Analisis dan Perancangan Kebijakan *Incident Management* pada bidang SIM DISKOMINFOTIK DKI Jakarta Menggunakan COBIT 5

Analysis and Design of Incident Management Policies in the field of DISKOMINFOTIK SIM DKI Jakarta Using COBIT 5

Nurul Asyfa [1], Falahah[2], Fitriyana Dewi[3]

[1,2,3] Universitas Telkom, Bandung
nurulasyfa@telkomuniversity..ac.id[1], falahah@telkomuniversity.ac.id[2], fitrianadewi@telkomuniversity.ac.id[3]

Abstrak

Dinas Komunikasi, Informatika dan Statistik Pemerintah Provinsi DKI Jakarta (DISKOMINFOTIK DKI Jakarta) merupakan penyelenggara urusan pemerintahan dan mempunyai tugas di bidang Komunikasi dan Informatika, Statistik dan Persandian yang memiliki berbagai bidang salah satunya bidang SIM. Pada bidang SIM ini terdapat sebuah layanan teknologi informasi yang mencakup aplikasi, integrasi dan basisdata. Pada instansi belum ada kebijakan yang mengatur penanganan insiden layanan teknologi informasi. Penelitian ini merancang kebijakan menggunakan *framework COBIT 5* dengan domain DSS02 *Manage Service Requests and Incidents* . Proses penelitian ini dimulai dengan melakukan studi literatur, wawancara terkait kondisi eksisting dan melakukan analisis. Hasil yang didapatkan, dari 24 aktivitas yang ada pada domain DSS02 *Manage Service Requests and Incidents* hanya 4 aktivitas yang masih dilakukan walaupun masih belum seutuhnya. Untuk mendekati kondisi ideal sesuai dengan domain DSS02 *Manage Service Requests and Incidents* maka kebijakan yang akan dirancang adalah kebijakan penanganan insiden, kebijakan eskalasi insiden, dan kebijakan penutupan insiden.

Hasil perancangan kebijakan *incident management* dapat digunakan sebagai panduan kerja untuk meningkatkan penanganan insiden. Panduan kerja yang dihasilkan telah sesuai dengan COBIT 5 sehingga dapat digunakan secara langsung sebagai panduan dalam menangani insiden layanan TI.

Kata Kunci : COBIT 5, *incident management,* DISKOMINFOTIK

Abstract

The Department of Communication, Information and Statistics of the DKI Jakarta Provincial Government (DISKOMINFOTIK DKI Jakarta) is the organizer of government affairs and has duties in the fields of Communication and Information, Statistics and Encryption which have various fields in the SIM field. In the field of MIS there is an information technology service that includes applications, integration and databases. In the agency there is no policy that regulates the handling of information technology service incidents. This study designs a policy using the COBIT 5 framework with the domain DSS02 Manage Service Requests and Incidents . The research process begins with conducting literature studies, interviews related to existing conditions and conducting analysis. The results obtained, of the 24 activities in the DSS02 Manage Service Requests and Incidents domain, only 4 activities are still being carried out although they are still incomplete.

To approach the ideal conditions in accordance with the DSS02 Manage Service Requests and Incidents domain, the policies that will be designed are incident handling policies, incident escalation policies, and incident closure policies.

The results of the design of incident management policies can be used as a work guide to improve incident handling. The resulting work guide is compliant with COBIT 5 so that it can be used directly as a guide in dealing with IT service incidents.

Keywords: **COBIT 5, *incident management,* DISKOMINFOTIK**

1. Pendahuluan

Dinas Komunikasi, Informatika dan Statistik Pemerintah Provinsi DKI Jakarta dipimpin oleh seorang Kepala Dinas yang berkedudukan di bawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah yang merupakan penyelenggara urusan pemerintahan dan mempunyai tugas di bidang Komunikasi dan Informatika, Statistik dan Persandian. Instansi ini memiliki tugas dalam memberikan pelayanan dibidang teknologi informasi dan menempatkan teknologi informasi sebagai hal yang sangat mendukung dalam menjalankan kegiatan bisnisnya. Diskominfotik Jakarta memiliki bidang yang salah satunya bidang sistem informasi manajemen yang didalamnya terdapat layanan inisiden yaitu aplikasi, database dan integrsi. Pada bidang SIM saat ini belum memiliki kebijakan *incident management* . Hal ini berdampak pada menurunya kinerja layanan TI dalam memenuhi kebutuhan bisnis.

