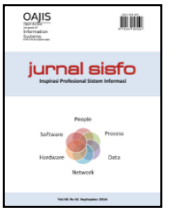
OAJIS
Open Access Journal of Information Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 07 No. 01 (2017) 57–70



Pembuatan Perangkat Audit Berbasis Risiko Berdasarkan COBIT 5 dan *Service Desk Standard* pada *Service Desk*

Sarah Putri Ramadhani*, Anisah Herdiyanti, Hanim Maria Astuti

Departemen Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember

Abstract

A service desk of DPTSI is responsible for handling incidents and providing IT services. However, DPTSI has never held an internal control over its processes, i.e. audit. An audit program shall be provided before an audit is conducted. It is a set of instructions an auditor should follow in order to meet the audit objectives. This study aims at designing a risk based service requests and incident management audit program based on audit control objectives in Service Desk Standard mapped with processes in COBIT 5 DSS02 Manage Service Requests and Incidents. The scope of the audit was determined according to the control objectives that are mapped to IT risks at the service desk following COBIT 5 for Risk APO12 Manage Risk. The results from the study are an audit program and a user guide providing as a reference for DPTSI when performing an audit on the service desk.

Keywords: Audit Program, Service Desk, Service Requests, Incidents, COBIT 5, COBIT 5 for Risk, Service Desk Standard

Abstrak

Service Desk pada Direktorat Pengembangan Sistem dan Teknologi Informasi (DPTSI) bertugas menangani insiden dan memenuhi permintaan layanan teknologi informasi (TI). Namun DPTSI belum pernah mengadakan pengendalian internal terhadap prosesnya. Untuk memastikan pengelolaan telah diterapkan sesuai dengan kontrolnya diperlukan audit TI terhadap unit tersebut. Salah satu hal yang perlu disiapkan dalam melaksanakan audit adalah perangkat audit agar auditor memiliki kertas kerja dalam menjalankan proses audit. Penelitian ini berfokus pada pengembangan perangkat audit pada service desk DPTSI yang dibuat berdasarkan *control objective* pada *Service Desk Standard* yang dipetakan dengan proses pada *best practice* COBIT 5 Domain DSS02 *Manage Service Requests and Incidents*. Ruang lingkup perangkat audit juga ditetapkan melalui *control objective* yang dipetakan dengan risiko TI pada service desk berdasarkan COBIT 5 *for Risk* APO12 *Manage Risk*. Hasil dari penelitian ini adalah sebuah dokumen perangkat audit beserta panduan penggunaannya, yang nantinya diharapkan dapat membantu DPTSI untuk melakukan audit pada service desk.

Kata kunci: Perangkat Audit, *Service Desk*, Permintaan Layanan, Insiden, COBIT 5, COBIT 5 *for Risk*, *Service Desk Standard*.

Histori Artikel : Disubmit 13 Januari 2017; Diterima 31 Maret 2017; Tersedia online 30 September 2017

*Corresponding Author
Email address: sarahputrirmdhni@gmail.com (Sarah Putri Ramadhani)

1. Pendahuluan

DPTSI (Direktorat Pengembangan Teknologi dan Sistem Informasi) merupakan unit di Institut Teknologi Sepuluh Nopember (ITS) Surabaya yang bertugas membantu organisasi dalam memberikan layanan prima bagi civitas akademik melalui pengelolaan teknologi dan sistem informasi secara terpadu [1]. *Service desk* sebagai unit fungsional pada DPTSI berfungsi untuk menghubungkan antara unit teknologi sistem informasi dengan semua pengguna layanan TI yang ada pada ITS Surabaya. Suatu unit *service desk* harus memberikan respon yang tepat waktu dan efektif untuk memenuhi permintaan pengguna dan resolusi dari semua jenis insiden dengan cepat dan tepat [2].

Dalam aktivitas operasional pemberian layanan TI kepada pengguna, tidak jarang *service desk* mengalami gangguan dan risiko dalam melakukan aktivitas pengelolaan insiden, pemenuhan permintaan layanan di luar insiden, maupun penerimaan permintaan akses [3]. Begitu juga dengan *service desk* DPTSI yang selama ini hanya sebatas pada melakukan pencatatan dan penanganan tanpa memberikan prioritas dan klasifikasi terhadap permintaan layanan dan insiden yang dapat menyebabkan kesalahan mengambil keputusan dalam penanganannya. Gangguan dan risiko ini mengakibatkan kualitas performa pada *service desk* menjadi berkurang. Oleh karena itu *service desk* membutuhkan suatu kontrol untuk memastikan bahwa proses pengelolaan permintaan layanan dan insiden pada *service desk* dilaksanakan dengan baik, serta untuk memitigasi risiko pada proses. Salah satu upaya kontrol terhadap proses pada *service desk* yang belum dilakukan oleh DPTSI adalah pengendalian internal.

