan atau organisasi. Tujuan dilakukannya *risk assessment* adalah untuk mengukur seberapa besar risiko yang dihadapi dan seberapa besar dampak terhadap organisasi, sehingga dapat digunakan untuk meminimalisir dampak. Dari *risk assessment* dapat menentukan mitigasi risiko yang merupakan metode atau cara yang sistematis digunakan untuk mengurangi dampak yang timbul akibat adanya suatu risiko. Stategi dalam melakukan pengurangan risiko misalnya menerima risiko (*risk assumption*), mencegah risiko (*risk avoidance*), membatasi level risiko (*risk limitation*), atau mentransfer risiko (*risk transference*). (ISACA,2012).

3. METODOLOGI DAN PEMBAHASAN

3.1 METODOLOGI

Metode yang akan dipakai di sini adalah studi literatur, pengumpulan data, analisis data dan mengimplementasikan pedoman manajemen risiko COBIT 5.

Berikut adalah uraian metode yang digunakan :

1. Melakukan Studi Literatur terhadap berbagai jenis buku, jurnal, dan teori mengenai COBIT 5.
2. Mendefinisikan masalah dengan menentukan sistem informasi yang akan diteliti dalam hal ini Perpustakaan Digital (*Digital Library*)
3. Pengumpulan data-data yang diperlukan untuk evaluasi teknologi informasi, dengan cara menyebar kuesioner, observasi dan wawancara.
4. Melakukan analisis *risk assessment* berdasarkan pedoman COBIT 5 domain APO12.
5. Melakukan evaluasi terhadap hasil dari analisis untuk menyusun sebuah rekomendasi.

3.2 PEMBAHASAN

Kondisi sistem *Digital Library* saat ini berjalan sebagai berikut:

Sistem *Digital Library*adalah kumpulan dokumen yang disimpan dalam bentuk elektronis, dapat disimpan dalam bentuk media disk, CD dan/atau ditampilkan dalam suatu situs web. *Digital library* di suatu perguruan tinggi X sudah berjalan sekitar 12 tahun. Untuk mengetahui apakah sistem digital library tersebut sudah bermanfaat secara efektif dan efisien bagi pemakainyamaka dilakukan pengumpulan data dengan cara kuesioner kepada civitas akademik sebagai pemakai sistem. Selanjutnya adalah mengimplementasikan sub proses APO 12.01 sampai dengan APO 12.06.

3.2.1 PENGUMPULAN DATA

APO 12.01 merupakan proses mengidentifikasi dan mengumpulkan data yang relevan untuk mengidentifikasi risiko, analisis dan pelaporan yang efektif terkait dengan TI.

Observasi dilakukan untuk melengkapi kebutuhan informasi yang dibutuhkan untuk subdomain APO12 (*Manage Risk*) untuk evaluasi manajemen risiko sistem *Digital Library (DL)* sebuah perguruan tinggi swasta di Bandung. Observasi dilakukan dengan pengamatan terhadap proses bisnis yang ada dan menyebarkan kuesioner yang berkaitan dengan sistem tersebut.

Berdasarkan hasil pengumpulan bukti adalah belum mempunyai dokumen tersendiri untuk manajemen risiko TI, sebagian besar (90%) personal *civitas academica* di X mengetahui adanya sistem DL, pernah memakai sistem DL (80,6%) dan cukup sering (41,1%), mengetahui prosedur login (86,1%), mengetahui fasilitas searching (66,7%). Hasil lainnya seperti pada tabel berikut ini.

Tabel 1. Hasil Pengumpulan Data

Pertanyaan lainnya tentang	**Hasil**	**sangat puas**	**puas**	**kurang puas**	**tidak berpendapat**	**sangat tidak puas**
Style font sudah sesuai	48%					
Warna font dan backgrount sudah sesuai	72%					
Penempatan daftar ebook sudah rapi	52%					
Jaringan DL terhubung dengan baik	48%					
Portal DL sangat strategi bagi kampus	25%					
Tersedia forum komunikasi antar mahasiswa dengan admin DL	36%					
Link ebook sudah sesuai	33%					
Tampilan ebook (output dari link-link)		3%	30 %	42%	22%	3%
Kecepatan akses saat membuka ebook		3%	30 %	10%	27%	30%
Pencarian ebook		50%		33%	17%	
Menu ebook (kelengkapan ebook)			30 %	28%	42%	

Pertanyaan lainnya tentang	Hasil	sangat puas	puas	kurang puas	tidak berpendapat	sangat tidak puas
Keamanan sistem			25 %	40%	35%	

3.2.2 IMPLEMENTASI APO 12 (MENGELOLA RISIKO)

APO 12 merupakan pedoman proses mengelola risiko yang secara terus menerus mengidentifikasi, menilai dan mengurangi risiko terkait TI dalam tingkat toleransi yang ditetapkan oleh manajemen eksekutif perusahaan.

