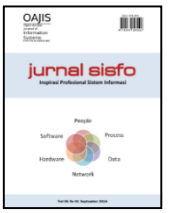
OAJIS
Open Access
Journal of
Information
Systems
is.its.ac.id/pubs/oajis/

jurnal sisfo

Jurnal Sisfo Vol. 06 No. 01 (2016) 105–120



Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002

Wildan Radista Wicaksana, Anisah Herdiyanti*, Tony Dwi Susanto

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

Abstract

Surabaya has been adopting e-government within its administration process. Among those adoptions, one of its unit namely Bina Program Kota Surabaya developed Government Resources Management Systems (GRMS) to support government activities in all government units in Surabaya. The implementation of the system is important and so is the effective use of the system. To be able to ensure the effective use of the system, a standard operating procedure (SOP) is required. This research focuses on the governance-side of the GRMS by developing an SOP for access management to support e-Performance – one of the GRMS applications. E-performance system is complex in nature because it involves a number of users from various users' level application. In order to develop an SOP for access management, gap analysis were conducted by identifying the missing process between existing and expected (ideal) situation for managing access. Following this, step-by-steps to manage access based on the level of access rights were developed within the SOP. All of the six SOPs resulted from this study have been reviewed and simulated within Bina Program. The SOPs for access management has given a standard to manage access rights in order to avoid ambiguities, and further misuse of data and information.

Keywords: Standard Operating Procedure, Access Management, GAP Analysis, ITIL V3, ISO 27002

Abstrak

Salah satu diantara aplikasi yang dikembangkah oleh Bagian Bina Program Pemerintah Kota Surabaya adalah aplikasi E-Performance. Aplikasi ini memungkinkan kontrol kinerja individu di masing-masing Satuan Kerja Perangkat Daerah (SKPD). Terlepas dari kompeksitas aplikasi karena melibatkan berbagai level pengguna aplikasi yang berbeda, aplikasi E-Performance belum dilengkapi dengan standar penyelenggaraan proses dalam mengelola level hak akses. Diantara permasalahan yang timbul terjadinya redudansi peran (roles) yang berpotensi penyalahgunaan wewenang. Sebuah prosedur operasional standar (SOP) dapat memastikan perilaku pengguna terhadap sistem sesuai dengan standar yang diacu. Penelitian ini berfokus kepada pembuatan SOP untuk manajemen akses yang dibangun melalui analisis kesenjangan kondisi kekinian dengan kondisi ekspektasi (ideal). Selanjutnya langkah-langkah dalam pengelolaan akses dideskripsikan ke dalam dokumen prosedur dan formulir. Hasil dari penelitian ini berupa 6 (enam) prosedur dan 12 formulir. Dengan adanya dokumen SOP tersebut diharapkan dapat mengontrol penggunaan aplikasi berdasarkan level hak akses yang dimiliki oleh pengguna sekaligus melindungi aset informasi yang bersifat rahasia.

Kata kunci: Standar Operasional Prosedur, Manajemen Akses, Analisis Kesenjangan, ITIL V3, ISO 27002

Histori Artikel : Disubmit 15 Juli 2016; Diterima 16 September 2016; Tersedia online 16 September 2016

*Corresponding Author
Email address: anisah.herdiyanti@gmail.com (Anisah Herdiyanti)

1. Pendahuluan

Dalam mengoptimalkan kinerja aparatur Pemerintah Kota Surabaya dalam rangka penyelenggaraan Pemerintahan serta memberikan pelayanan kepada masyarakat maka perlu didukung dengan adanya pemanfaatan teknologi informasi dan komunikasi yang memadai [1]. Oleh karenanya, Pemerintah Kota Surabaya mencanangkan penerapan *E-Government* dalam proses pemerintahan dan mendirikan sebuah fungsi internal dalam pemerintahan, yang dinamakan Bagian Bina Program Kota Surabaya. Dalam mendukung fungsi dan tugasnya, Bagian Bina Program Kota Surabaya membuat sebuah sistem yang dinamakan *Government Resources Management Systems* (GRMS). Sistem ini terdiri atas enam sistem yang saling terintegrasi, yaitu *E-Budgeting*, *E-Project*, *E-Procurement*, *E-Delivery*, *E-Controlling*, dan *E-Performance* [2]. Saat ini Bina Program telah memiliki sertifikasi ISO 27002:2005 pada aplikasi *E-Procurement* dan berusaha meningkatkan layanan pada sistem-sistem yang lain. Namun di dalam penerapannya, sistem-sistem ini memerlukan sebuah standard operasional prosedur (SOP) yang dapat mengontrol perilaku organisasi terhadap sistem. Salah satu bentuk penerapan SOP dapat digunakan dalam pengelolaan manajemen akses.

Adanya manajemen akses pada aplikasi dapat mengurangi terjadinya penyalahgunaan hak akses oleh pihak tertentu dan penyalahgunaan data dan informasi didalamnya [3]. Selain itu dapat melindungi data dan informasi yang bersifat rahasia dan hanya pihak tertentu saja yang dapat mengaksesnya. Salah satu sistem yang berkaitan dengan kinerja pegawai Pemkot Surabaya dan memerlukan manajemen akses adalah aplikasi *E-Performance*. *E-Performance* merupakan sistem informasi manajemen kinerja dalam rangka penilaian prestasi kinerja pegawai yang lebih objektif, terukur, akuntabel, partisipatif dan transparan, sehingga terwujud manajemen pegawai berdasarkan prestasi kerja dan sistem karir kerja Pegawai Negeri Sipil (PNS) di lingkungan Pemerintah Kota Surabaya [4]. Penggunaan aplikasi *E-Performance* saat ini juga tak luput dari permasalahan. Permasalahan pertama adalah dapat terjadinya penyalahgunaan hak akses oleh beberapa admin SKPD yang memiliki hak akses yang sama. Permasalahan kedua adalah apabila terdapat kesalahan pemberian hak akses maka dapat mempengaruhi penilaian kinerja pegawai dan mempengaruhi tunjangan gaji yang diterima pegawai. Permasalahan ketiga adalah informasi di dalam aplikasi bersifat rentan dan rahasia, sehingga perlu dilakukan pencegahan terkait dengan hak akses. Permasalahan keempat adalah ketidakjelasan proses komunikasi antara admin SKPD dan Super Admin Bina Program perihal manajemen akses.