Hal tersebut menggambarkan bahwa bidang SIM perlu meningkatkan tata Kelola dalam mengelola penanganan insiden. Tahap awal yang dilakukan dalam membangun penanganan insiden dengan membuat perencanaan *incident management* yang mengadopsi seebuah *framework.* Hasil dari perencanaan tersebut dapat digunakan untuk bahan *knowledge base* dan panduan kerja bagi pihak manajemen dalam melakukan proses penanganan inisiden yang terstandarisasi.

Untuk mencegah terjadi resiko yang ada, maka solusi yang yang ditawarkan berupa kebijakan incident management dengan menggunakan framework COBIT 5. Framework COBIT mendukung tata kelola TI dengan menyediakan kerangka kerja untuk mengelola integrasi TI dengan perusahaan. Selain itu, kerangka kerja ini memastikan bahwa TI menjalankan bisnisnya, memaksimalkan keuntungan, mengelola risiko TI dengan tepat, dan menggunakan sumber daya TI secara bertanggung jawab (Tanuwijaya dan Sarno (2010)).

Perancangan kebijakan *incident management framework COBIT 5* dapat mengoptimalkan peran SDM dalam menengani permasalahan insiden dengan tujuan untuk memastikan tingkat terbaik kualitas layanan. Pembuatan prosedur incident management ini menghasilkan standar dan prosedur yang sesuai dengan yang diharapkan. Pembuatan prosedur incident management ini memerlukan *framework COBI*T 5 agar dapat mengatasi permasalahan yang telah disebutkan sebelumnya.

2. Dasar Teori

2.1 Kebijakan Keamanan Teknologi Informasi

Kebijakan adalah sebuah prosedur, cara, atau petunjuk dalam bentuk dokumen yang disusun dengan baik yang berguna untuk menjalankan suatu proses yang sesuai dengan standar yang ditentukan atau ditetapkan.

Kebijakan keamanan teknologi informasi adalah sebuah prosedur , proses dan petunjuk yang dirancang untuk merancang menjalankan sebuah aktivitas dalam bidang keamanan informasi yang sesuai dengan kebutuhan perusahaan. Kebijakan ini sangat penting dilakukan untuk untuk menjaga atau melindungi keamanan teknologi informasi sebuah perusahaan.

Tujuan untuk membuat sebuah kebijakan keamanan dapat meningkatkan keamanan data dan jaringan, melidungi kepemilikan informasi, mencegah resiko penggunaan sumber daya oleh pihak yang tak memliki kewenangan, dan yang lebih penting mengurangi biaya perusahaan.

Ada beberapa tipe – tipe kebijakan keamanan TI, yaitu :

1) Promiscuos Policy, merupakan sebuah kebijakan yang tidak membatasi penggunaan sumber daya yang membuat kebijakn ini sangat tidak direkomendasikan.
2) Permissive Policy, kebijakan membatasi pada bagian tertentu saja.
3) Prudent Policy, adalah kebijakan dengan kemanan yang sangat maksimal. Hanya layanan yang benar – benar dibutuhkan yang dibuka.
4) Paranoid policy, merupakan kebijakan yang membatasi hubungan dengan internet.

2.2 Incident Management

Incident management adalah proses yang bertanggung jawab dalam mengelola siklus hidup semua insiden. Insiden dapat dikenali oleh staf teknis, terdeteksi dan dilaporkan oleh alat bantu komunikasi dari pengguna.

Incident management dilakukan untuk mengembalikan gangguan layanan IT secara normal secepat mungkin untuk meminimalisir dampak buruk terhadap berjalannya proses bisnis. Pengelolaan insiden harus dilakukan secara berkala dan dikomunikasikan oleh service desk. Penyelesaian insiden perlu dikoordinasikan dengan bagian unit bisnis yang lain untuk menetukan prioritas dengan kebutuhan bisnis utama.

2.3 COBIT 5

Control Objective for Information & Related Technology (COBIT) adalah kumpulan praktik terbaik manajemen TI yang dapat membantu auditor, pengguna, dan manajemen menjembatani kesenjangan antara risiko bisnis, kebutuhan kontrol, dan masalah teknis TI. COBIT 5 salah satu kerangka kerja yang mencakup tata kelola dan manajemen TI yang dibangun di atas pengalaman lebih dari 15 tahun menggunakan COBIT oleh bisnis dan pengguna dari bisnis, komunitas TI, risiko, asuransi, dan keamanan. COBIT 5 bersifat generik dan berguna untuk bisnis dari semua ukuran, baik itu sektor komersial, sektor nirlaba, pemerintah, atau sektor publik. COBIT 5 didasarkan pada lima prinsip utama tata kelola perusahaan dan manajemen TI.