Berikut adalah sub domain pada APO 12 :

1. APO12.01 *Collect Data* / mengumpulkan data

   Mengidentifikasi dan mengumpulkan data yang relevan untuk mengidentifikasi risiko, analisis dan pelaporan yang efektif terkait dengan TI.

   Kegiatan yang dilakukan diantaranya :

   a. Menetapkan metode pengumpulan, klasifikasi dan analisis data terkait risiko TI, mengakomodasi beberapa jenis kejadian, beberapa kategori risiko TI dan beberapa faktor risiko.
   b. Mencatat data yang relevan mengenai lingkungan operasi internal dan eksternal perusahaan yang dapat memainkan peran penting dalam pengelolaan TI risiko.
   c. Survei dan analisis pengalaman dan kehilangan data historis risiko TI dari data dan tren eksternal yang tersedia, rekan industri melalui industri - event log, database, dan perjanjian industri untuk pengungkapan kejadian bersama.
   d. Mencatat data kejadian risiko yang menyebabkan atau menimbulkan dampak terhadap pemberdayaan manfaat / nilai TI, program TI dan / atau Operasi TI dan pemberian layanan data yang relevan dari isu, insiden, masalah dan investigasi terkait.
   e. Untuk kelas kejadian yang serupa, atur data yang dikumpulkan dan sorot faktor yang berkontribusi. Tentukan faktor kontribusi umum di seluruh beberapa kejadian
   f. Tentukan kondisi spesifik yang ada atau tidak ada saat terjadi kejadian risiko dan bagaimana kondisi mempengaruhi frekuensi kejadian dan kehilangan besarnya.
   g. Lakukan analisis kejadian dan analisis faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang baru muncul dan untuk mendapatkan pemahaman tentang internal yang terkait dan faktor risiko eksternal.

Dari kasus DL yang diteliti, hasil dari APO 12.01 berdasarkan hasil kuesioner, teridentifikasi risiko sistem DL sebagai berikut :

a. kesulitan menangani risiko yang terjadi karena belum adanya dokumen tentang manajemen risiko
b. proses login menggunakan password yang jarang diganti
c. keamanan sistem memiliki tingkat kepuasan yang kurang
d. keberhasilan pencarian ebook
e. kecepatan akses tidak terpenuhi

f. link ebook tidak tersedia
g. Perancangan antar muka aplikasi
h. Koneksi Jaringan terganggu

2. APO12.02 *Analyse Risk* / menganalisis risiko
Mengembangkan informasi yang berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi faktor risiko
Kegiatan yang dilakukan diantaranya :
   a. Menentukan kedalaman upaya analisis risiko yang tepat dengan mempertimbangkan semua faktor risiko dan kekritisan aset bisnis.
   b. Menetapkan lingkup analisis risikonya setelah melakukan analisis biaya / manfaat.
   c. Membangun dan memperbarui secara teratur skenario risiko TI, termasuk skenario gabungan jenis ancaman bertingkat dan tidak terduga, dan mengembangkan harapan untuk aktivitas pengendalian tertentu, kemampuan untuk mendeteksi dan tindakan respons lainnya.
   d. Memperkirakan frekuensi dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko TI.
   e. Memperhatikan semua faktor risiko yang berlaku, evaluasilah kontrol operasional yang diketahui dan perkiraan tingkat risiko residual.

Analisis risiko untuk kasus DL, adalah upaya untuk memahami risiko lebih dalam. Hasil analisis risiko ini akan menjadi masukan bagi evaluasi risiko dan proses pengambilan keputusan mengenai perlakuan risiko terhadap risiko tersebut. James W. Meritt, dalam *A Method for Quantitative Risk Analysis*, menjelaskan bahwa Analisis Resiko Kualitatif digunakan untuk meningkatkan kesadaran atas masalah keamanan sistem informasi dan sikap dari sistem yang sedang dianalisis tersebut. Analisis risiko secara kualitatif meninjau dua aspek risiko, yaitu dampak dan peluang. Tingkat risiko akan ditentukan oleh kombinasi dari dampak dan kemungkinan. Pada proses analisis risiko ini dilakukan penilaian terhadap risiko-risiko yang muncul pada sistem DL Hal ini mencakup penilaian terhadap dampak apabila suatu risiko terjadi, serta peluang terjadinya risiko.
Kriteria untuk dampak memiliki nilai dampak ringan, sedang dan berat. Kriteria untuk peluang memiliki nilai peluang kecil, sedang dan tinggi.