Audit internal sebagai upaya pengendalian perlu dilakukan untuk memastikan bahwa tingkat layanan terhadap pengelolaan permintaan layanan dan insiden yang diberikan oleh *service desk* DPTSI telah memenuhi standar yang diinginkan dan sesuai dengan *best practice* [4]. Dalam melakukan audit, ada banyak hal yang harus dipersiapkan seperti salah satunya dengan mempersiapkan perangkat audit. Perangkat audit sebagai alat atau *tools* yang di dalamnya berisi dokumen-dokumen kerja terstandar dapat digunakan para auditor internal DPTSI dalam membantu proses audit agar lebih efektif dan efisien. Suatu perangkat audit penting untuk dibuat karena menyediakan serangkaian instruksi dari proses yang harus dilakukan *service desk* sehingga membantu seorang auditor dalam menjalankan audit sesuai dengan tujuan dan memastikan seluruh proses telah dilakukan [5]. Perangkat audit tersebut menyajikan struktur dan rencana kerja dari aktivitas audit terhadap *service desk* [6].

Berdasarkan refleksi terhadap permasalahan dari kondisi kekinian yang dialami oleh DPTSI, makalah ini bertujuan untuk menghasilkan dokumen perangkat audit berbasis risiko berdasarkan *best practice* COBIT 5 Domain DSS02 *Manage Service Requests and Incidents* dan *Service Desk Standard* yang disesuaikan dengan prosedur operasional layanan pada unit *service desk*. Dengan adanya perangkat audit untuk pengelolaan permintaan layanan dan insiden diharapkan Direktorat Pengembangan Teknologi dan Sistem Informasi ITS Surabaya dapat meningkatkan performa kualitas layanan terhadap pemberian layanan TI dan mengurangi permasalahan layanan TI sehingga layanan tersebut dapat memberikan nilai secara prima bagi setiap pengguna layanan.

2. Tinjauan Pustaka/Penelitian Sebelumnya

Pada bagian ini dipaparkan beberapa teori yang digunakan dalam pengerjaan penelitian ini.

2.1 Audit SI/TI

Audit adalah akumulasi dan evaluasi dari bukti mengenai informasi untuk menentukan dan melaporkan derajat kesesuaian antara informasi dan kriteria yang telah ditentukan [7]. Sedangkan Audit Sistem Informasi merupakan aktivitas audit yang dilakukan untuk memastikan pengelolaan sistem informasi sehingga terarah

dalam kerangka perbaikan berkelanjutan dan penyesuaian terhadap kepatutan apakah sistem berjalan sesuai dengan standard yang berlaku [8].

Memahami penilaian risiko dapat sangat membantu auditor dalam merencanakan aktivitas audit. Menurut Lawrence B. Sawyer, *risk-based auditing* atau audit berbasis risiko merupakan observasi dan analisis kontrol yang kemudian berlanjut ke penentuan risiko terkait operasional dan akhirnya menentukan apakah suatu aktivitas sesuai dengan tujuan organisasi. Tidak dapat terhindarnya risiko di seluruh aktivitas operasional menjadikan konsep manajemen risiko semakin diterima dalam aktivitas audit [9].

2.2 Perangkat Audit

Perangkat audit merupakan sebuah alat atau *tools* yang dapat digunakan dalam membantu proses audit agar lebih efektif dan efisien. Dengan menggunakan sebuah perangkat audit, seorang auditor dapat menjalankan audit sesuai dengan tujuan dan selain itu juga memastikan seluruh proses audit telah dilakukan [5]. Dalam pembuatan perangkat audit pada penelitian ini mengacu pada standar IS/ISO 19011 : 2011 terkait pembuatan dokumen kerja yang akan digunakan oleh tim audit untuk mengumpulkan dan menganalisa relevansi informasi dan bukti-bukti yang nantinya akan dicatat pada *audit report* [10].

2.3 Analisis Risiko TI

Menurut Metinaro, Risiko Teknologi Informasi (TI) merupakan risiko yang berkaitan dengan teknologi informasi yang mana dari sudut pandang ilmu manajemen risiko secara umum dan industri finansial, merupakan bagian dari risiko operasional [11]. Risiko TI membutuhkan adanya suatu pengelolaan yang sistematik dari organisasi sehingga meminimalisir dampak atau bahkan meniadakan terjadinya risiko tersebut. Oleh karena itu, organisasi membutuhkan suatu manajemen risiko TI yang merupakan proses pengidentifikasian, penilaian, dan prioritas risiko dengan tujuan untuk lebih mengkoordinasi sumber daya perusahaan agar lebih tepat sasaran untuk meminimalkan, memantau, dan mengendalikan kemungkinan terjadinya sebuah risiko dan dampak yang dapat ditimbulkan oleh risiko tersebut. Proses analisis risiko TI merupakan bagian dari aktivitas manajemen risiko TI, termasuk diantaranya tahap identifikasi, penilaian, dan prioritas risiko [12].

2.4 COBIT 5 for Risk

Risiko merupakan pemaparan terhadap kemungkinan adanya kerugian, cedera, atau keadaan yang merugikan dan yang tidak diinginkan lainnya [13]; peristiwa yang tidak pasti atau kondisi yang, jika terjadi, memiliki efek pada setidaknya satu proyek tujuan [14]. Risiko TI membutuhkan adanya suatu pengelolaan yang sistematik dari organisasi sehingga meminimalisir dampak atau bahkan meniadakan terjadinya risiko tersebut [12]. COBIT 5 *for Risk* merupakan panduan komprehensif atau kerangka kerja yang khusus dibuat untuk mengidentifikasi, menganalisis, dan merespon risiko organisasi/perusahaan [15]. Pada penelitian ini hanya dilakukan dari tahap pertama hingga kedua, yaitu mengumpulkan data dan menganalisis risiko.

