Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Pada Government Resources Management Systems (GRMS) Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002 (Studi Kasus : Aplikasi E-Performance Bina Program Kota Surabaya)

Wildan Radista Wicaksana, Tony Dwi Susanto, Anisah Herdiyanti
Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Institut Teknologi Sepuluh Nopember (ITS)
Sukolilo, Surabaya 60111 Indonesia
e-mail: wildan.radista12@mhs.is.its.ac.id tonydwisusanto@is.its.ac.id anisah@is.its.ac.id

Abstrak—Pemerintah Kota Surabaya saat ini sudah menerapkan *E-Government* di dalam proses pemerintahannya. Tak terkecuali terhadap perencanaan keuangan daerah Kota Surabaya yang dilakukan oleh Bagian Bina Program Kota Surabaya. Untuk mendukung proses tersebut Bagian Bina Program menggunakan sebuah sistem yang dinamakan *Government Resources Management Systems* (GRMS). Dalam penerapan sistem ini diperlukanlah sebuah standard operasional prosedur (SOP) yang dapat mengontrol perilaku organisasi terhadap sistem. Apabila tidak ada SOP maka tidak ada prosedur yang terstandar yang mengakibatkan ketidakjelasan dalam aktivitas dari proses yang dijalankan. Penerapan SOP juga dapat digunakan dalam mengelola manajemen akses pada GRMS. Salah satu contoh sistem dalam GRMS adalah aplikasi *E-Performance*. Pentingnya SOP manajemen akses dalam aplikasi *E-Performance* berkaitan erat dengan jumlah pengguna aplikasi dan berbagai level pengguna aplikasi. Dengan adanya SOP manajemen akses maka dapat mengontrol penggunaan aplikasi berdasarkan level hak akses yang dimiliki oleh pengguna serta dapat melindungi aset informasi yang bersifat rahasia. Apabila tidak terdapat manajemen akses maka dapat terjadi penyalahgunaan hak akses yang diberikan dan adanya peluang untuk penyalahgunaan data dan informasi. Berdasarkan permasalahan tersebut maka diperlukan sebuah SOP manajemen akses pada aplikasi *E-Performance*. Penyusunan SOP manajemen akses pada aplikasi *E-Performance* didasarkan pada analisis kondisi kekinian dan kondisi ekspektasi maupun kondisi ideal berdasarkan kerangka kerja ITIL V3 , ISO 27002 serta metode analisis kesenjangan.

***Kata Kunci*—Aplikasi *E-Performance*, *Standard Operating Procedure*, *Access Management*, Analisis Kesenjangan, ITIL V3, ISO 27002**

I. 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, untuk mendukung hal tersebut Pemerintah Kota Surabaya mencanangkan penerapan *E-Government* dalam proses pemerintahannya dan mendirikan sebuah fungsi internal dalam pemerintahan, yang dinamakan Bagian Bina Program Kota Surabaya. Dalam mendukung fungsi dan tugas nya, maka 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. Selain itu penerapan SOP ini juga berkaitan dengan value yang akan didapatkan oleh Bina Program Kota Surabaya.

Adanya manajemen akses pada aplikasi dapat mengurangi terjadinya penyalahgunaan hak akses oleh pihak tertentu dan penyalahgunaan data dan informasi didalamnya. 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 [3]. 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.

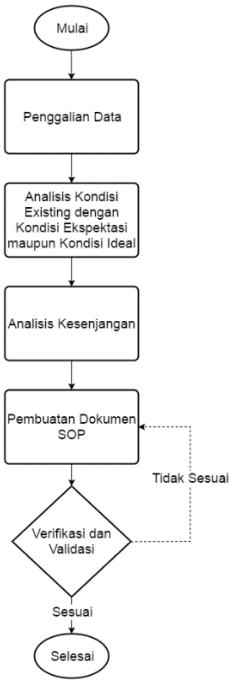
Keempat permasalahan tersebut harus diatasi karena jumlah SKPD di Kota Surabaya sebanyak 72 unit dan pengguna aplikasi E-Performance sebanyak 7777 orang yang terbagi kedalam 6 level pengguna [4]. Banyaknya level pengguna tersebut menyebabkan kerentanan terhadap keamanan informasi di dalam aplikasi *E-Performance*. Adapun kerentanan informasi berkaitan dengan 3 aspek keamanan informasi, yaitu *Integrity* dan *Availability*. Selain itu manajemen akses pada aplikasi *E-Performance* akan berpengaruh pula pada pemberian tunjangan kinerja 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. Pembuatan SOP 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.