Tabel 2. Hasil Analisis Risiko Sistem DL

No.	Risiko	Pengendalian	Peluang	Dampak
1.	Dokumen tentang manajemen risiko	Menyiapkan beberapa referensi manajemen risiko	sedang	ringan
2.	password yang jarang diganti	Menampilkan notifikasi / alert penggantian password terakhir	tinggi	sedang
3.	keamanan sistem	• Menyediakan penanggung jawab sistem	sedang	berat

		• Memasang anti virus		
4.	keberhasilan pencarian *ebook*	Membuat daftar ebook berdasakan abjad	sedang	berat
5.	kecepatan akses tidak terpenuhi	Menampilkan proses loading	sedang	ringan
6.	link ebook tidak tersedia	Membuat daftar link internal dan eksternal	sedang	sedang
7.	Perancangan antar muka aplikasi	Menyediakan pengaturan tampilan	kecil	ringan
8.	Koneksi Jaringan terganggu	Memeriksa koneksi secara berkala	kecil	sedang

3. APO12.03 *Maintain A Risk Profile*
   Menjaga inventarisasi risiko dan atribut risiko yang diketahui, termasuk frekuensi yang diharapkan, dampak potensial, dan tanggapan, dan terkait sumber daya, kemampuan, dan kegiatan kontrol saat ini
   Kegiatan yang dilakukan diantaranya adalah :
   1. Menginventarisasi personil pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok dan agen outsourcing, dan mendokumentasikan ketergantungan pada proses manajemen layanan TI dan sumber daya infrastruktur TI.
   2. Menentukan layanan TI dan sumber daya infrastruktur TI yang penting untuk memelihara dan merawat pengoperasian proses bisnis.
   3. Menganalisa ketergantungan dan mengidentifikasi koneksi lemah.
   4. Secara reguler, mengambil semua informasi profil risiko dan konsolidasikan ke dalam profil risiko gabungan.
   5. Berdasarkan semua data profil risiko, tentukan seperangkat indikator risiko yang memungkinkan identifikasi cepat dan pemantauan risiko saat ini dan tren risiko.
   6. Kumpulkan informasi tentang kejadian risiko TI yang telah terwujud, untuk dimasukkan dalam profil risiko TI perusahaan.
   7. Kumpulkan informasi mengenai status rencana aksi risiko, untuk dimasukkan ke dalam profil risiko TI perusahaan.

   Hasil dari proses ini untuk kasus sistem DL dapat dilihat pada Tabel 3.

Tabel 3. Hasil Profil Risiko Sistem DL

No.	Risiko	Tingkat Risiko
1.	Dokumen tentang manajemen risiko	sedang
2.	password yang jarang diganti	tinggi
3.	keamanan sistem	sedang
4.	keberhasilan pencarian *ebook*	sedang
5.	kecepatan akses tidak terpenuhi	sedang

6.	link ebook tidak tersedia	sedang
7.	Perancangan antar muka aplikasi	kecil
8.	Koneksi Jaringan terganggu	kecil

4. APO12.04 *Articulate Risk*
   Memberikan informasi tentang keadaan terkini dari IT - cara mendeskripsikan peluang terkait secara tepat waktu untuk semua pemangku kepentingan yang dibutuhkan dengan respon yang tepat
   Kegiatan yang dilakukan adalah :
   a. Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terkena dampak dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Mencakup probabilitas dan rentang kerugian atau keuntungan seiring dengan tingkat kepercayaan yang memungkinkan manajemen untuk menyeimbangkan pengembalian risiko.
   b. Memberikan pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan uji tuntas, dan signifikan reputasi, pertimbangan hukum atau peraturan.
   c. Meaporkan profil risiko terkini kepada semua pemangku kepentingan, termasuk keefektifan proses manajemen risiko, efektivitas pengendalian, kesenjangan, ketidakkonsistenan, redudansi, status remediasi, dan dampaknya terhadap profil risiko.
   d. Meninjau hasil penilaian penilaian pihak ketiga, audit internal, dan penjaminan yang obyektif yang objektif dan rujuklah profil tersebut ke profil risiko.