Penilaian risiko pada tahap analisis risiko berdasarkan COBIT 5 *for Risk* menggunakan dua penilaian yaitu peringkat frekuensi dan dampak. Penilaian dampak terdiri dari rata-rata empat dampak, yaitu produktivitas, biaya tanggapan, keunggulan kompetitif, dan hukum. Setiap penilaian memiliki skala peringkat dari 1 hingga 5. Berikut ukuran parameter yang digunakan dalam menentukan tingkat frekuensi terjadinya risiko ditampilkan pada Tabel 1 [15, 16]. Skala yang digunakan menggunakna peringkat frekuensi 1 (*very low*) hingga peringkat frekuensi 5 *very high*. Masing-masing peringkat menunjukkan deskripsi frekuensi skenario yang berbeda-beda sesuai dengan frekuensinya.

Tabel 1. Skala Penilaian Frekuensi Risiko

Peringkat Frekuensi	Frekuensi Skenario	Keterangan
1	N ≤ 0,1	**Very Low**

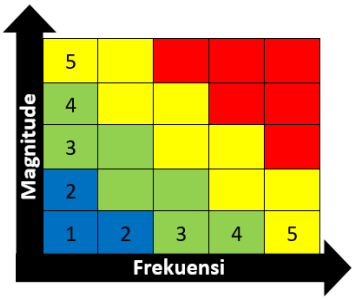
Peringkat Frekuensi	Frekuensi Skenario	Keterangan
		- Kemungkinan skenario risiko terjadi sangat rendah. - Ada kemungkinan terjadi dalam keadaan yang sangat khusus (kemungkinan kecil). - Frekuensi kegagalan terjadi kurang dari sama dengan 0,1 kali dalam satu tahun.
2	$0{,}1 < N \leq 1$	**Low** - Kemungkinan skenario risiko terjadi rendah. - Mungkin terjadi dalam beberapa keadaan. - Frekuensi kegagalan terjadi lebih dari 0,1 kali dan kurang dari sama dengan 1 kali dalam satu tahun.
3	$1 < N \leq 10$	**Moderate** - Kemungkinan skenario risiko terjadi cukup tinggi. - Cenderung terjadi pada beberapa keadaan (kadang-kadang terjadi). - Frekuensi kegagalan terjadi lebih dari 1 dan kurang dari sama dengan 10 kali dalam satu tahun.
4	$10 < N \leq 100$	**High** - Kemungkinan skenario risiko terjadi tinggi. - Ada kemungkinan terjadi pada sebagian besar keadaan (mungkin terjadi). - Frekuensi kegagalan terjadi lebih dari 10 kali dan kurang dari sama dengan 100 kali dalam satu tahun.
5	$100 < N$	**Very High** - Skenario risiko sangat tidak mungkin untuk dihindari. - Cenderung terjadi pada sebagian besar keadaan (sering terjadi). - Frekuensi terjadinya kegagalan sangat tinggi, yaitu lebih dari 100 kali dalam satu tahun.

Sedangkan berikut ukuran parameter yang digunakan dalam menentukan tingkat empat dampak terjadinya risiko ditampilkan pada Tabel 2. Peringkat dampak dimulai dari dampak terendah (skala 1) hingga dampak tertinggi (skala 5). Dampak didefinisikan ke dalam empat aspek, yaitu: produktivitas, biaya tanggapan, keunggulan kompetitif, dan hokum. Nilai peringkat empat dampak risiko tersebut akan dirata-rata untuk menjadi satu peringkat keseluruhan dampak.

Tabel 2. Skala Penilaian Dampak Risiko

Peringkat Dampak	Dampak			
	Produktivitas	**Biaya Tanggapan**	**Keunggulan Kompetitif**	**Hukum**
1	I≤1%	I≤Rp1juta	$I \leq 1$	<Rp1 juta
2	1%<I≤3%	Rp1juta<I≤Rp10juta	$1 < I \leq 1{,}5$	<Rp10 juta
3	3%<I≤5%	Rp10juta<I≤Rp100 juta	$1{,}5 < I \leq 2$	<Rp100 juta
4	5%<I≤10%	Rp100juta<I≤Rp500juta	$2 < I \leq 2{,}5$	<Rp500 juta
5	10%<I	Rp500 juta<I	$2{,}5 < I$	>Rp500 juta

Hasil penilaian frekuensi dan dampak kemudian dipetakan pada suatu peta risiko yang dibagi berdasarkan empat wilayah warna. Berikut peta risiko ditampilkan pada Gambar 1.



