Analisis Manajemen Risiko Layanan Sistem Manajemen Dealer Menggunakan COBIT 5

Dimas Adi Prastiyawan, Awalludiyah Ambarwati, Eman Setiawan
Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama
ambarwati1578@yahoo.com

Abstrak: Sistem manajemen *dealer* merupakan layanan Teknologi Informasi (TI) suatu perusahaan otomotif yang berfungsi untuk pengelolaan insiden dan pemenuhan permintaan. Layanan TI tersebut memegang peranan penting bagi perusahaan namun berisiko. Sistem manajemen dealer tersebut memiliki risiko di antaranya kesalahan pencatatan (*logging*) insiden atau permintaan layanan, *helpdesk* tidak mencatat insiden atau permintaan layanan TI. Analisis manajemen risiko pada sistem manajemen dealer perlu dilakukan guna meminimalkan risiko. COBIT 5 (*Control Objectives for Information and Related Technology*) digunakan sebagai kerangka acuan untuk melakukan analisis manajemen risiko tersebut. APO (*Align, Plan and Organize*) dan DSS (*Deliver, Service and Support*) adalah dua dari lima domain yang ada pada COBIT 5. APO11 (*Manage Quality*) dan DSS01 (*Manage Operations*) merupakan proses pendukung pada COBIT 5 yang digunakan untuk mengelola risiko. Hasil penelitian ini berupa analisis manajemen risiko dan rekomendasi langkah mitigasi untuk meminimalkan dampak risiko.

Kata kunci: *analisis manajemen risiko, COBIT 5, layanan TI*

Abstract: *Dealer management system is an Information Technology (IT) service for an automotive company that functions to manage incident and fulfill demand. IT services has an important role for the company but also has several risks. Dealer management system has risks including error logging incidents or service requests, helpdesk does not record incidents or requests for IT services. Risk management analysis on the dealer management system needs to be done to minimize risk. COBIT 5 (Control Objectives for Information and Related Technology) is used as a reference framework for conducting risk management analysis. APO (Align, Plan and Organise) and DSS (Deliver, Service and Support) are two out of five domains in COBIT 5. APO11 (Manage Quality) and DSS01 (Manage Operations) are the supporting processes in COBIT 5 to manage risk. The results of this study are in the form of risk management analysis and recommendations for mitigation measures to minimize the impact of risks.*

Keywords: *risk management analysis, COBIT 5, IT service*

I. PENDAHULUAN

Teknologi Informasi (TI) telah menjadi kebutuhan bagi suatu perusahaan otomotif, terlebih bagi perusahaan otomotif yang memiliki sejumlah dealer. Dukungan TI sangat penting bagi kelancaran bisnis perusahaan. *System Management Dealer* (SMD) merupakan layanan TI yang dimiliki salah satu perusahaan otomotif yang memiliki sejumlah *dealer* di beberapa kota di Indonesia. Perusahaan otomotif ini mempunyai Departemen Teknologi Informasi (DTI) yang berada di kantor pusat. Salah satu tanggungjawab DTI adalah menjaga ketersediaan layanan SMD.

SMD memegang peran yang sangat penting bagi keberlangsungan proses bisnis perusahaan, terutama dalam permintaan layanan. Penerapan SMD mempermudah kerja karyawan yang berada di *dealer* utamanya pengelolaan insiden dan pemenuhan permintaan. Permintaan layanan pada manajemen layanan TI di perusahaan otomotif ini dilakukan oleh *helpdesk* yang terdiri dari dua proses, yaitu pemenuhan permintaan (*request fulfillment*) dan manajemen akses (*access management*). Layanan TI tersebut memegang peranan penting bagi perusahaan namun memiliki risiko. Berdasarkan observasi dan wawancara di perusahaan otomotif ini, diketahui beberapa risiko yang pernah dan cukup sering terjadi berupa kesalahan pencatatan (*logging*) insiden atau permintaan layanan serta *helpdesk* tidak mencatat insiden atau permintaan layanan TI yang masuk. Kejadian tersebut cukup berdampak bagi perusahaan. DTI belum pernah melakukan analisis penilaian risiko terkait pengelolaan layanan TI.