Keempat permasalahan tersebut harus diatasi karena jumlah SKPD di Kota Surabaya sebanyak 72 unit dan pengguna aplikasi E-Performance sebanyak 7777 orang yang terbagi kedalam 6 level pengguna [5]. Banyaknya level pengguna tersebut menyebabkan kerentanan terhadap keamanan informasi di dalam aplikasi *E-Performance*. Adapun kerentanan informasi berkaitan dengan 3 aspek keamanan informasi, yaitu *Integrity* dan *Availability* [6]. Selain itu manajemen akses pada aplikasi *E-Performance* akan berpengaruh pula pada pemberian tunjangan kinerja Pegawai Negeri Sipil Daerah (PNSD) Kota Surabaya. Untuk menyelesaikan permasalahan tersebut maka diperlukanlah SOP manajemen akses yang berkaitan dengan pengelolaan hak akses pada aplikasi *E-Performance*. Dalam pembuatan SOP, digunakanlah metode analisis kesenjangan dengan melihat kondisi kekinian layanan pada Bagian Bina Program terhadap kondisi ekspektasi maupun kondisi ideal sesuai dengan kerangka kerja. Dalam melakukan peyusunan dokumen SOP, digunakan acuan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan dalam menyusun kriteria dan format SOP yang ada di dalam dokumen SOP [7]. Pembuatan SOP juga mengacu pada kerangka kerja mengenai manajemen akses yang ada, yaitu proses *Access Management* ITIL V3 pada tahap *service operation* dan kontrol akses pada ISO 27002 yang berkaitan dengan keamanan informasi. Penggunaan ISO 27002:2005 didasarkan pada sertifikasi ISO 27002 yang telah diperoleh Bina Program pada aplikasi *E-Procurement*. Dengan adanya SOP diharapkan dapat meningkatkan layanan pada aplikasi *E-Performance* Bagian Bina Program Kota Surabaya.

2. Tinjauan Pustaka

2.1. Aplikasi E-Performance Bina Program Kota Surabaya

Aplikasi *E-Performance* adalah salah satu aplikasi dalam *Management Government Resources Management Systems (GRMS).* Aplikasi *E-Performance* merupakan sistem informasi manajemen kinerja dalam rangka penilaian prestasi kinerja pegawai yang lebih objektif, terukur, akuntabel, partisipatif dan transparan, sehingga terwujud manajemen pegawai berdasarkan prestasi kerja dan sistem karir kerja Pegawai Negeri Sipil (PNS) di lingkungan Pemerintah Kota Surabaya [4].

Manfaat aplikasi *E-Performance* antara lain:

1) Tersedianya database Pegawai Negeri Sipil Daerah (PNSD) di Lingkungan Pemerintah Kota Surabaya.
2) Alat untuk melakukan monitor aktivitas Pegawai Negeri Sipil Daerah (PNSD) di Lingkungan Pemerintah Kota Surabaya.
3) Alat untuk mengukur kinerja Pegawai Negeri Sipil Daerah (PNSD) di Lingkungan Pemerintah Kota Surabaya.

2.2. Standard Operating Procedure

Menurut Griffin, Standar Operasional Prosedur (SOP) merupakan suatu standar perencanaan yang menguraikan langkah-langkah yang harus dilaksanakan pada keadaan tertentu [8]. SOP merupakan serangkaian panduan yang disusun secara sistematis mengenai proses, tugas, dan peran dari masing-masing individu atau kelompok yang dilakukan sehari-hari dalam suatu organisasi. Dengan adanya SOP maka aktivitas yang dilakukan akan terstandarisasi dan memudahkan dalam transparansi serta akuntabilitas di organisasi. Selain itu adanya SOP juga memberikan arahan kerja berupa konsep yang jelas serta pihak yang bersangkutan.

Beberapa manfaat yang didapatkan dalam penerapan SOP diantaranya:

1) Dapat menstandarkan aktivitas yang dilakukan oleh pihak yang bersangkutan
2) Dapat meningkatkan efisiensi dan efektivitas pelaksanaan tugas dan tanggung jawab oleh pihak yang melaksanakan tugas
3) Dapat mengurangi kesalahan yang mungkin dilakukan dalam melakukan aktivitas
4) Dapat menjelaskan secara detail semua kegiatan dalam suatu proses secara lebih jelas dan terperinci
5) Dapat memudahkan komunikasi antara pihak-pihak terkait
6) Dapat menciptakan ukuran standar kinerja bagi penilaian kinerja pihak yang bersangkutan
7) Dapat memberikan informasi dalam upaya peningkatan kinerja pegawai

2.3. Access Management

Access Management merupakan salah satu proses pada ITIL V3 yang terletak dalam tahapan *Service Operation*. Manajemen akses merupakan proses pengklasifikasian akses pada pengguna layanan dengan memberikan hak akses kepada pengguna yang berhak dan pencegahan pemberian hak akses kepada pengguna yang tidak berhak [3]. Manajemen akses selayaknya sebuah aturan tentang bagaimana sebuah layanan dapat digunakan untuk *user* tertentu.

Tujuan dari manajemen akses meliputi:

1) Mengelola penggunaan pemberian akses terhadap layanan, data, maupun fungsi tertentu

2) Mengatur pemberian hak akses kepada pengguna agar pengguna dapat mengakses layana secara efektif dan sesuai dengan hak akses yang diberikan
3) Menghapus akses ketika pengguna berganti pekerjaan atau tanggung jawab
4) Melindungi keamanan informasi dan data yang terdapat dalam layanan TI.
5) Dapat mempermudah ketika melakukan audit layanan TI

2.4. Klausul ISO/IEC 27002:2005

Standar ISO/IEC 27002:2005 merupakan standar mengenai keamanan informasi. Standar ini memberikan panduan dalam perencaan dan implementasi suatu program untuk melindung aset-aset informasi, salah satunya adalah data di dalam aplikasi [9]. ISO/IEC 27002 menyediakan rekomendasi *best practice* terhadap manajemen keamanan informasi yang dapat digunakan dalam proses inisiasi, implementasi, dan pemeliharaan *Information Security Management Systems* (ISMS) pada suatu organisasi.

2.5. Analisis Kesenjangan

Analisis kesenjangan dapat mengidentifikasi proses-proses yang kurang efektif sehingga dapat mengurangi kesenjangan agar tercapainya kondisi yang diharapkan. Tujuan dari analisis kesenjangan adalah untuk mencapai kondisi yang diharapkan oleh organisasi sehingga tujuan dari organisasi dapat tercapai.