Gambar 1. Peta Frekuensi dan Magnitude

Berdasarkan empat wilayah warna kemudian diklasifikasikan berdasarkan level prioritas kegagalan yang memerlukan penanganan lanjut. Gambar 1 menunjukkan frekuensi risiko yang didefinisikan dalam Tabel 1, dan dampak risiko seperti yang didefinisikan pada Tabel 2. Keterangan warna untuk peta frekuensi dan dampak (*magnitude*) terlihat pada Tabel 3 berikut.

Tabel 3. Level Prioritas Risiko

Pemetaan Warna	Level Prioritas
Merah	Very High
Kuning	High
Hijau	Medium
Biru	Low

2.5 COBIT 5 DSS02 Mengelola Permintaan Layanan dan Insiden

Mengelola permintaan layanan dan insiden pada COBIT 5 terdapat pada domain DSS02 *Manage Service Requests and Incidents*. DSS02 sendiri menyediakan standarisasi respon yang efektif dan efisien untuk *request* dari pengguna dan memberikan resolusi untuk semua jenis insiden yang umumnya ditangani oleh *service desk* [17]. COBIT 5 DSS02 terdiri dari tujuh proses, diantaranya sebagai berikut [2]:

1) DSS02.01 : Mendefinisikan skema klasifikasi insiden dan permintaan layanan
2) DSS02.02 : Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden
3) DSS02.03 : Memverifikasikan, menyetujui dan memenuhi permintaan layanan
4) DSS02.04 : Menginvestigasikan, mendiagnosis dan mengalokasikan insiden
5) DSS02.05 : Menyelesaikan dan Memulihkan Insiden
6) DSS02.06 : Menutup Permintaan Layanan dan Insiden
7) DSS02.07 : Melacak Status dan Membuat Laporan

2.6 Service Desk Standard

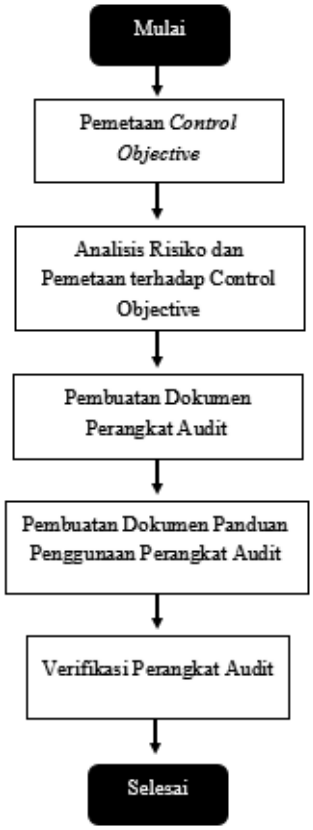
Service Desk Standard merupakan standar yang diterbitkan oleh *Service Desk Institute* (SDI) yang merepresentasikan standar kualitas untuk proses manajemen *service desk* dan komitmen untuk peningkatan pelayanan terus-menerus. *Service Desk Standard* terdiri dari sembilan konsep beserta sub-konsep di dalamnya. Pada sub-konsep terdapat kendali tujuan (*control objective*) [18].

2.7 Penelitian Sebelumnya terkait Pembuatan Perangkat Audit

Pembuatan perangkat audit telah dibahas oleh penelitian sebelumnya, diantaranya: Sulistyaningrum [19] yang menyusun perangkat audit untuk pengelolaan insiden yang menjadi tanggung jawab *service desk* di institusi pemerintahan di Surabaya; sementara Christian [20] mengembangkan perangkat audit dalam sebuah panduan audit. Di sisi lain, audit berbasis risiko digunakan untuk mengevaluasi pengelolaan teknologi informasi seperti yang pendekatannya dipaparkan dalam Messier [21] serta contoh penerapannya dalam evaluasi tingkat layanan [22] dan penerapan sistem enterprise [16].

3. Metodologi

Metodologi penelitian merupakan acuan bagi penulis dalam melakukan penelitian sehingga alur penelitian dapat terstruktur. Berikut metodologi penelitian ditampilkan pada Gambar 2.



Gambar 2. Metodologi Penelitian

Dalam pembuatan perangkat audit berbasis risiko ini, pada tahap pertama penulis melakukan pemetaan *control objective* berdasarkan sub-konsep atau kontrol pada *best practice Service Desk Standard* dengan proses pengelolaan permintaan layanan dan insiden berdasarkan *best practice* COBIT 5 domain DSS02 *Manage Service Requests and Incidents*. Pada tahap kedua dilakukan analisis risiko teknologi informasi berbasis proses pada *service desk* menggunakan kerangka kerja COBIT 5 *for Risk* domain APO12 dan pemetaan risiko dengan *control objecive* untuk mitigasi risiko. Analisis risiko mencakup aktivitas pengumpulan data – termasuk: pembuatan daftar risiko dan penentuan tipe, kategori dan faktor risiko, serta

pembuatan skenario risiko dan penilaian risiko terkait teknologi informasi (TI). Pada tahap ketiga dilakukan pembuatan perangkat audit berdasarkan setiap *control objective* yang terpetakan dengan risiko, serta pembuatan panduan penggunaan perangkat audit. Pada tahap akhir, penulis melakukan verifikasi berdasarkan *best practice* dan persetujuan perangkat audit.