Risiko dapat diartikan sebagai probabilitas terjadinya peristiwa yang dapat merugikan perusahaan akibat dari adanya kerentanan dan ancaman [1]. Manajemen risiko dapat dilakukan dengan memahami, melakukan identifikasi dan evaluasi terhadap kemungkinan risiko. Identifikasi risiko perlu dilakukan untuk mengantisipasi kerugian dan dampak yang dihadapi perusahaan dari sisi finansial dan operasional [2]. Risiko kombinasi dari ketidakpastian peristiwa dan efek yang akan terjadi. Manajamen risiko merupakan identifikasi, mengatur segala risiko serta strategi mengelola sumberdaya yang tersedia [3]. Manajemen risiko TI meliputi tiga proses yaitu penilaian terhadap risiko, *mitigate* risiko serta nilai evaluasi [4].

Kerangka kerja COBIT 5 (*Control Objectives for Information and Related Technology*) merupakan kerangka kerja komprehensif yang dapat digunakan perusahaan untuk mencapai tujuan dalam area tata kelola dan manajemen TI [5]. EDM (*Evaluate, Direct*

and Monitor) merupakan domain yang terdapat pada area tata kelola. Area manajemen memiliki empat domain yaitu APO (*Align, Plan and Organise*), BAI (*Build, Acquire and Implement*), DSS (*Deliver, Service and Support*) dan MEA (*Monitor, Evaluate and Assess*). COBIT 5 dapat membantu memenuhi kebutuhan perusahaan, mengorganisasi aktivitas TI ke dalam proses model yang dapat diterima secara umum, mengidentifikasi sumber teknologi informasi utama, mendefinisikan sasaran proses TI manajemen perusahaan yang harus dipertimbangkan [6].

COBIT 5 *for risk* memiliki perspektif manajemen risiko yang terkait cara identifikasi, analisis serta cara untuk merespons risiko serta tahapan dalam melakukan manajemen risiko. Proses APO11 (*Manage Quality*) dan DSS01 (*Manage Operations*) merupakan dua proses pendukung dalam fungsi risiko [7]. Kedua proses tersebut digunakan dalam penelitian ini untuk analisis manajemen risiko SMD agar dapat dilakukan rekomendasi untuk mitigasi.

Beberapa penelitian sebelumnya menggunakan COBIT 5 sebagai kerangka kerja acuan dalam tata kelola sistem informasi. Evaluasi tata kelola sistem informasi SANKEN dilakukan dengan tujuan mengetahui nilai kematangan dan memberikan rekomendasi. Nilai kematangan yang diperoleh pada evaluasi tata kelola sistem informasi SANKEN adalah 2,93. Rekomendasi yang diberikan untuk peningkatan nilai, di antaranya berupa pelatihan dan penilaian kinerja serta evaluasi sistem secara berkala [8]. COBIT 5 dapat diimplementasikan untuk perlindungan aset informasi menggunakan DSS05 (*Manage Security Service*) [9]. Penerapan COBIT 5 pada suatu perusahaan memberikan dampak positif pada kualitas informasi [10]. COBIT 5 dapat digunakan untuk melakukan audit tata kelola TI [11].

II. METODE PENELITIAN

Salah satu kunci fokus meminimalisir risiko layanan SMD adalah mengetahui nilai risiko dan dampak risiko yang menghasilkan tingkatan risiko. Sebagai penjelasan, dapat dikatakan bahwa manajemen risiko teknologi informasi adalah penilaian terhadap suatu risiko.

Terdapat tiga pemetaan proses TI COBIT 5 *for risk* terhadap manajemen risiko teknologi informasi:

1. Pemetaan Proses TI COBIT 5
   Melakukan pengelolaan pemetaan proses TI permintaan layanan pada SMD sesuai dengan domain *Deliver Service and Support* (DSS) berdasarkan COBIT 5 Enabling process. Sedangkan domain *Align Plan and Organize* (APO) digunakan untuk meminimalisir risiko pada langkah terakhir.
2. Pemetaan Tipe Risiko
   Menentukan pemetaan tipe risiko pada layanan SMD yang sudah disediakan oleh COBIT 5 *for risk*. Terdapat tiga tipe risiko, antara lain IT *programme* and *project delivery risk*, IT *benefit/value enablement risk* dan *IT operations and service delivery risk.*
3. Kategori Risiko
   Melakukan pemetaan yang mengacu kepada standar COBIT 5 *for Risk*. Terdapat dua puluh kategori risiko TI. Dalam penelitian ini, hanya dipilih beberapa kategori yang sesuai dengan layanan.