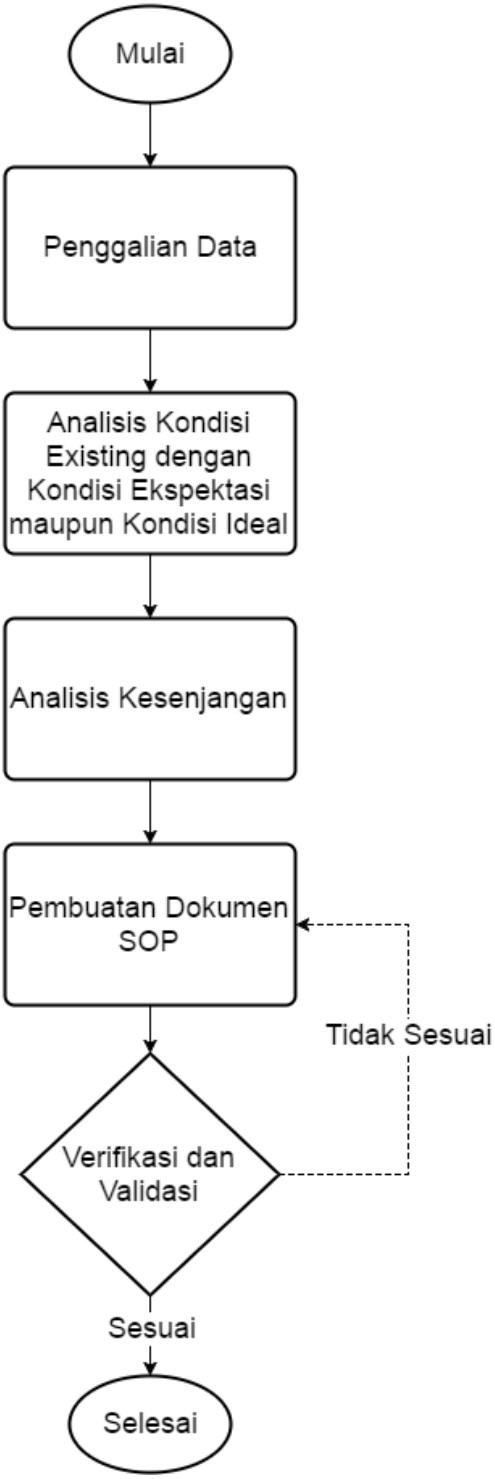
3. Metodologi

Metodologi penelitian merupakan acuan bagi peneliti dalam melakukan penelitian sehingga alur penelitian dapat terstruktur. Gambar 1 merupakan metodologi penelitian ini. Tahap Penggalian Data merupakan tahap pertama dalam penelitian. Dalam tahap ini, peneliti akan melakukan pengumpulan data dan informasi yang terkait dengan penelitian. Di dalam tahap ini terdapat dua proses yang dilakukan, yaitu menyusun *interview protocol* dan menggali kondisi *existing*. Tahap kedua adalah Analisis Kondisi *Existing* dengan Kondisi Ekspektasi maupun Kondisi Ideal. Tahapan ini bertujuan untuk memetakan kondisi *existing* serta hasil kondisi kekinian yang telah terverifikasi dengan kondisi ideal berdasarkan kerangka kerja manajemen akses ITIL V3 dan ISO/IEC 27002:2005. Dari hasil pemetaan yang dilakukan akan didapatkan analisis proses pada kondisi existing terhadap kondisi ekspektasi atau kondisi ideal. Menurut manajemen akses ITIL V3, kondisi ideal dalam manajemen akses mencakup tujuh aktivitas yang perlu dilakukan, yaitu: *request access, verification, providing rights, monitoring identity status, removing or restricting access*, dan *logging and tracking*.

Dalam tahap ketiga, yaitu Tahap Analisis Kesenjangan, peneliti melakukan analisis kesenjangan dengan menggunakan hasil analisis proses pada kondisi *existing* terhadap kondisi ideal yang selanjutnya dilakukan analisis gap. Selain itu di dalam aktivitas ini dilakukan relevansi antara hasil proses yang mengalami kesenjangan dengan kontrol-kontrol yang ada di dalam ISO 27002:2005. Karena di dalam tabel analisis kesenjangan hanya menjelaskan kesenjangan antara proses dalam bisnis dengan proses *Access Management*. Sehingga relevansi antara hasil proses yang mengalami kesenjangan dengan kontrol-kontrol ISO 27002 digunakan untuk mendapatkan prosedur yang sesuai dan sebaiknya dilakukan.

Pada tahap keempat, peneliti menggunakan pedoman pembuatan SOP dalam melakukan pembuatan dokumen SOP. Peneliti menggunakan acuan Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan dalam menyusun kriteria dan format SOP yang ada di dalam dokumen SOP [9]. Selain itu, dalam melakukan pembuatan dokumen SOP manajemen akses, peneliti menggunakan tabel analisis kesenjangan yang telah dilakukan sebelumnya. Adapun prosedur yang terdapat dalam dokumen SOP mencakup tujuh aktivitas dalam melakukan manajemen akses seperti yang telah dijelaskan dalam tahap analisis data. Setelah dokumen SOP manajemen akses tersusun, peneliti

melakukan verifikasi dan validasi dokumen SOP manajemen akses sebagai bukti bahwa pembuatan dokumen SOP manajemen akses telah sesuai dengan objek penelitian.