4. Hasil dan Pembahasan

Pada bagian ini akan menjelaskan hasil yang didapatkan dari penulisan dan pembahasan secara keseluruhan yang didapatkan dari penelitian.

4.1 Pemetaan Control Objective

Pada bagian ini, penulis menentukan c*ontrol objective* yang dihasilkan dari proses pemetaan antara proses ideal berdasarkan *best practice* COBIT 5 Domain DSS02 *Manage Service Requests and Incidents* dengan acuan standar lain yang digunakan oleh penulis yaitu sub-konsep atau kontrol pada *Service Desk Standard* [18]. Semua proses dan aktivitas pada COBIT 5 Domain DSS02 digunakan dengan pertimbangan perusahaan harus menggunakan dan mengikuti semua proses ideal pada standar ini.

Pemetaan dilakukan dengan mencari hubungan antara proses ideal berdasarkan COBIT 5 domain DSS02 *Manage Service Requests and Incidents* dengan kontrol yang dibutuhkan dalam setiap prosesnya sehingga didapatkan pemetaan *control objective*. Berikut pada Tabel 4 ditampilkan beberapa pemetaan *control objective*:

Tabel 4. Pemetaan Control Objective

Proses COBIT 5	Sub-konsep Service Desk Standard	*Control Objective*
DSS02.01 Mendefinisikan skema klasifikasi insiden dan permintaan layanan	*4.05 Stafing and scheduling* *4.13 Service catalogue management* *5.03 Service level management*	Memastikan Adanya Pendefinisian Layanan
	4.06 IT service management system *4.07 IT service management system – product capability* *4.10 Self-service*	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
DSS02.02 Mencatat, mengklasifikasikan dan memprioritasikan permintaan dan insiden	*5.05 Incident and service request management*	
	5.06 Incident and service request logging	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
	5.07 Prioritization	Memastikan Adanya Skema Prioritisasi Permintaan Layanan dan Insiden

Proses COBIT 5	Sub-konsep Service Desk Standard	*Control Objective*
DSS02.03 Memverifikasikan, menyetujui dan memenuhi permintaan layanan	*5.08 Categorization*	Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden
	4.15 Security	Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan
	4.14 Financial management	Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan
	4.16 Supplier and partner/3rd party management *5.10 Incident resolution and service request fulfillment*	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden

4.2 Analisis Risiko dan Pemetaan terhadap Control Objective

Pada bagian ini, penulis melakukan analisis risiko berdasarkan *best practice* COBIT 5 *for Risk.* Melalui hasil pengumpulan data terhadap staf *Service Desk* DPTSI, didapatkan empat belas risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk* DPTSI. Pada proses analisis risiko, salah satunya dilakukan tahap penilaian terhadap skenario risiko terhadap bisnis DPTSI. Penilaian risiko yang teridentifikasi dilakukan berdasarkan *best practice* COBIT 5 *for Risk* menggunakan dua penilaian yaitu peringkat frekuensi dan dampak. Dampak dihasilkan berdasarkan hasil survei kepada 53 pengguna sebagai sampel tingkat penurunan kepuasan pengguna sementara frekuensi didapatkan dari hasil wawancara dan observasi lapangan kepada staf *Service Desk* DPTSI.

Hasil dari analisis termasuk penilaian risiko akan dipetakan dalam *control objective* yang dihasilkan dari pemetaan proses berdasarkan COBIT 5 DSS02 dengan *Service Desk Standard.* Pemetaan dilakukan dengan menghubungkan antara risiko dengan *control objective* guna memastikan apakah organisasi telah menerapkan kontrol yang tepat untuk menangani risiko. Level risiko ini nantinya akan digunakan sebagai acuan pada perangkat audit yang telah disusun yaitu Laporan Temuan Audit dalam mengidentifikasi risiko terkait temuan audit yang nantinya akan digunakan sebagai dasar dalam melakukan rekomendasi perbaikan. Berikut hasil pemetaan risiko terhadap *control objective* ditampilkan pada Tabel 5.

Tabel 5. Penilaian Risiko dan Pemetaan Control Objective

ID Risiko	Risiko	Frekuensi	Dampak	Level Penilaian Risiko	Control Objective
IT01	Penanganan insiden dan pemenuhan permintaan layanan overdue	4	1	Medium	CO.08
IT02	Kesalahan penanganan insiden dan pemenuhan permintaan layanan	2	2	Medium	CO.08 CO.09 CO.10
IT03	Kesalahan pemahaman permintaan pengguna layanan	3	2	Medium	CO.01 CO.06