Selain ketiga pemetaan proses TI COBIT 5 tersebut, terdapat juga beberapa tahapan lain, berupa analisis terhadap risiko. Tahap pertama adalah faktor risiko yang mencakup penentuan kategori risiko berdasarkan ketentuan yang ada pada *best pratice*. Selanjutnya, menentukan sebuah faktor dari penyebab yang mempengaruhi risiko itu terjadi pada saat proses pengelolaan permintaan layanan dan manajemen insiden, baik dalam faktor penyebab internal maupun eksternal.

Tahap kedua berupa Skenario Risiko TI yang terbagi atas dua jenis, yaitu skenario positif dan skenario negatif. Skenario positif berisi dampak apabila risiko tersebut tidak terjadi, sehingga mendeskripsikan proses bisnis yang dapat berjalan lancar dan optimal. Sedangkan skenario negatif berisi dampak apabila risiko terjadi, sehingga menghasilkan sebuah gangguan atau hambatan terhadap proses bisnis perusahaan serta apakah risiko yang terjadi dapat mengalami kerugian yang cukup besar atau tidak.

Tahap ketiga adalah penilaian risiko TI yang membahas mengenai tingkatan risiko layanan SMD, berdasarkan penilaian risiko berapa kali kejadi dalam setahun (frekuensi). Dengan nilai dampak risiko diperoleh dari kuesioner karyawan pada perusahaan transportasi tersebut, yang telah disediakan oleh COBIT 5 *for risk*. Nilai dampak terdiri dari empat diantaranya nilai dampak produktivitas, nilai dampak biaya kerugian akibat risiko, dampak keunggulan kompetitif serta dampak hukum yang berakibat pidana (terkait biaya denda yang harus ditanggung oleh organisasi akibat terjadinya risiko yang berdampak pada hukum). Proses mitigasi COBIT 5 digunakan untuk meminimalisir risiko layanan sistem manajemen dealer. Pengambilan keputusan aktivitas kunci yang relevan untuk diimplementasikan kedalam DTI.

III. HASIL DAN PEMBAHASAN

A. Analisis Pemetaan Proses TI

Setelah dilakukan analisis hasil wawancara dan observasi, maka pemetaan proses TI ini mencakup aktivitas pada proses DSS01. Aktivitas tersebut disesuaikan dengan risiko SMD. Terdapat juga penjelasan berdasarkan risiko yang sendiri terjadi, keterangan terkait mengapa risiko bisa terjadi serta penyebab risiko itu ada. Uraian hasil Pemetaan Risiko TI proses DSS01 dijabarkan dalam Tabel 1.

Tabel 1. Hasil pemetaan risiko TI proses DSS01

Risiko	Keterangan	Penyebab
Helpdesk tidak mencatat permintaan layanan TI yang masuk	*Helpdesk* tidak mencatat insiden atau permintaan layanan TI sehingga tidak terdapat *log* insiden atau permintaan layanan TI	Pengelolaan insiden dan permintaan layanan TI tidak diawasi serta tidak mengacu pada standar
Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	*Helpdesk* melakukan kesalahan pencatatan informasi insiden dan permintaan layanan	Terdapat kesalahan pencatatan kategori, tingkat prioritas, identitas pelapor, tanggal kejadian, status insiden atau permintaan layanan TI
Pengguna enggan memberikan *feedback* layanan TI	Pengguna tidak memberikan *feedback* terhadap penyelesaian insiden atau pemenuhan permintaan layanan TI yang diajukan	Kinerja *helpdesk* tidak sesuai dengan keinginan pengguna dan pengguna tidak puas terhadap pelayanan
Ketidakpuasan pengguna terhadap layanan yang diberikan	Pengguna atau pelaporan insiden dan permintaan layanan TI tidak puas dengan pelayanan yang diberikan oleh *helpdesk* dalam memenuhi permintaannya	Kinerja unit *helpdesk* tidak sesuai dengan keinginan pengguna