Gambar 1. Metodologi Penelitian

4. Hasil dan Pembahasan

4.1 Penggalian Data Kondisi Existing Manajemen Akses

Pada bagian ini, peneliti melakukan penggalian data terhadap kondisi kekinian dari manajemen akses yang dilakukan terhadap aplikasi *E-Performance*. Dalam melakukan penggalian data, penulis menggunakan teknik wawancara, observasi dan *review* dokumen terkait yang dibutuhkan dalam penelitian. Berikut adalah data dan informasi yang dibutuhkan dalam penelitian :

1) Peraturan /kebijakan pengelolaan akses, terkait dengan keamanan informasi berdasarkan standar acuan kontrol ISO 27002
2) Tentang aplikasi *E-Performance*, terkait dengan pengelolaan hak akses berdasarkan standar acuan manajemen akses ITIL, analisis kesenjangan dan kontrol ISO 27002.
3) Aktor aplikasi *E-Performance*, terkait dengan pengelolaan hak akses berdasarkan standar acuan manajemen akses ITIL
4) *Role* aplikasi *E-Performance*, terkait dengan pengelolaan hak akses berdasarkan standar acuan manajemen akses ITIL
5) Modul di dalam aplikasi *E-Performance*, terkait dengan pengelolaan hak akses berdasarkan standar acuan manajemen akses ITIL
6) Proses penggajian PNSD, terkait dengan keamanan informasi berdasarkan standar acuan kontrol ISO 27002
7) Proses penilaian kinerja PNSD, terkait dengan keamanan informasi berdasarkan standar acuan kontrol ISO 27002
8) Proses mutasi PNSD, terkait dengan pengelolaan hak akses berdasarkan standar cuan manajemen akses ITIL dan kontrol ISO 27002.
9) Alur pembuatan akses aplikasi *E-Performance* saat ini, terkait dengan aktivitas *requesting access, verification* dan *providing rights* pada manajemen akses ITIL
10) Alur pencatatan dan pelacakan akses aplikasi *E-Performance* saat ini, terkait dengan aktivitas *logging and tracking access* pada manajemen akses ITIL
11) Alur pengelolaan akses saat ini, terkait dengan aktivitas *monitoring identity status* dan *removing or restricting rights* pada manajemen akses ITIL
12) Pihak terkait selain aktor aplikasi *E-Performance*, terkait dengan keamanan informasi berdasarkan standar acuan kontrol ISO 27002
13) Alur pembuatan akses aplikasi *E-Performance* yang diharapkan, terkait dengan analisis kesenjangan antara kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal standar acuan
14) Alur pencatatan dan pelacakan akses aplikasi *E-Performance* yang diharapkan, terkait dengan analisis kesenjangan antara kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal standar acuan
15) Alur pengelolaan akses aplikasi *E-Performance* yang diharapkan, terkait dengan analisis kesenjangan antara kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal standar acuan

Setelah mendapatkan data dan informasi yang dibutuhkan, selanjutnya penulis melakukan analisis kondisi kekinian dengan kondisi ekspektasi yang diharapkan oleh Bagian Bina Program maupun Kondisi Ideal standar acuan.

4.2 Analisis Kondisi Existing dengan Kondisi Ekspektasi maupun Kondisi Ideal Manajemen Akses

Pada bagian ini, peneliti melakukan analisis kondisi kekinian dengan kondisi ekspektasi yang diharapkan oleh Bagian Bina Program maupun Kondisi Ideal standar acuan. Dalam melakukan analisis, penulis mengacu pada 4 aspek penting dalam mendesain sebuah layanan TI berdasarkan tahapan *service design* ITIL V3, yaitu *People, Processes, Product* dan *Partners* [10]. Dalam penelitan, penulis menggunakan aspek *people* dan *processes* karena berdasarkan standar, sebuah organisasi dapat merasakan keuntungan dari penggunaan ITIL ketika terdapat kesesuaian dan kejelasan terhadap proses dan pihak yang terkait

dengan proses. Sedangkan di dalam studi kasus yang berfokus pada manajemen akses, kesesuaian proses dan sumber daya terkait menjadi hal yang penting. Oleh karena itu peneliti menggunakan dua aspek dari empat aspek yang digunakan. Sedangkan terkait kondisi ideal manajemen akses, penulis menggunakan acuan ITIL V3 *Access Management.* Tabel 1 merangkum kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal berdasarkan aspek yang digunakan dan aktivitas pada *access management* ITIL V3.

Tabel 1. Kondisi Kekinian dan Kondisi Ekspektasi

Aspek	Aktivitas	Kondisi Kekinian	Kondisi Ekspektasi
Proses	*Requesting Access*	User Baru : PNSD baru yang terdaftar dicatat oleh BKD dan admin SKPD, lalu admin SKPD terkait menyusun list permintaan pengguna baru yang diserahkan melalui email/surat kepada Super Admin Bina Program. BKD juga menyerahkan list PNSD baru kepada Super Admin Bina Program melalui email/surat untuk dicek kesesuaiannya. Jika telah sesuai maka Super Admin akan membuka akses login admin SKPD untuk membuat pengguna baru. User Lama : PNSD yang telah terdaftar memberikan Surat Keputusan kepada admin SKPD melalui email/surat untuk merubah hak akses maupun status pengguna. Apabila SK sesuai dengan permintaan perubahan maka admin SKPD akan melakukan perubahan	User Baru : PNSD baru yang terdaftar dicatat oleh BKD dan admin SKPD. PNSD baru melakukan permintaan akses baru yang selanjutnya akan diterima oleh Service Desk. Service Desk akan mencatat permintaan dan meneruskan nya kepada admin SKPD. Admin SKPD terkait menerima list permintaan pengguna baru dan diserahkan melalui email/surat kepada Super Admin Bina Program. BKD juga menyerahkan list PNSD baru kepada Super Admin Bina Program melalui email/surat untuk dicek kesesuaiannya. Apabila telah sesuai maka Super Admin akan membuka akses login admin SKPD untuk membuat pengguna baru dan melakukan perekaman permintaan akses baru. User Lama : PNSD yang telah terdaftar memberikan Surat Keputusan kepada admin SKPD melalui email/surat untuk merubah hak akses maupun status pengguna. Apabila SK sesuai dengan permintaan perubahan maka admin SKPD akan melakukan perubahan. Admin SKPD mencatat permintaan perubahan akses.
	Verification	Verifikasi dilakukan dengan melakukan pencocokan data antara SK terkait dengan permintaan pengguna. Admin SKPD juga berperan sebagai verifikator permintaan. Selain itu admin SKPD juga melakukan pengecekan basis data pengguna aplikasi E-Performance	Verifikasi dilakukan dengan melakukan pencocokan data antara SK terkait dengan permintaan pengguna. Admin SKPD juga berperan sebagai verifikator permintaan. Sedangkan Super Admin maupun Tim Manajemen Kinerja berperan sebagai validator dari akses yang dibuat oleh admin SKPD. Selain itu admin SKPD juga melakukan pengecekan basis data pengguna aplikasi *E-Performance*
	Providing rights	Pemberian hak akses aplikasi E-Performance dilakukan oleh admin SKPD terkait kepada pengguna baru/lama dengan menggunakan email/surat.	Pemberian hak akses aplikasi *E-Performance* dilakukan oleh admin SKPD terkait kepada pengguna baru/lama dengan menggunakan email/surat beserta rincian kebijakan serta modul yang dapat diakses maupun yang tidak dapat diakses. Selain itu adanya perekaman pemberian akses