ID Risiko	Risiko	Frekuensi	Dampak	Level Penilaian Risiko	Control Objective
IT04	Keterlambatan respon *service desk*	4	2	High	CO.01
SO01	Kesalahan pencatatan permintaan layanan dan insiden	3	2	Medium	CO.01 CO.03
SO02	Log permintaan layanan dan insiden tidak lengkap	3	2	Medium	CO.02 CO.03
SO03	Pengabaian laporan insiden oleh teknisi/staf *service desk*	1	2	Low	CO.08
SO04	Kesalahan mengalokasikan penanganan insiden dan pemenuhan permintaan layanan	3	2	Medium	CO.09
SO05	Ketidakpuasan user dengan layanan	4	1	Medium	CO.04 CO.05 CO.10
SO06	Ketidakjelasan status permintaan layanan dan insiden	4	1	Medium	CO.10 CO.11
SO07	Kesalahan pendefinisan tren pada laporan	3	2	Medium	CO.12
SW01	Kegagalan akses sistem e-ticket	3	1	Medium	CO.02
SW02	Laporan pengelolaan permintaan layanan dan insiden tidak terdistribusikan	2	1	Low	CO.11
LA01	Penyalahgunaan hak akses permintaan layanan secara sengaja	3	2	Medium	CO.06 CO.07

Berdasarkan hasil pemetaan kemungkinan risiko proses pengelolaan permintaan layanan dan insiden dengan kendali/kontrol tujuan yang dilakukan guna memitigasi risiko yang ada, maka akan digunakan keseluruhan *control objective* tersebut. Setiap *control objective* yang terpetakan dengan risiko ini akan disusun menjadi dokumen perangkat audit.

4.3 Pembuatan Dokumen Perangkat Audit

Pada bagian ini, penulis membuat dokumen perangkat audit proses pengelolaan permintaan layanan dan insiden. Perangkat audit memiliki dua belas (12) dokumen perangkat yang telah disusun berdasarkan *control objective* yang terpetakan dengan risiko. Setiap *control objective* yang disusun menjadi dokumen perangkat audit ini memiliki ID dokumen dengan penamaan "P" yaitu Perangkat Audit, "02" yaitu berasal dari COBIT domain DSS02, kemudian diikuti dengan penomoran berupa angka urutan nomor ID *control objective*. Berikut daftar dokumen perangkat audit yang dibuat ditampilkan pada Tabel 6.

Tabel 6. Daftar Perangkat Audit

No.	ID Control Objective	ID Dokumen	Nama Dokumen
1	CO.01	PA02.01	Memastikan Adanya Pendefinisian Layanan
2	CO.02	PA02.02	Memastikan Adanya Sistem Pengelolaan Permintaan Layanan dan Insiden
3	CO.03	PA02.03	Memastikan Adanya Prosedur Pencatatan Permintaan Layanan dan Insiden
4	CO.04	PA02.04	Memastikan Adanya Prioritisasi Permintaan Layanan dan Insiden
5	CO.05	PA02.05	Memastikan Adanya Klasifikasi Permintaan Layanan dan Insiden
6	CO.06	PA02.06	Memastikan Adanya Verifikasi Hak Penggunaan Permintaan Layanan
7	CO.07	PA02.07	Memastikan Adanya Persetujuan Pemenuhan Permintaan Layanan
8	CO.08	PA02.08	Memastikan Adanya Mekanisme Pemenuhan Permintaan Layanan dan Penanganan Insiden
9	CO.09	PA02.09	Memastikan Adanya Penggunaan Informasi Pengelolaan Insiden
10	CO.10	PA02.10	Memastikan Adanya Penutupan Permintaan Layanan dan Insiden
11	CO.11	PA02.11	Memastikan Adanya Laporan Pengelolaan Permintaan Layanan dan Insiden
12	CO.12	PA02.12	Memastikan Adanya Peningkatan Pengelolaan Permintaan Layanan dan Insiden

Setiap dokumen perangkat audit terdiri dari Daftar Cek Audit (*Audit Checklist*) dan Laporan Temuan Audit.

1) Daftar Cek Audit

Di dalam daftar cek audit, terdapat poin pemeriksaan yang mengacu pada sub-konsep atau kontrol pada *Service Desk Standard* yang terpetakan dalam setiap dokumen perangkat audit. Pada setiap poin pemeriksaan akan diurakan menjadi beberapa langkah pemeriksaan atau prosedur. Setiap prosedur audit berisi pertanyaan-pertanyaan yang disebut *audit cheklist*. Penguraian prosedur audit untuk memastikan tercapainya poin pemeriksaan yang telah dirumuskan yang disesuaikan dengan Jenis Pengujian (*Testing*) yang akan dilakukan, yaitu jenis *testing compliance* dan *substantive*. *Audit checklist* ditentukan berdasarkan prosedur dengan melakukan pengisian pada bagian yang harus diisi dengan tanda centang (√). Berikut ditampilkan contoh dari Daftar Cek Audit pada perangkat audit dengan nomor ID Dokumen PA02.01 pada Gambar 3.