COBIT 5 mempunyai lima prinsip kunci untuk tata kelola dan manajemen teknologi informasi perusahaan.

1. *Meeting Stakeholder Needs*
   Pada prinsip ini keberadaan sebuah perusahaan dapat menciptakan nilai atau keuntungan kepada stakeholdernya. Kebutuhan stakeholder harus berubah menjadi strategi praktis perusahaan. Cobit 5 mengartikan kebutuhan stakeholder untuk menjelaskan tujuan dan sasaran yang sesuai dan nyata di berbagai tingkat tanggung jawab.
2. *Covering the Enterprise End-to-End*
   Pada prinisp ini Cobit 5 mengintegrasikan tata kelola TI perusahaan dengan organisasi pemerintahan dengan cara mengakomodasi semua stakeholder, fungsi dan proses yang relevan dengan keamanan informasi.
3. *Applying A Single Intgrated Fmarework*
   Pada prinisp ini Cobit 5 dapat diselaraskan dengan standar framework lainnya seperti :
   - Enterprise : COSO, COSO ERM, ISO/IEC 9000, ISO/IEC 31000
   - IT- related: ISO/IEC 38500, ITIL,ISO/IEC 27000 series, TOGAF
4. *Enabling a Holistic Approach*
   Pada prinsip ini Cobit 5 menjelaskan pedekatan secara holistic atau menyeluruh yang dibutuhkan oleh pemerintahan dan manajemen IT yang efektif dan efisien. Pada Cobit 5 terdapat kumpulan pemicu yang

disebut enabler untuk mendukung implementasi pemerintahan dan manajemen sistem TI. Framework Cobit 5 mendefinisikan 7 kategori enablers

2.1 Fokus Proses

Penelitian ini hanya fokus pada domain DSS02 yang ruang lingkupnya tentang penanganan *incident management.* DSS02 mempunyai 7 sub proses yang sebagai berikut.

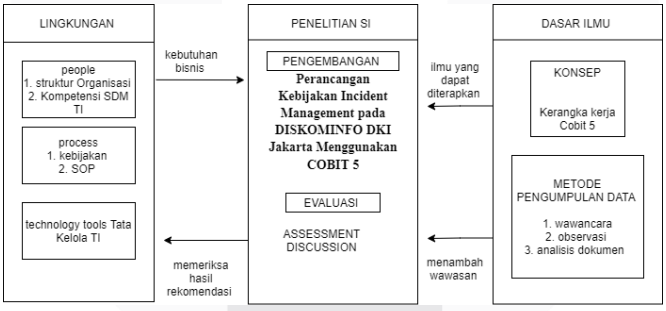
1. DSS02 - *Manage Service Requests and Incidents*
   Memberikan respons yang tepat waktu dan efektif terhadap permintaan pengguna dan resolusi semua jenis insiden. Kembalikan layanan normal; merekam dan memenuhi permintaan pengguna; dan merekam, menyelidiki, mendiagnosis, mengeskalasi, dan menyelesaikan insiden.
   Sub pada DSS02, yaitu :

a) DSS02.01 *Define incident and service request classification schemes.*
b) DSS02.02 *Record, classify and prioritise requests and incidents.*
c) DSS02.03 *Verify, approve and fulfil service requests*
d) DSS02.04 *investigate, diagnose and allocate incidents.*
e) DSS02.05 *Resolve and recover from incidents.*
f) DSS02.06 *Close service requests and incidents.*
g) DSS02.07 *Track status and produce reports*.