Aspek	Aktivitas	Kondisi Kekinian	Kondisi Ekspektasi
			yang telah dilakukan.
	Monitoring identity status	Pemantauan status identitas dilakukan bersamaan dengan proses pencatatan dan pelacakan akses.	Adanya pemantauan status identitas akses secara berkala, terutama pada proses pengisian tes perilaku kerja untuk tipe aktor tertentu.
	Removing or restricting rights	Admin SKPD maupun Super Admin menggunakan SK pengguna terkait sebagai dasar dalam melakukan penghapusan maupun pembatasan akses. Namun data PNSD yang telah dihapus tidak hilang secara permanen.	Admin SKPD maupun Super Admin menggunakan SK pengguna terkait sebagai dasar dalam melakukan penghapusan maupun pembatasan akses. Namun data PNSD yang telah dihapus tidak hilang secara permanen. Selain itu, adanya perekaman penghapusan akses dan verifikasi serta validasi oleh Tim Manajemen Kinerja.
	Logging and tracking accesss	Secara otomatis sistem akan melakukan pencatatan log akses sistem oleh pengguna. Selain itu proses pencatatan dan pelacakan dilakukan ketika dibutuhkan.	Sistem akan melakukan pencatatan tidak hanya log akses sistem saja, namun terdapat log histori akses modul. Dari penggunaan log akses dapat diketahui pemetaan akses pengguna aplikasi. Serta terdapat alur dalam melakukan pelaporan permasalahan akses

Dalam aspek *people*, terdapat 2 tipe aktor dan 6 tipe *role* dari aplikasi. Adapun 2 tipe aktor adalah Pejabat Struktural dan Pejabat Non Struktural, sedangkan 6 tipe *role* adalah Super Admin Bina Program, Admin SKPD, Pejabat Level 1, Pejabat Level 2, Pejabat Level 3 dan Pegawai Level 4. Setelah melakukan analisis kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal, penulis melakukan analisis kesenjangan.

4.3 Analisis Kesenjangan Kondisi Existing dengan Kondisi Ekspektasi maupun Kondisi Ideal Manajemen Akses

Pada bagian ini, penulis melakukan analisis kesenjangan untuk mengetahui kelemahan atau kekurangan dari kondisi kekinian terhadap kondisi ekspektasi maupun kondisi ideal berdasarkan standar acuan. Analisis kesenjangan juga dapat mengidentifikasi proses-proses yang kurang efektif sehingga dapat mengurangi kesenjangan agar tercapainya kondisi yang diharapkan [11]. Caranya adalah dengan membandingkan kondisi kekinian dengan kondisi ekspektasi maupun kondisi ideal. Dari hasil kesenjangan yang ada akan didapatkan usulan-usulan yang dapat digunakan sebagai *input* dalam membuat dokumen *Standard Operating Procedure* Manajemen Akses Aplikasi *E-Performance*. Selain itu dengan adanya analisis kesenjangan akan didapatkan perubahan, dampak dan solusi atas kesenjangan yang terjadi. Tabel 2 memaparkan mengenai analisis kesenjangan.

Tabel 2. Analisis Kesenjangan

Aspek	Aktivitas	Kesenjangan Proses	Perubahan
Proses	*Requesting Access*	Diperlukan perekaman terhadap permintaan akses baru dan permintaan terhadap perubahan akses	Terdapat kebutuhan dalam pendokumentasian permintaan akses dan perubahan struktur organisasi

Aspek	Aktivitas	Kesenjangan Proses	Perubahan
	Verification	Adanya validator akses sebagai bukti akses telah terverifikasi dan dapat berupa tanda tangan validator	Terdapat kebutuhan dalam pendokumentasian verifikasi
	Providing rights	Diperlukan pemberian rincian kebijakan serta modul kepada pegawai dan terdapat perekaman pemberian akses yang telah dilakukan	Terdapat kebutuhan dalam pendokumentasian pemberian akses
	Monitoring identity status	Diperlukan pemantauan status identitias akses secara berkala dan saat proses pengisian tes perilaku kerja	Terdapat kebutuhan dalam pendokumentasi pemantauan identitas akses
	Removing or restricting rights	Adanya perekaman penghapusan akses dan verifikasi serta validasi	Terdapat kebutuhan dalam pendokumentasi penghapusan maupun pembatasan akses
	Logging and tracking accesss	Diperlukan pencatatan terhadap log histori akses modul dan alur pelaporan permasalahan akses	Terdapat kebutuhan dalam pendokumentasi pencatatan dan pelacakan akses serta perubahan struktur organisasi

Dalam aspek *People* tidak terdapat kesenjangan karena kebutuhan akan pengelolaan akses dengan sumber daya manusia yang dimiliki saat ini telah tercukupi. Hal ini berdasarkan standar acuan proses *Change Management* pada *service transition* ITIL V3, yang menyatakan bahwa jumlah dan ketersediaan sumber daya manusia yang dibutuhkan bergantung pada perubahan layanan yang terjadi, dan perubahan layanan akan semakin efektif apabila dikerjakan oleh SDM dalam jumlah sedikit [12]. Selain analisis kesenjangan, akan diidentifikasi pula dampak dan perubahan dari adanya identifikasi perubahan pada analisis kesenjangan. Identifikasi dampak diperoleh dari hasil identifikasi perubahan pada analisis kesenjangan. Identifikasi dampak diperlukan untuk mengetahui akibat dari perpindahan kondisi saat ini ke kondisi ekspektasi atau kondisi ideal berdasarkan standar acuan. Selanjutnya akan diidentifikasi solusi dari dampak perubahan yang terjadi, sehingga akan didapatkan manfaat dari perubahan yang terjadi. Adapun hasil identifikasi dampak dan solusi dari analisis kesenjangan dapat dilihat pada Tabel 3.