B. Analisis Tipe Risiko

Berdasarkan analisis tipe risiko yang diperoleh, dapat diketahui ada empat risiko terkait *IT Operations and Service Delivery Risk*. Hal ini dikarenakan proses bisnis terkait dengan stabilitas operasional, ketersediaan, perlindungan, dan pemulihan layanan TI, yang dapat membawa penghancuran atau pengurangan nilai bagi layanan SMD, sehingga kedua tipe diisi dengan S (Sekunder), dan P (Primer). Terdapat tiga tipe risiko yang dituliskan pada kolom. Tipe 1 (T1) adalah risiko pemberdayaan manfaat. Tipe 2 (T2) merupakan program TI dan risiko pengiriman proyek. Sedangkan Tip 3 (T3) adalah operasi TI dan risiko penyampaian layanan [2]. Uraian hasil pemetaan tipe risiko dijabarkan dalam Tabel 2.

C. Analisis Kategori Risiko

Setelah dilakukan pemetaan tipe risiko kemudian dilakukan analisis risiko. Penelitian ini hanya mengacu kepada satu kategori risiko, yakni *staff operations* (*human error and malicious intent*) yang mengatur layanan SMD. Hasil analisis kategori risiko dijabarkan dalam bentuk Tabel 3.

Tabel 2. Hasil pemetaan tipe risiko

No	Risiko	T1	T2	T3
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	S	S	P
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	S	S	P
3	Pengguna enggan memberikan *feedback* layanan TI	S	S	P
4	Ketidakpuasan pengguna terhadap layanan yang diberikan	S	S	P

Tabel 3. Hasil analisis kategori risiko

No	Kategori Risiko	Risiko
1	*Staff Operation*	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk
		Kesalahan pencatatan *(logging)* insiden atau permintaan layanan
		Pengguna enggan memberikan *feedback* layanan TI
		Ketidakpuasan pengguna terhadap layanan yang diberikan

D. Faktor Risiko

Faktor risiko terjadi saat pengelolaan permintaan layanan sedang berlangsung. Faktor risiko dibagi menjadi dua, yaitu faktor internal dan faktor eksternal. Faktor internal membahas mengenai kenapa risiko itu terjadi dalam perusahaan. Sedangkan faktor eksternal dilihat dari sisi luar perusahaan yang dapat mengancam layanan SMD. Faktor risiko dijabarkan pada Tabel 4.

E. Skenario Risiko TI

Hasil pembuatan skenario risiko TI digunakan untuk menentukan nilai dampak risiko layanan SMD. Skrenario risiko dapat berupa skenario positif dan skenario negatif. Tabel 5 merupakan hasil pembuatan skenario risiko TI.

F. Penilaian Risiko TI

Setelah diketahui nilai dampak pada risiko serta nilai frekuensi, kemudian dilakukan perhitungan rata-rata nilai dampak pada layanan SMD. Kemudian, keseluruhan hasil jumlah dibagi empat (kuesioner nilai dampak layanan sistem) sesuai aturan COBIT 5 *for risk*. Apabila hasil dari pembagian angkanya berupa desimal, maka mengikuti aturan pembulatan desimal. Jika nilai desimal di bawah angka 0,5 maka akan

dibulatkan ke angka di bawah satu digit berarti menjadi 0,0. Sedangkan nilai desimal di atas angka 0,5 maka dibulatkan ke angka di atas satu digit yang berarti menjadi angka 1.