Tabel 4. Hasil Artikulasi Risiko Sistem DL

No.	Risiko	Peluang	Rekomendasi
1.	Dokumen tentang manajemen risiko	sedang	Membuat panduan manajemen risisko
2.	password yang jarang diganti	tinggi	a. Notifikasi Perubahan password secara berkala b. Pengaturan dalam pembuatan password c. Penghapusan password terhadap akun yang sudah tidak aktif
3.	keamanan sistem	sedang	a. Memasang anti virus dan sejenisnya. b. Meng-update anti virus secara berkala
4.	keberhasilan pencarian *ebook*	sedang	Menambah daftar pencarian
5.	kecepatan akses tidak terpenuhi	sedang	Meningkatkan layanan koneksi
6.	link ebook tidak	sedang	Menambah daftar link

	tersedia		
7.	Perancangan antar muka aplikasi	kecil	Menyediakan pegaturan tampilan
8.	Koneksi Jaringan terganggu	kecil	Memeriksa secara berkala

5. APO12.05 *Define a Risk Management Action Portofolio*
   Memastikan bahwa tindakan untuk merancang strategi kesempatan dan mengurangi risiko ke tingkat yang dapat diterima dikelola sebagai portofolio.
   Kegiatan yang dilakukan adalah :
   1. Mempertahankan inventarisasi aktivitas pengendalian yang ada untuk mengelola risiko dan memungkinkan risiko diambil sesuai dengan toleransi risiko. Klasifikasikan kegiatan pengendalian dan mengacu pada laporan risiko TI spesifik dan agregasi risiko TI.
   2. Menentukan apakah setiap entitas organisasi memonitor risiko dan menerima pertanggungjawaban untuk beroperasi dalam tingkat toleransi individu dan portofolio.
   3. Menentukan satu set proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan / atau proyek yang memungkinkan peluang perusahaan strategis, pertimbangkan biaya / manfaat, berpengaruh terhadap profil risiko saat ini, dan peraturan.

   Jenis-jenis cara mengelola atau menangani risiko adalah : [8]
   a. Menghindari risiko (risk avoidance), berarti tidak melaksanakan atau meneruskan kegiatan yang menimbulkan risiko tersebut.
   b. Berbagi risiko (risk sharing / risk transfer), yaitu suatu tindakan untuk mengurangi kemungkinan timbulnya risiko atau dampak risiko.
   c. Mitigasi (mitigation), yaitu melakukan perlakuan risiko untuk mengurangi kemungkinan timbulnya risiko, atau mengurangi dampak risiko bila terjadi, atau mengurangi keduanya.
   d. Menerima risiko (risk acceptance), yaitu tidak melakukan perlakuan apapun terhadap risiko tersebut.

Tabel 5. Tindakan Penanganan Risiko Sistem DL

No.	Risiko	Pengendalian	Peluang	Tindakan
1.	Dokumen tentang manajemen risiko	Menyiapkan beberapa referensi manajemen risiko	sedang	Mitigasi
2.	password yang jarang diganti	Menampilkan notifikasi / alert penggantian password terakhir	tinggi	Menghindari
3.	keamanan sistem	• Menyediakan penanggung jawab sistem • Memasang	sedang	Menghindari

No.	Risiko	Pengendalian	Peluang	Tindakan
		anti virus		
4.	keberhasilan pencarian *ebook*	Membuat daftar ebook berdasakan abjad	sedang	Mitigasi
5.	kecepatan akses tidak terpenuhi	Menampilkan proses loading	sedang	Mitigasi
6.	link ebook tidak tersedia	Membuat daftar link internal dan eksternal	sedang	Mitigasi
7.	Perancangan antar muka aplikasi	Menyediakan pengaturan tampilan	kecil	Menerima
8.	Koneksi Jaringan terganggu	Memeriksa koneksi secara berkala	kecil	Mitigasi

6. APO12.06 *Respond to Risk*

Menanggapi secara tepat waktu dengan efektiflangkah untuk membatasi besarnya kerugian darikejadian terkait IT akibat munculnya risiko.

Proses ini dapat merupakan tindakan peringanan terhadap risiko yang sudah terdokumentasi. Hasil dari penilaian risiko ini berupa profil risiko dengan berbagai rekomendasi yang sekiranya dapat menjadi solusi dalam proses meringankan risiko yang sesuai dengan kebutuhan sistem informasi.