Tabel 3. Identifikasi Dampak dan Solusi

Aspek	Aktivitas	Dampak atas Proses	Solusi
Proses	*Requesting Access*	Adanya penyusunan prosedur baru yang jelas agar dapat meningkatkan kinerja dan efisiensi organisasi dalam menyelesaikan permintaan akses	Pembuatan prosedur baru terkait permintaan akses untuk semua struktur pengguna aplikasi
		Adanya aktivitas dalam mengambil formulir permintaan akses, mengisikan formulir permintaan akses dan mengembalikan formulir permintaan akses	Pembuatan formulir permintaan akses sesuai dengan konten informasi yang diperlukan serta terdapat bukti tandatangan penanggung jawab

Aspek	Aktivitas	Dampak atas Proses	Solusi
		Adanya penjabaran mengenai penambahan peran masing-masing SDM dalam menangani permintaan akses	Pembuatan usulan tambahan tupoksi baru bagi SDM dalam melakukan penerimaan permintaan akses dengan adanya Service Desk
		Adanya aktivitas untuk mencatat permintaan akses yang masuk dalam formulir perekaman permintaan akses	Pembuatan formulir perekaman permintaan akses sesuai dengan konten informasi yang diperlukan
	Verification	Adanya penyusunan prosedur baru yang terkait dengan bukti berupa SK PNSD terkait dalam melakukan pengecekan kesesuaian data dan bukti validasi oleh validator	Pembuatan prosedur verifikasi akses untuk semua struktur pengguna aplikasi disertai bukti validasi oleh validator
		Adanya penyusunan prosedur baru yang jelas dalam pemberian akses	Pembuatan prosedur baru dalam pemberian akses untuk semua struktur pengguna aplikasi
		Adanya aktivitas dalam memberikan bukti terselesainya pembuatan akses kepada pengguna terkait beserta bukti tanda tangan penanggung jawab	Pembuatan formulir pemberian akses sesuai dengan konten informasi yang diperlukan serta terdapat bukti tandatangan penanggung jawab
	Providing rights	Adanya dokumen tambahan sebagai acuan bagi PNSD terkait atas modul yang dapat diakses dan tidak dapat diakses	Pembuatan dokumen yang berisikan daftar modul yang dapat diakses maupun yang tidak dapat diakses sesuai dengan struktur pengguna
		Adanya dokumen tambahan sebagai acuan bagi PNSD terkait atas kebijakan yang mengikat dalam penggunaan akses beserta sanksi terkait	Pembuatan dokumen yang berisikan daftar kebijakan terkait dalam penggunaan akses beserta informasi pendukung lainnya
		Adanya aktivitas untuk mencatat pemberian akses yang keluar dalam formulir perekaman pemberian akses	Pembuatan formulir perekaman pemberian akses sesuai dengan konten informasi yang diperlukan
		Adanya penyusunan prosedur baru yang jelas agar dapat meningkatkan kinerja dan efisiensi organisasi dalam melakukan pemantauan status identitas pengguna secara berkala	Pembuatan prosedur pemantauan status identitas pengguna secara berkala
	Monitoring identity status	Adanya penambahan prosedur baru dalam melakukan pemantauan status identitas pengguna ketika proses penilaian tes perilaku kerja	Pembuatan prosedur pemantauan status identitas pengguna ketika proses penilaian tes perilaku kerja
		Adanya aktivitas dalam melakukan pencatatan status identitas pengguna dalam formulir perekaman pemantauan status identitas pengguna	Pembuatan formulir perekaman pemantauan status identitas pengguna sesuai dengan konten informasi yang diperlukan
		Adanya kebutuhan akan teknologi baru yang mampu menunjang kinerja SDM dalam melakukan pemantauan status identitas akses pengguna	Penyediaan teknologi terkait agar memudahkan SDM dalam melakukan pemantauan status identitas akses pengguna secara otomatis
	Removing or restricting rights	Adanya perubahan prosedur dalam melakukan penghapusan maupun pembatasan akses	Pembuatan prosedur penghapusan maupun pembatasan akses disertai bukti validasi oleh validator

Aspek	Aktivitas	Dampak atas Proses	Solusi
		Adanya aktivitas dalam mengambil formulir penghapusan maupun pembatasan akses, mengisikan formulir penghapusan maupun pembatasan akses dan mengembalikan formulir penghapusan maupun pembatasan akses	Pembuatan formulir penghapusan maupun pembatasan akses sesuai dengan konten informasi yang diperlukan serta terdapat bukti tandatangan penanggung jawab
		Adanya aktivitas dalam melakukan pencatatan akses yang dihapus dalam formulir perekaman penghapusan maupun pembatasan akses	Pembuatan formulir perekaman penghapusan maupun pembatasan akses sesuai dengan konten informasi yang diperlukan
		Adanya pembuatan prosedur baru terkait pencatatan dan pelacakan akses	Pembuatan prosedur pencatatan dan pelacakan akses
		Adanya dokumen baru yang berisi bukti laporan berdasarkan hasil pemetaan akses pengguna dengan dukungan teknologi terkait	- Pembuatan dokumen yang berisi laporan mengenai hasil pemetaan akses - Penyediaan teknologi terkait untuk melakukan pemetaan akses pengguna aplikasi
	Logging and tracking accesss	Adanya penjabaran mengenai penambahan peran baru masing-masing SDM dalam melakukan pencatatan dan pelacakan akses	Pembuatan usulan tambahan tupoksi baru sebagai SDM dalam melakukan pencatatan dan pelacakan akses
		Adanya aktivitas dalam mengambil formulir pelaporan permasalahan akses, mengisikan formulir pelaporan permasalahan akses dan mengembalikan formulir pelaporan permasalahan akses	Pembuatan formulir pelaporan permasalahan akses sesuai dengan konten informasi yang diperlukan serta terdapat bukti tandatangan penanggung jawab
		Adanya aktivitas dalam melakukan pencatatan atas permasalahan akses yang masuk dalam formulir perekaman permasalahan akses	Pembuatan formulir perekaman permasalahan akses sesuai dengan konten informasi yang diperlukan

4.4 Pembuatan Dokumen SOP Manajemen Akses

Pembuatan *Standard Operating Procedure* disusun berdasarkan hasil analisis kesenjangan yang telah dilakukan. Pembuatan SOP mengacu pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 35 Tahun 2012 Tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan. Dalam penyusunan SOP, penulis menggunakan ISO 27002 sebagai kontrol yang digunakan dalam prosedur. Penentuan kontrol ISO/IEC 27002 yang digunakan dalam prosedur telah disesuaikan dengan relevansi antara aktivitas manajemen akses serta kondisi *existing* maupun kondisi ideal manajemen akses [13].