Tabel 4. Hasil faktor risiko

No	Risiko	Faktor Internal	Faktor Eksternal
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	Terciptanya prosedur yang mengharuskan *helpdesk* untuk mencatat	Tingginya standar layanan TI di organisasi lain yang mempengaruhi standar
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	Kesalahan dalam pencatatan operasional pengelolaan permintaan dan insiden	Perkembangan teknologi untuk *helpdesk* dalam mengelola pencatatan pelaporan
3	Pengguna enggan memberikan *feedback* layanan TI	Tidak terciptanya budaya berorientasi kepada kepuasan pengguna	Tingginya standar layanan TI di organisasi lain
4	Ketidakpuasan pengguna terhadap layanan yang diberikan	*Helpdesk* tidak melaksanakan operasional layanan sesuai standar	Tingginya standar layanan TI di organisasi lain

Uraian hasil perhitungan nilai frekuensi dijabarkan dalam bentuk Tabel 6. Sedangkan Tabel 7 merupakan hasil kuesioner nilai dampak produktivitas. Hasil kuesioner nilai dampak biaya kerugian atau keutungan akibat risiko yang terjadi pada layanan SMD disajikan pada Tabel 8. Hasil kuesioner nilai dampak keunggulan kompetitif dihitung berdasarkan nilai rata-rata (*mean*) kuesioner keunggulan kompetitif yang telah diisi oleh karyawan perusahaan. Hasil ini ditampilkan pada Tabel 9.

Hasil kuesioner nilai dampak akibat risiko yang terjadi hingga sampai ke hukum dapat dilihat pada Tabel 10. Sedangkan Tabel 11 merupakan hasil perhitungan nilai dampak yang terdiri dari dampak produktivitas (D1), dampak biaya kerugian akibat risiko (D2), dampak keunggulan kompetitif (D3) serta dampak hukum yang berakibat pidana (D4).

Setelah hasil penilaian dampak risiko diselesaikan, selanjutnya dilakukan penentuan tingkatan risiko dengan menggabungkan nilai dampak dengan nilai frekuensi sehingga menghasilkan tingkatan risiko. Rincian penentuan tingkatan risiko diuraian pada Tabel 12. Berdasarkan tingkatan risiko, dapat diketahui level atau tingkatan risiko yang terjadi sebagai berikut:

1. Risiko yang memiliki tingkatan *high* paling banyak berada di kategori *staff operations* (*human error and malicious intent*), yaitu sebanyak satu risiko.
2. SMD memiliki 2 risiko tingkat medium, yakni risiko *helpdesk* tidak mencatat permintaan layanan TI yang masuk dan kesalahan pencatatan (*logging*) insiden atau permintaan layanan.
3. Terakhir risiko yang berada dalam tingkat *low* ialah risiko ketidakpuasan pengguna terhadap layanan yang diberikan.

Tabel 5. Hasil pembuatan skenario risiko TI

No	Risiko	Skenario Positif	Skenario Negatif
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	Data insiden tercatat lengkap memudahkan identifikasi dan penanganan insiden atau permintaan layanan TI	Kesulitan dalam mengidentifikasi dan menangani insiden atau permintaan layanan TI karena mengabaikan pencatatan insiden sehingga data tidak lengkap
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	Proses penanganan insiden dan permintaan layanan TI berjalan dengan baik sesuai harapan pengguna	Proses penanganan insiden menjadi tidak tepat dikarenakan adanya kesalahan
3	Pengguna enggan memberikan *feedback* layanan TI	*Helpdesk* bisa meningkatkan kinerjanya berdasarkan kritik dan saran dari pengguna	*Helpdesk* tidak ada gambaran mengenai kritik dan saran pengguna sebagai masukan untuk meningkatkan kinerjanya
4	Pengguna tidak puas terhadap layanan yang diberikan	Berkurangnya komplain pengguna dan meningkatkan kepercayaan pengguna terhadap layanan *Helpdesk*	Pengguna kecewa sehingga tidak menggunakan layanan *Helpdesk* lagi

G. Respons Terhadap Risiko

Pemberian respons terhadap risiko dilakukan setelah penilaian risiko telah diselesaikan. Respons terhadap risiko dapat berupa *acceptance* (menerima risiko), *mitigate* (mitigasi risiko), *avoidance* (menghindar risiko), *share/transfer* (membagi risiko) [7]. Hasil kuesioner respons terhadap risiko diuraikan pada Tabel 13.