Kegiatan yang dilakukan adalah :

a. Mempersiapkan, pertahankan dan uji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil saat kejadian berisiko dapat menyebabkan operasi yang signifikan atau kejadian pembangunan dengan dampak bisnis yang serius, termasuk jalur eskalasi di seluruh perusahaan.
b. Mengkategorikan insiden, dan membandingkan eksposur aktual dengan ambang toleransi risiko. Mengkomunikasikan dampak bisnis kepada pengambil keputusan sebagai bagian dari pelaporan, dan memperbarui profil risiko.
c. Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat terjadi insiden risiko.
d. Memeriksa dampak kerugian yang terjadi di masa lalu dan kehilangan peluang dan tentukan akar penyebabnya. Komunikasikan akar penyebab, respon risiko tambahan persyaratan dan perbaikan proses terhadap proses tata kelola risiko dan pengambil keputusan yang tepat.

Pada kasus sistem DL, dalam hal ini pengelola sistem atau pihak terkait, perlu menindak lanjuti rekomendasi seperti pada Tabel 5.

4 KESIMPULAN

Kesimpulan untuk implementasi manajemen risiko sistem informasi menggunakan COBIT 5 adalah sebagai berikut :

a. Domain proses yang dipakai dalam penelitian ini adalah APO (*Align, Plan, Organize*) 12 yag memiliki subdomain APO 12.01 sampai dengan APO 12.06 yaitu

mengumpulkan data, menganalisis risiko, menjaga profil risiko, mengartikulasi risiko, menentukan portofolio tindakan pengelolaan risiko dan menanggapi risiko.

b. Berdasarkan pengumpulan data, temuan risiko yang tinggi pada kasus sistem Digital Library adalah password yang jarang diganti, sedangkan dokumentasi, keamanan sistem, link , pencarian dan kecepatan akses bernilai sedang. Perancangan antar muka aplikasi dan koneksi jaringan memiliki nilai risiko kecil.
c. Untuk mengoptimalkan proses manajemen risiko, perlu dilakukan penangan atau tanggapan risiko dengan melakukan tindak lanjut terhadap rekomendasi berdasarkan hasil temuan risiko.

5 DAFTAR PUSTAKA

[1]. Deni, A., Teduh, D., dan Hendrik. (2013). Manajemen Risiko Sistem Informasi Akdemik Pada Perguruan Tinggi Menggunakan Metode Octave Allegro. Seminar Nasional Aplikasi Teknologi Informasi. Yogyakarta.

[2]. Siahaan,Hinsa.(2007). Manajemen Risiko: Konsep,Kasus, dan Implementasi. Elex Media Komputindo,Jakarta.

[3]. Andreas,G.,Sanyoto.G.,&Irvan.T. (2008). Pengukuran Resiko Teknologi Informasi (TI) Dengan Metode Octave-S. CommIT,Vol 2 No.1 Mei 2008, Hal.33-38.

[4]. O'Brien,James A.& Marakas, George M.(2006). Management Information System, edisi ke-7.McGraw-Hill,New York

[5]. Arif Lokobal Marthin D. J. Sumajouw, Bonny F. Sompie (2014) ,Manajemen Risiko Pada Perusahaan Jasa Pelaksana Konstruksi Di Propinsi Papua, Jurnal Ilmiah Media Engineering Vol.4 No.2, Manado

[6]. ISACA. (2013). COBIT Process Assessment Model(PAM): Using COBIT 5. Illinois: ISACA.

[7]. ISACA. (2013). Self-Assessment Guide: UsingCOBIT 5. Illinois: ISACA.

[8]. [Online]. Available: https://www.academia.edu/9860893/ PROSES_MANAJEMEN_RISIKO/alfa sitetsu. [Accessed 1 Juni 2018].

[9]. Stoneburner, A. Goguen and A. Feringa. (2002)"Risk Management Guide for Information Technology System", Recommedation ofNational Institute of Standards and Technology Special Publication 800-30.

[10]. Yaumi dan Surendro. (2012). Model ManajemenRisiko pada Penerapan Cloud Computing untukSistem Informasi di Perguruan tinggiMenggunakan Framework COSO ERM dan FMEA (Studi Kasus: ITB). ITB.

[11]. Meritt, James W. CISSP."A Method for Quantitative Risk Analysis", NIST Computer Security, 1999