Tabel 4. Pemetaan Kontrol pada Prosedur

Aktivitas Access Management	Kontrol ISO 27002	Deskripsi Kontrol	Aktivitas pada Prosedur
Requesting Access	*11.2.1 User registration*	- ID pengguna yang bersifat *unique*	- Membuat akun email pegawai dengan domain surabaya.go.id
		- Memastikan pengguna memiliki otorisasi akses	- Membuat akun aplikasi *E-Performance* dengan *username* berdasarkan NIP Pegawai

Aktivitas Access Management	Kontrol ISO 27002	Deskripsi Kontrol	Aktivitas pada Prosedur
			dan *password* awal secara acak
		- Pencatatan pengguna yang melakukan permintaan akses	- Melakukan pencatatan pada formulir perekaman permintaan akses
Verification	*8.1.1 Roles and responsibilities*	- Melakukan pengecekan kesesuaian akses terhadap masing-masing aktor	- Melakukan peninjauan terhadap kesesuaian akses masing-masing aktor dan rolenya dari daftar acuan role
		- Melindungi asset informasi dari akses yang tidak terotorisasi	- Memastikan bahwa role dan akses yang dimiliki pegawai telah sesuai
	11.3.1 Password use	- Menjamin kerahasiaan password	- Memastikan password pegawai telah terenkripsi dan tercatat dalam database
	11.5.2 User identification and authentication	- Melakukan pengecekan ID pengguna dan status pengguna	- Melihat kesesuaian antara SK Pegawai dengan akses yang diberikan kepada pegawai dengan melihat database identitas pegawai
		- Melakukan verifikasi dan otentikasi ID pengguna	- Mengirimkan link verifikasi kepada email pegawai sebagai bukti bahwa akses yang akan diberikan sesuai dengan identitas pegawai
Providing rights	*6.1.5 Confidentiality agreements*	- Memastikan pengguna menyetujui perjanjian kerahasiaan informasi	- Memberikan daftar kebijakan terkait manajemen akses kepada masing-masing pegawai beserta sanksi terkait
	11.2.2 Privilege management	- Memastikan pengguna memahami hak akses yang diperolehnya	- Memberikan daftar modul yang dapat diakses serta yang tidak dapat diakses kepada masing-masing pegawai
			- Menekan link verifikasi yang diberikan kepada pegawai
		- Pencatatan pengguna yang telah diberikan akses	- Melakukan pencatatan pada formulir perekaman pemberian akses
	11.2.3 User password management	- Memastikan pengguna memahami aturan mengenai manajemen password	- Memberikan daftar acuan kepada pegawai mengenai kebijakan dalam penggantian password dan konten password yang sesuai dengan standar acuan
	11.4.1 Policy on use of network service	- Memastikan pengguna memahami kebijakan terkait layanan akses	- Memberikan daftar acuan mengenai layanan akses yang dapat diakses dari jaringan umum maupun khusus
Monitoring identity status	*11.1.1 Access control policy*	- Melakukan pengecekan kesesuaian akses pengguna berdasarkan kebijakan kontrol akses	- Memastikan akses pegawai sesuai dengan kontrol-kontrol dalam acuan

Aktivitas Access Management	Kontrol ISO 27002	Deskripsi Kontrol	Aktivitas pada Prosedur
	11.2.4 Review of user access rights	- Melakukan peninjauan ulang terhadap hak akses pengguna secara berkala	- Melakukan pengecekan akses pegawai secara berkala - Melakukan pencacatan status pegawai dalam proses penilaian tes perilaku kerja - Mencatat hasil pemantauan status identitas dalam formulir
		- Pencatatan perubahan identitas status pengguna	- Melakukan pencatatan pada formulir pemantauan status identitas pengguna
Removing or restricting rights	*8.3.3 Removal of access rights*	- Memastikan hak akses telah dihapus atau dibatasi sesaat setelah kontrak benar-benar selesai	- Melakukan perubahan role berdasarkan SK pegawai terkait - Melakukan pengecekan perubahan role sesuai dengan status identitas pegawai
		- Pencatatan penghapusan maupun pembatasan akses pengguna	- Melakukan pencatatan pada formulir perekaman penghapusan maupun pembatasan akses
	11.6.1 Information access restriction	- Memastikan kontrol akses berdasarkan *read, write, delete* dan *execute*	- Memastikan bahwa role dan akses yang dimiliki pegawai telah sesuai - Melakukan pengecekan perubahan role sesuai dengan status identitas pegawai
Logging and tracking accesss	*11.5.1 Secure logon procedures*	- Memastikan kesesuaian akses pengguna	- Melakukan pengecekan username dan password pegawai ketika mengakses dan memberikan informasi *error* apabila terdapat ketidaksesuaian
		- Menampilkan informasi *warning* yang menyatakan bahwa komputer tersebut hanya dapat diakses oleh pengguna yang terotorisasi	- Melakukan tindakan apabila terdapat laporan permasalahan akses yang tidak sesuai - Melakukan pengecekan log aktivitas pegawai - Melakukan penelusuran terhadap akses yang mencurigakan dengan teknologi terkait
		- Pencatatan perekaman permasalahan akses pengguna	- Melakukan pencatatan pada formulir perekaman permasalahan akses apabila terdapat permasalahan akses

Adapun dalam penyusunan format SOP, didasarkan pada tujuan dari pembuatan SOP dan tidak terdapat format baku dalam penyusunan format SOP [14]. Sehingga apabila terdapat perbedaan tujuan pembuatan SOP, maka format SOP juga akan berbeda. Dalam melakukan pembuatan dokumen SOP, penulis memetakan kontrol yang ada di dalam ISO/IEC 27002:2005 ke dalam aktivitas yang tertera dalam prosedur seperti disajikan dalam Tabel 4.

Setelah melakukan pemetaan kontrol, penulis melakukan penyusunan struktur dan konten SOP sesuai dengan acuan pembuatan SOP. Tabel 5 mendaftar prosedur dan formulir yang terdapat dalam SOP Manajemen Akses aplikasi *E-Performance*.