Tabel 6. Hasil perhitungan nilai frekuensi

No	Risiko	Nilai Frekuensi
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	2
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	3
3	Pengguna enggan memberikan *feedback* layanan TI	4
4	Pengguna tidak puas terhadap layanan yang diberikan	1

Tabel 7. Hasil kuesioner nilai dampak produktivitas

No	Risiko	Produktivitas
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	1
2	Kesalahan pencatatan (*logging*) insiden atau permintaan layanan	1
3	Pengguna enggan memberikan *feedback* layanan TI	1
4	Pengguna tidak puas terhadap layanan yang diberikan	1

Tabel 8. Hasil kuesioner nilai dampak biaya kerugian atau keuntungan akibat risiko yang terjadi pada layanan SMD

No	Risiko	Biaya Tanggapan
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	1
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	1
3	Pengguna enggan memberikan *feedback* layanan TI	1
4	Pengguna tidak puas terhadap layanan yang diberikan	1

Tabel 9. Hasil kuesioner nilai dampak keunggulan kompetitif

No	Risiko	Keunggulan Kompetitif
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	3
2	Kesalahan pencatatan (*logging*) insiden atau permintaan layanan	3
3	Pengguna enggan memberikan *feedback* layanan TI	3
4	Pengguna tidak puas terhadap layanan yang diberikan	4

H. Langkah Mitigasi Risiko

Setelah dilakukan tanggapan terhadap respons risiko, langkah berikutnya adalah melakukan mitigasi terhadap layanan SMD. Langkah mitigasi risiko ini perlu dilakukan agar perusahaan tidak mengalami kerugian yang lebih besar. Langkah mitigasi untuk layanan SMD mengacu pada proses yang dipilih, yaitu APO11 dan DSS01. Uraian langkah mitigasi layanan SMD dijabarkan dalam Tabel 14.

Tabel 10. Hasil kuesioner nilai dampak akibat risiko yang terjadi hingga sampai ke hukum

No	Risiko	Hukum
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	1
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	1
3	Pengguna enggan memberikan *feedback* layanan TI	1
4	Pengguna tidak puas terhadap layanan yang diberikan	1

Tabel 11. Hasil perhitungan nilai dampak

No	Risiko	D1	D2	D3	D4	Hasil
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	1	1	3	1	1,5
2	Kesalahan pencatatan (*logging*) insiden atau permintaan layanan	1	1	3	1	1,5
3	Pengguna enggan memberikan feedback layanan TI	1	1	3	1	1,5
4	Pengguna tidak puas terhadap layanan yang diberikan	1	1	4	1	1,75

Tabel 12. Hasil penentuan tingkatan risiko

No	Risiko	Nilai Dampak	Nilai Frekuensi	Tingkat risiko
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	1,5	3	*High*
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	1,5	3	*Medium*

3	Pengguna enggan memberikan *feedback* layanan TI	1,5	4	*Medium*
4	Pengguna tidak puas terhadap layanan yang diberikan	1,75	1	*Low*

Tabel 13. Hasil kuesioner respons terhadap risiko

No	Risiko	Respons Risiko
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	*Mitigate*
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	*Mitigate*
3	Pengguna enggan memberikan *feedback* layanan TI	*Mitigate*
4	Pengguna tidak puas terhadap layanan yang diberikan	*Mitigate*

Tabel 14. Hasil mitigasi risiko layanan SMD

No	Risiko	Langkah Mitigasi
1	*Helpdesk* tidak mencatat permintaan layanan TI yang masuk	DSS01.01 *Perform Operational Procedures* 1. Melakukan training terhadap *helpdesk* 2. Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten
2	Kesalahan pencatatan *(logging)* insiden atau permintaan layanan	*DSS01.01 Perform Operational Procedures* 1. Memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten 2. Mengevaluasi kegiatan *helpdesk* tiap minggu (1-2x) 3. Melakukan *Training/workshop* untuk *helpdesk*
3	Pengguna enggan memberikan *feedback* layanan TI	*APO11.03 Focus quality management on customers* 1. Analisis pengguna enggan memberi *feedback* 2. Analisis kekurangan *helpdesk* dalam memberikan layanan 3. Identifikasi kebutuhan utama pelanggan. 4. Identifikasi kriteria penerimaan kualitas pelanggan dengan menyelaraskannya terhadap standar kualitas TI
4	Pengguna tidak puas terhadap layanan yang diberikan	*APO11.03 Focus quality management on customers* 1. Identifikasi kebutuhan utama pelanggan. 2. Identifikasi kriteria penerimaan kualitas pelanggan dengan menyelaraskannya terhadap standar kualitas TI. 3. Analisis kekurangan pelayanan yang diberikan oleh SMD