	PERANGKAT AUDIT PENGELOLAAN PERMMINTAAN LAYANAN DAN INSIDEN PADA SERVICE DESK DIREKTORAT PENGEMBANGAN TEKNOLOGI DAN SISTEM INFORMASI (DPTSI) INSTITUT TEKNOLOGI SEPULUH NOPEMBER KOTA SURABAYA		
	CO.01 Memastikan Adanya Pendefinisian Layanan	PA02.01	
		AUDITOR: Andika	AUDITEE: Putri
TANGGAL :	30/12/2016		

Poin Pemeriksaan	Prosedur	Jenis Testing	Audit Checklist	Ya	Tidak	Partial	Bukti dan Temuan
1. Pemeriksaan adanya pendefinisian layanan yang disetujui oleh pelanggan bisnis dan dipublikasikan pada pengguna akhir	Auditor melakukan cek terkait adanya pendefinisian layanan	Compliance	Apakah organisasi memiliki pendefinisian layanan yang disediakan untuk pengguna?	√			Tersedia pendefinisian layanan pada Dokumen katalog layanan dan screenshot website
	Auditor melakukan cek terkait persetujuan layanan oleh pelanggan bisnis	Substantive	Apakah layanan yang terdefinisi telah disetujui oleh pelanggan bisnis?	√			Tanda tangan pada dokumen Service Level Agreements (SLAs) (Pencapaian 100%)

Gambar 3. Daftar Cek Audit

2) Laporan Temuan Audit

Laporan Temuan Audit merupakan sebuah formulir laporan pemeriksaan yang digunakan auditor dalam merangkum temuan dari proses pemeriksaan setiap *control objective*. Berikut ditampilkan contoh dari template Laporan Temuan Audit pada Gambar 4.

LAPORAN TEMUAN AUDIT No. Perangkat Audit : PA02.01 Control Objective : CO.01 Memastikan Adanya Pendefinisian Layanan		
Tanggal Pemeriksaan : 30/12/2016	Auditor : Andika	Auditee : Putri
Jumlah checklist : 20	Jumlah temuan : 8	Persentase temuan : 40%
Kesimpulan Temuan : 1. Pendefinisian layanan yang dimiliki organisasi tidak dipublikasikan pada pengguna layanan 2. Pada proses manajemen tingkat layanan tidak menegosiasi dan membuat perjanjian tingkat operasional 3. Pendefinisian tingkat staf tidak memenuhi layanan sesuai kontrak dan tingkat layanan yang ditetapkan		Klasifikasi : ◯ Major non-conformity ⊗ Minor non-comformity ◯ Observation ◯ Improvement Possibility Risiko Terkait : Risiko: Keterlambatan respon service desk — Level: medium
Rekomendasi : 1. Perlu adanya sosialisasi dan publikasi lebih lanjut terkait layanan yang disediakan oleh organisasi pada pengguna 2. Perlu untuk membuat perjanjian tingkat operasional yang terdokumentasi dalam dokumen OLAs 3. Perlu untuk memperhitungkan kebutuhan tingkat layanan dan penjadwalan jam kerja untuk memenuhi layanan yang telah disepakati		Penanggung Jawab Perbaikan: Rama Aji Tanggal Penyelesaian Perbaikan : 25/01/2017

Gambar 4. Template Laporan Temuan Audit

4.4 Pembuatan Dokumen Panduan Penggunaan Perangkat Audit

Pada bagian ini, penulis membuat dokumen panduan penggunaan perangkat audit yang terdiri dari beberapa bagian seperti berikut:

1) Pendahuluan
   Pada bagian pendahuluan menjelaskan mengenai latar belakang pembuatan panduan penggunaan perangkat audit.

2) Panduan Umum
   Pada bagian panduan umum menjelaskan Petunjuk Penggunaan Bagian Penilaian Risiko, Petunjuk Pengisian Daftar Cek Audit, dan Petunjuk Pengisian Laporan Temuan Audit.

3) Panduan Khusus
   Bagian Panduan Khusus dibuat sebagai panduan bagi auditor internal dalam melakukan audit dengan beberapa kegiatan inisiasi yang dapat dilakukan.

4.5 Verifikasi Perangkat Audit

Pada bagian ini, penulis melakukan verifikasi perangkat audit setelah perangkat audit telah disusun. Verifikasi perangkat audit dilakukan kepada Kepala SubDirektorat Layanan Teknologi dan Sistem Informasi setelah perangkat audit telah disusun. Proses verifikasi ini dilakukan dengan melakukan penyesuaian antara control objective yang digunakan pada pembuatan perangkat dengan kesesuaiannya pada standar yang penulis gunakan yaitu COBIT 5 DSS02 dan Service Desk Standard. Setelah perbaikan dilakukan dan perangkat audit telah sepenuhnya sesuai dengan pendekatan *best practice*, maka selanjutnya akan dilakukan persetujuan rilisnya perangkat audit dan siap digunakan oleh Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI). Keseluruhan perangkat audit yang telah dibuat berdasarkan dua belas control objective memiliki rincian 58 poin pemeriksaan, 236 prosedur, serta 415 pertanyaan checklist audit dengan jenis testing 230 substantive dan 185 compliance.