II. METODOLOGI PENELITIAN

Metodologi penelitian merupakan acuan bagi peneliti dalam melakukan penelitian sehingga alur penelitian dapat terstruktur. Berikut merupakan metodologi penelitian ini :

Gambar 1. Metodologi Penelitian



III. HASIL PEMBAHASAN

A. 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.

B. 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* [5]. 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.* Berikut adalah 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 : Terdapat sebuah pencatatan atas penerimaan akses baru yang masuk, list akses apa saja yang dihasilkan, serta rekapan penanggung jawab terkait pembuatan akses . User Lama : Terdapat rekapan perubahan akses dan terdapat penanggung jawab terkait perubahan / pembuatan akses pegawai lama.
	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	Terdapat verifikator tambahan untuk memastikan kesesuaian akses yang diberikan
	Providing rights	Pemberian hak akses aplikasi E-Performance dilakukan oleh admin SKPD terkait kepada pengguna baru/lama dengan menggunakan email/surat.	Diberikan dokumen mengenai hak akses modul, kebijakan terkait dalam hak akses.
	Monitoring identity status	Pemantauan status identitas dilakukan bersamaan dengan proses pencatatan dan pelacakan akses.	Terdapat pemantauan pada proses penilaian tes perilaku kerja oleh pejabat level 1, pejabat level 2 dan pejabat level 3
	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.	Terdapat dokumentasi penghapusan maupun pembatasan akses serta verifikasi 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.	Adanya manfaat lebih yang dapat digali berdasarkan log akses aplikasi

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.

C. 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 [6]. 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. Berikut adalah paparan 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 melakukan dokumentasi atas permintaan akses yang meliputi formulir permintaan akses, prosedur permintaan akses beserta penanggung jawab permintaan akses.
	Verification	Adanya validator akses sebagai bukti akses telah terverifikasi dan dapat berupa tanda tangan validator	Terdapat kebutuhan mengenai prosedur dalam melakukan verifikasi data PNSD terkait yang dicocokkan dengan SK dan database existing beserta bukti validasi oleh validator
	Providing rights	Diperlukan pemberian rincian kebijakan serta modul	Terdapat kebutuhan dalam melakukan dokumentasi atas pemberian akses yang meliputi formulir pemberian

Aspek	Aktivitas	Kesenjangan Proses	Perubahan
		kepada pegawai dan terdapat perekaman pemberian akses yang telah dilakukan	akses, prosedur pemberian akses beserta penanggung jawab pemberian akses dan daftar modul yang dapat diakses maupun yang tidak dapat diakses
	Monitoring identity status	Diperlukan pemantauan status identitias akses secara berkala dan saat proses pengisian tes perilaku kerja	Terdapat kebutuhan dalam melakukan dokumentasi atas pemantauan identitas akses yang meliputi prosedur pemantauan identitas akses secara berkala terutama pada proses penilaian tes perilaku kerja
	Removing or restricting rights	Adanya perekaman penghapusan akses dan verifikasi serta validasi	Terdapat kebutuhan dalam melakukan dokumentasi atas penghapusan maupun pembatasan akses yang meliputi formulir penghapusan maupun pembatasan akses, prosedur penghapusan maupun pembatasan akses beserta penanggung jawab penghapusan maupun pembatasan akses
	Logging and tracking accesss	Diperlukan pencatatan terhadap log histori akses modul dan alur pelaporan permasalahan akses	Terdapat kebutuhan dalam melakukan dokumentasi pencatatan dan pelacakan akses yang meliputi prosedur pencatatan dan pelacakan akses yang jelas dan berkaitan dengan eskalasi penyelesaian masalah akses, serta pelaporan hasil pemetaan akses pengguna

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 [7].

D. 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. Adapun dalam penyusunan format SOP, didasarkan pada tujuan dari pembuatan SOP dan tidak terdapat format baku dalam penyusunan format SOP [8]. 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.

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 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

Aktivitas Access Management	Kontrol ISO 27002	Deskripsi Kontrol	Aktivitas pada Prosedur
	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 services	- 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
	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

Setelah melakukan pemetaan kontrol, penulis melakukan penyusunan struktur dan konten SOP sesuai dengan acuan pembuatan SOP. Berikut adalah 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	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

IV. KESIMPULAN DAN SARAN

A. Kesimpulan

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. Selain itu 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. 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.

B. Saran

Saran yang dapat disampaikan untuk penelitian selanjutnya adalah :

- 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.
- 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.

V. DAFTAR PUSTAKA

[1] Walikota Surabaya, “Peraturan Walikota Surabaya Nomor 5 Tahun 2013 Tentang Pedoman Pemanfaatan Teknologi Informasi Dan Komunikasi Dalam Penyelenggaraan Pemerintahan Daerah.” Pemerintah Kota Surabaya, 2013.

[2] Bina Program Kota Surabaya, “Dokumen Profil Bagian Bina Program Kota Surabaya.” Bina Program Kota Surabaya, 2015.

[3] Pemerintah Kota Surabaya, “E-Performance,” 2015. [Online]. Available: https://eperformance.surabaya.go.id/2015/. [Accessed: 25-Jan-2016].

[4] Badan Kepegawaian Daerah Kota Surabaya, “Kondisi Umum Kepegawaian,” 2015. [Online]. Available: http://bkd.surabaya.go.id/content.php?page=10. [Accessed: 16-Jan-2016].

[5] Office of Government Commerce (OCG), *ITIL Version 3 Service Design*. United Kingdom : The Stationery Office, 2007.

[6] J. Murray, “A GAP Analysis Process To Improve IT Management,” *Auerbach*, vol. 1, no. 4, p. 35, 2000.

[7] Office of Government Commerce (OCG), *ITIL Version 3 Service Transition*. United Kingdom : The Stationery Office, 2007.

[8] Badan Kepegawaian Daerah Kota Semarang, “Pedoman Penyusunan Administrasi Pemerintahan.” BKD Kota Semarang, 2012.