IV. KESIMPULAN

Berdasarkan uraian analisis manajemen risiko layanan SMD di salah satu perusahaan otomotif pada proses APO11 dan DSS01, dapat ditarik kesimpulan, sebagai berikut :

1. Berdasarkan perhitungan nilai dampak dengan nilai frekuensi tingkatan risiko paling tinggi adalah risiko pengguna enggan memberikan *feedback* layanan TI. Tingkat *medium* terdapat dua risiko, yakni risiko *helpdesk* tidak mencatat permintaan layanan TI yang masuk dan kesalahan pencatatan (*logging*) insiden atau permintaan layanan. Sedangkan tingkat *low*, yaitu risiko pengguna tidak puas terhadap layanan yang diberikan.
2. Langkah mitigasi yang direkomendasikan berdasarkan proses DSS01, antara lain perusahaan perlu memelihara dan menjalankan kebijakan, prosedur dan operasional dan tugas operasional secara andal dan konsisten, melakukan evaluasi kegiatan *helpdesk* tiap minggu, melakukan *training/workshop* untuk *helpdesk*.
3. Langkah mitigasi yang direkomendasikan berdasarkan proses APO11, antara lain perusahaan perlu melakukan analisis risiko dan identifikasi kebutuhan utama pelanggan serta identifikasi kriteria penerimaan kualitas pelanggan dengan menyelaraskannya terhadap standar kualitas TI.

DAFTAR PUSTAKA

[1] F. Husaini, A. Ambarwati, and L. Junaedi, “Analisis Risiko Aset TI Menggunakan Metode Octave Pada SWD Resto,” in *SENASIF 3*, vol. 3, 2019.

[2] H. M. Astuti, F. A. Muqtadiroh, E. W. Tyas Darmaningrat, and C. U. Putri, “Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk,” *Procedia Comput. Sci.*, vol. 124, 2017.

[3] ISACA, *A Business Framework for the Governance and Management of Enterprice IT*. USA: ISACA. 2012.

[4] G. Stoneburner, A. Goguen, and A. Feringa, *Risk Management Guide for Information Technology Systems : Recommendations of the National Institute of Standards and Technology*, *NIST*.

USA: Department of Commerce, 2002.
[5] ISACA, *COBIT 5: Enabling Information*. Rolling Meadows, Ill.: ISACA, 2013.
[6] ISACA, *COBIT 5 Enabling Processes*. USA : ISACA. 2012.
[7] ISACA, *COBIT 5 for Risk*. USA : ISACA. 2013.
[8] K. P. D. Dharmayanti, I. P. A. Swastika, and I. G. L. A. Raditya Putra, "Tata Kelola Sistem Informasi Sanken Menggunakan Framework COBIT 5," *MATRIK J. Manaj. Tek. Inform. Dan Rekayasa Komput.*, vol. 18, no. 1, 2018.
[9] A. M. Mayasari and Y. Kusumawati, "Implementasi Domain Deliver, Service And Support (DSS05) Berdasarkan COBIT 5 Sebagai Upaya Proteksi Aset Informasi Pada PT Astragraphia TBK," in *Seminar Nasional Teknologi Informasi dan Komunikasi Terapan,* 2015.
[10] W.-H. Tsai, C.-L. Hsieh, C.-W. Wang, C.-T. Chen, and W.-H. Li, "The impact of IT management process of COBIT 5 on internal control, information quality, and business value," in Singapore 2015 *IEEE International Conference on Industrial Engineering and Engineering Management (IEEM)*, 2015.
[11] V. Jarsa and K. Christianto, "IT Governance Audit with COBIT 5 Framework on DSS Domain," *Kinet. Game Technol. Inf. Syst. Comput. Netw. Comput. Electron. Control*, vol. 3, no. 4, 2018.