5. Kesimpulan

Bagian ini akan menjelaskan kesimpulan yang dihasilkan dari pengerjaan penelitian, beserta saran yang dapat bermanfaat untuk perbaikan di penulisan selanjutnya

5.1 Simpulan

Berdasarkan proses dan tahapan yang telah dilakukan dalam penelitian ini, maka berikut kesimpulan yang diperoleh:

1) Risiko yang paling banyak terjadi pada proses operasional yang dilakukan *service desk* adalah risiko kesalahan pemahaman permintaan pengguna layanan, keterlambatan respon *service desk*, dan ketidakpuasan *user* (pengguna) dengan layanan.
2) Risiko terkait proses pengelolaan permintaan layanan dan insiden pada *service desk* dengan level tertinggi adalah keterlambatan respon *service desk*.
3) *Control objective* yang dapat memitigasi risiko dengan level penilaian tertinggi adalah memastikan adanya pendefinisian layanan. Sedangkan *control objective* yang paling banyak dapat memitigasi risiko adalah memastikan adanya pendefinisian layanan, memastikan adanya mekanisme pemenuhan permintaan layanan dan penanganan insiden, serta memastikan adanya penutupan permintaan layanan dan insiden di mana masing-masing dapat memitigasi tiga risiko. Oleh karena itu, ketiga *control objective* tersebut dapat diprioritaskan dalam pelaksanaan audit.

5.2 Saran

Saran yang dapat diberikan oleh penulis yang diharapkan dapat dikembangkan di masa mendatang diantaranya adalah untuk memperoleh hasil penilaian dampak penurunan kepuasan pengguna yang lebih akurat, dapat digunakan nilai indeks penurunan kepuasan pengguna berdasarkan survei yang dilakukan *service desk* untuk seluruh pengguna layanan di lingkungan ITS dengan tingkat kepercayaan di atas 90%.

Penulis membutuhkan waktu yang cukup lama dan kurang efisien dalam melakukan pemetaan *control objective* sehingga untuk memudahkan penelitian selanjutnya dapat dibuat sebuah alur tata cara pemetaan antara aktivitas pada COBIT 5 DSS02 dan *Service Desk Standard* untuk menghasilkan *control objective*.

6. Daftar Rujukan

[1] DPTSI, "Direktorat Pengembangan Teknologi dan Sistem Informasi," 2013. [Online]. Available: http://dptsi.its.ac.id/?page_id=150.

[2] ISACA, COBIT 5 : Enabling Process, Amerika: ISACA, 2012.

[3] J. V. Bon, A. d. Jong, A. Kolthof, M. Pieper, R. Tjassing, A. v. d. Veen dan T. Verheijen, Foundations of IT Service Management Based on ITIL V3. 3th ed, Van Haren Publishing, Zaltbommel, 2007.

[4] J. L. Mohr, The Help Desk Audit: Blueprint for Success, ITGapPress.com, 2003.

[5] A. A. TYBCom, "Accountancy Auditing," [Online]. Available: http://archive.mu.ac.in/myweb_test/study%20TYBCom%20Accountancy%20Auditing-II.pdf.

[6] P. Lamantia, "An Audit Work Program for a Help Desk Activity," *The EDP Audit, Control, and Security Newsletter*, vol. 28, 2006.

[7] A. A. Arens, R. J. Elder dan M. S. Beasley, Auditing and Assurance Services: An Integrated Approach. 4th ed., Upper Saddle River, New Jersey: Pearson Prentice Hall, 2012.

[8] R. Sarno, Audit Sistem Informasi & Teknologi Informasi, Surabaya: ITS Press, 2009.

[9] L. B. Sawyer, Internal Auditing, New York, 2005.

[10] ISO, IS/ISO 19011 (2011): Guidelines for Auditing Management, NEW DELHI, 2012.

[11] H. Metinaro, "Analisis Risiko Menggunakan Metode Cause-Effect," *Journal of Business and Entrepreneurship*, vol. 2, p. 3, 2014.

[12] D. Hubbard, The Failure of Risk Management: Why It's Broken and How to Fix It, New York: John Wiley & Sons, 2009, p. 46.

[13] O. University, Oxford English Dictionary, Oxford: Oxford University Press, 1997.

[14] P. M. Institute, A Guide to the Project Management Body of Knowledge (4th Edition), Project Management Institute, 2009.

[15] ISACA, Cobit 5 for risk, Amerika: ISACA, 2013.

[16] D. R. Indah, Harlili dan M. A. Firdaus, "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk," *Proceeding of The 1st International Conference on Computer Science and Engineering*, pp. 113-118, 2014.

[17] The ITIL Advisory Group, ITIL V3 Service Operation.

[18] SDI, The Service Desk Standard, Service Desk Institute.

[19] D. R. Sulistyaningrum, "Pembuatan Perangkat Audit Berbasis Risiko untuk Manajemen Insiden pada Service Desk Unit Teknologi Sistem Informasi PDAM Surya Sembada Kota Surabaya," ITS, Surabaya, 2015.

[20] S. Christian, "Pembuatan Panduan Audit Keamanan Fisik dan Lingkungan Teknologi Informasi Berbasis Risiko Berdasarkan ISO/IEC 27002:2013 pada Direktorat Sistem Informasi Universitas Airlangga," ITS, Surabaya, 2015.

[21] J. Wiliam F. Messier, An Approach to Learning Risk-Based Auditing, 2014, pp. 276-287.

[22] O. Illoh, S. Aghili dan S. Butakov, "Using COBIT 5 for Risk to Develop Cloud Computing SLA Evaluation Templates," dalam *Conference Paper*, 2015.

Halaman ini sengaja dikosongkan