3. Metodologi Penelitian

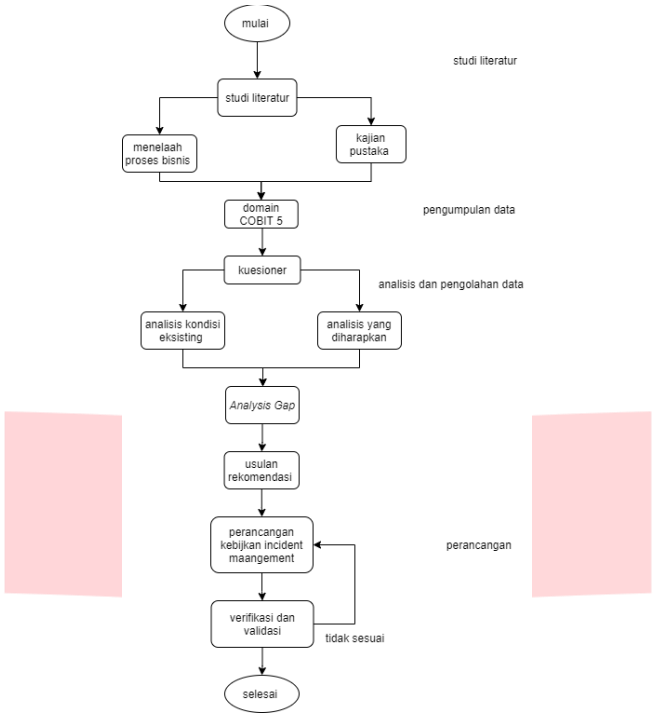
3.1 Kerangka Pemecahan Masalah / Pengembangan Model Konseptual

Model konseptual merupakan salah satu bentuk alur yang menjelaskan secara teoritis model konseptual variabel penelitian dengan menggambarkan sebuah metode dalam pemecahan masalah secaar terstruktur.



3.2 Sistematika Penelitian

Sistematika penelitian adalah sebuah alur tahapan penelitian yang bertujuan untuk memperolah dan mengumpulkan data yang diperoleh dan membuat rekomendasi terkait pembuatan kebijakan, penelitian ini menggunakan metode kualitatif. Objek penelitian di Diskomfotik DKI Jakarta terkait tentang pengelolaan teknologi informasi. Dibawah ini merupakan alur untuk mendapatkan data.



3.3 Pengumpulan Data

Pada penelitan ini pengumpulan data dilakukan dengan data primer dan data sekunder. Data primer yaitu memperolah atau mendapatkan data secara langsung sedangkan data sekunder dari studi literatur.

3.3.1 Studi literatur

Studi literatur yang ambil berdasarkan jurnal-jurnal yang memiliki topik yang sama dengan penelitian ini. COBIT 5 sebagai acuan utama dalam studi literatur ini yang dikeluarkan oleh ISACA seperti COBIT 5 Framework, COBIT 5 Enabling Process, COBIT 5 Implementation, COBIT 5 Process Assessment Model dan COBIT 5 Process Reference Guide.

3.3.2 Pengumpulan Data Primer

Data yang diperoleh langsung dari lapangan ketika peneliti memberikan kuesioner ke Diskominfo DKI Jakarta. Kuesioner berisi pertanyaan yang mengacu pada kerangka kerja COBIT 5 dengan domain DSS02. Kuesioner ini diserahkan melalui aplikasi (whatsapp atau lainnya) kepada / ibu Bidang SIM.

3.3.3 Tahap Analisis

Setelah terkumpul semua data. Semua data di analisis sesuai dengan kondisi sekarang dan kondisi yang diharapkan untuk mendapatkan data dan infromasi tentang kondisi kebijakan *incident management* di Diskominfo DKI Jakarta

3.3.4 Tahap Perancangan

Tahap ini merancang kebijakan berdasarkan hasil analisis pada tahap sebelumnya dan rekomendasi. Rekomedasi berupa kebijakan yang berguna untuk menangani incident management sesuai kebutuhan instansi dan juga sesuai dengan referensi framework yang digunakan.

4. Analisis

4.1 GAP ANALYSIS

Berikut adalah tabel perbandingan kondisi eksisting dengan kondisi ideal yang ada pada Cobit5 dengan domain DSS02 *Manage Service Requests and Incident* :

Nama Kontrol	DSS02 *Manage Service Requests and Incidents*		
Sub Kontrol	DSS02.01 *Define incident and service request classification schemes.*		
Tujuan Wawancara	*Define incident and service request classification schemes and models*		
Aktivitas	Yes / No	Proses eksisting	keterangan
1. *Define incident and service request classification and prioritisation schemes and criteria for problem registration, to ensure consistent approaches for handling, informing users about and conducting trend analysis*	*Yes*	Sudah melakukan pendefinisian insiden	Namun Belum ada kategori insiden
2. *Define incident models for known errors to enable efficient and effective resolution*	*no*	Belum melaksanakan aktivitas ini	Belum ada insiden model
3. *Define service request models according to service request type to enable self-help and efficient service for standard requests*	*no*	Belum melaksanakan aktivitas ini	
4. *Define incident escalation rules and procedures, especially for major incidents and security incidents.*	*No*	Belum melaksanakan aktivitas ini	Belum ada eskalasi dalam menangani insiden
5. *Define incident and request knowledge sources and their use.*	*No*	Belum melaksanakan aktivitas ini	Untuk referensi masih berpedomnan ke pengalaman