Tabel 5. Prosedur dan Formulir Dokumen SOP

Nomor SOP	Nama SOP	Nomor Formulir	Nama Formulir
SOP-Akses-001	SOP Permintaan Akses	FRM-Akses-001	Formulir Permintaan Akses
		FRM-Akses-002	Formulir Perekaman Permintaan Akses
SOP-Akses-002	SOP Verifikasi dan Pemberian Akses	FRM-Akses-003	Formulir Pemberian Akses
		FRM-Akses-004	Formulir Perekaman Pemberian Akses
SOP-Akses-003	SOP Pemantauan Status Identitas	FRM-Akses-005	Formulir Perekaman Pemantauan Status Identitas Pengguna
SOP-Akses-004	SOP Pemantauan Akses Tes Perilaku Kerja	FRM-Akses-006	Formulir Perekaman Pemantauan Penilaian Tes Perilaku Kerja
SOP-Akses-005	SOP Penghapusan atau Pembatasan Akses	FRM-Akses-007	Formulir Penghapusan atau Pembatasan Akses
		FRM-Akses-008	Formulir Perekaman Penghapusan atau Pembatasan Akses
SOP-Akses-006	SOP Pencatatan dan Pelacakan Akses	FRM-Akses-009	Formulir Pelaporan Permasalahan Akses
		FRM-Akses-010	Formulir Perekaman Permasalahan Akses
		FRM-Akses-011	Formulir Laporan Pencatatan Akses
		FRM-Akses-012	Formulir Laporan Tindakan Keamanan Informasi

5. Kesimpulan

5.1 Simpulan

Berdasarkan hasil penggalian data, diketahui bahwa terdapat enam role dan dua tipe aktor. Aktor tersebut adalah Pejabat Struktural dan Pejabat Non Struktural. Pejabat Struktural dapat memiliki jenis role Pejabat Level 1, Pejabat Level 2, Pejabat Level 3 maupun Admin SKPD. Sedangkan Pejabat Non Struktural dapat memiliki jenis role Super Admin Bina Program, Admin SKPD dan Pegawai Level 4. Selain itu, dari hasil analisis kesenjangan yang telah dilakukan, didapatkan satu tambahan aktivitas dalam manajemen akses, yaitu terkait pemantauan status saat tes perilaku kerja berlangsung. Dari hasil analisis kesenjangan didapatkan pula adanya perubahan struktur dan peran SDM dalam pengelolaan akses, serta penambahan kebijakan terkait pengelolaan manajemen akses. Di dalam SOP, terdapat beberapa prosedur dan sub prosedur. Dalam menentukan sub prosedur, didasarkan pada perbedaan aktivitas dalam prosedur dan keterlibatan aktor dalam prosedur. Sedangkan dalam menentukan prosedur, didasarkan pada aktivitas manajemen akses sesuai dengan standar acuan. Hasil penelitian berupa dokumen SOP manajemen akses yang telah disesuaikan dengan standar acuan. Di dalam dokumen SOP juga terdapat dua belas formulir, daftar kebijakan manajemen *password*, daftar acuan modul dan daftar acuan *role* yang membantu terlaksananya prosedur manajemen akses. Setelah dokumen SOP selesai disusun, dilakukanlah verifikasi dan validasi SOP untuk memastikan kesesuaian informasi maupun aktivitas yang ada di dalam prosedur, formulir, dan daftar acuan terkait. Setelah dilakukan perbaikan dari hasil verifikasi dan validasi, dokumen

SOP dapat digunakan dalam penerapan manajemen akses aplikasi *E-Performance* oleh Bagian Bina Program Kota Surabaya.

5.2 Saran

Saran yang dapat disampaikan untuk penelitian selanjutnya adalah:

1) Dalam penelitian ini, dilakukan pembatasan terhadap pengidentifikasian kontrol yang terdapat dalam ISO/IEC 27002:2005 sebelum dilakukan analisis kesenjangan. Sehingga yang terjadi adalah terdapat kontrol diluar batasan yang dapat digunakan dalam penelitian. Dalam penelitian selanjutnya,dapat dilakukan pembatasan pengidentifikasian kontrol setelah dilakukan analisis kesenjangan untuk memastikan kontrol sesuai dengan kebutuhan dalam penelitian.
2) Penelitian ini tidak melakukan pemantauan terhadap penggunaan SOP di dalam aktivitas sehari-hari. Untuk penelitian selanjutnya dapat dilakukan penilaian kinerja dan evaluasi terhadap penerapan SOP yang nantinya dapat mengetahui keefektifan SDM terkait dalam menunjang penerapan SOP.

6. Daftar Pustaka

[1] Walikota Surabaya, 2013. Peraturan Walikota Surabaya Nomor 5 Tahun 2013 Tentang Pedoman Pemanfaatan Teknologi Informasi Dan Komunikasi Dalam Penyelenggaraan Pemerintahan Daerah. Surabaya.
[2] Bina Program Kota Surabaya, 2015. Dokumen Profil Bagian Bina Program Kota Surabaya. Surabaya.
[3] UCISA, 2002. ITIL – A Guide to Access Management. University of Oxford.
[4] Pemerintah Kota Surabaya, 2015. E-Performance [Online] .Available at: https://eperformance.surabaya.go.id/2015/. [Accessed 25 January 2016]
[5] Badan Kepegawaian Daerah Kota Surabaya, 2015. Kondisi Umum Kepegawaian [Online] .Available at: http://bkd.surabaya.go.id/content.php?page=10. [Accessed 16 January 2016]
[6] Carrtlidge, Hanna dan Rudd, C., 2007. An Introductory Overview of ITIL® V3, Version 1.0. UK: The UK Chapter of the itSMF.
[7] Badan Kepegawaian Daerah Kota Semarang, 2012. Pedoman Penyusunan Administrasi Pemerintahan. Semarang.
[8] Griffin, R. W., 2004. Manajemen. Jakarta: Erlangga.
[9] International Standard Organization (ISO), 2005. ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls, First Edition. Switzerland.
[10] Office of Government Commerce (OCG), 2007. ITIL Version 3 Service Design. United Kingdom: The Stationery Office.
[11] Murray, J., 2000. A GAP Analysis Process To Improve IT Management. 1 (4), pp.35.
[12] Office of Government Commerce (OCG), 2007. ITIL Version 3 Service Transition. United Kingdom: The Stationery Office.
[13] IT Governance Institute, 2008. Aligning CobiT®4.1, ITIL ®V3 and ISO/IEC 27002 for Business Benefit. United States.
[14] Budihardjo, M., 2014. Panduan Praktis Menyusun SOP. Yogyakarta: Gadjah Mada University Press.

Halaman ini sengaja dikosongkan