Tabel 1. subdomain DSS02.01

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*			
Sub Kontrol	*DSS02.02 Record, classify and prioritise requests and incidents*			
Tujuan Wawancara	*Identify, record and classify service requests and incidents, and assign a priority according to business criticality and service agreements*			
Aktivitas		Yes / No	Proses eksisting	keterangan
1. *Log all service requests and incidents, recording all relevant information so that they can be handled effectively*		*Yes*	Aktivitas ini sudah dilakukan,	Tidak semua insiden di catatan

and a full historical record can be maintained		tetapi belum semua insiden dilakuka pencatatan	
2. *To enable trend analysis, classify service requests and incidents by identifying type and category*	*No*	Aktivitas ini belum dilakukan	Belum ada identifikasi insiden berdasarkan kategori
3. *Prioritise service requests and incidents based on SLA service definition of business impact and urgency*	*No*	Aktivitas ini belum dilakukan	Belum ada identifikasi insiden berdasarkan prioritas

Tabel 2. Subdomain DSS02.02

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*		
Sub Kontrol	*DSS02.03 Verify, approve and fulfil service requests*		
Tujuan Wawancara	*select the appropriate request procedures and verify that the service requests fulfil defined request criteria. Obtain approval, if required, and fulfil the requests.*		
Aktivitas	*Yes / No*	Proses eksisting	keterangan
1. *Verify entitlement for service requests using, where possible, a predefined process flow and standard changes.*	*no*	Aktivitas ini belum dilakukan	Belum ada Verifikasi hak untuk permintaan layanan
2. *Obtain financial and functional approval or sign-off, if required, or predefined approvals for agreed-on standard changes.*	*no*	Aktivitas ini belum dilakukan	
3. *Fulfil the requests by performing the selected request procedure, using, where possible, self-help automated menus and predefined request models for frequently requested items*	*no*	Aktivitas ini belum dilakukan	Belum ada Penuhi permintaan dengan melakukan prosedur permintaan yang dipilih,

Tabel 3. Subdomain DSS02.03

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*		
Sub Kontrol	*DSS02.04 Investigate, diagnose and allocate incidents.*		
Tujuan Wawancara	*dentify and record incident symptoms, determine possible causes, and allocate for resolution*		
Aktivitas	Yes / No	Proses eksisting	keterangan
1. *Identify and describe relevant symptoms to establish the most probable causes, of the incidents. Reference available knowledge resources (including known errors and problems) to identify possible incident resolutions (temporary workarounds and/or permanent solutions*	*No*	Aktivitas ini belum dilakukan	

2. *If a related problem or known error does not already exist and if the incident satisfies agreed-on criteria for problem registration, log a new problem*	*no*	Aktivitas ini belum dilakukan	Tidak ada pencatatan masalah
3. *Assign incidents to specialist functions if deeper expertise is needed, and engage the appropriate level of management, where and if needed.*	*Yes*	Menggunakan pihak external	Tetapi hanya sekedar referensi saja

Tabel 4. Subdomain DSS02.04

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*		
Sub Kontrol	*DSS02.05 Resolve and recover from incidents.*		
Tujuan Wawancara	*Document, apply and test the identified solutions or workarounds and perform recovery actions to restore the IT-related service*		
Aktivitas	Yes / No	Proses eksisting	keterangan
1. *Select and apply the most appropriate incident resolutions (temporary workaround and/or permanent solution).*	*yes*	Resolusi insiden yang tepat Jika insiden telah teratasi	Namun Jika insiden tidak terselesaikan maka dibiarkan saja
2. *Record whether workarounds were used for incident resolution*	*No*	Aktivitas ini belum dilakukan	Tidak ada pencatatan
3. *Perform recovery actions, if required.*	*No*	Aktivitas ini belum dilakukan	
4. *Document incident resolution and assess if the resolution can be used as a future knowledge source*	*No*	Aktivitas ini belum dilakukan	Belum ada dokumen resolusi

Tabel 5. Subdomain DSS02.05

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*		
Sub Kontrol	*SS02.06 Close service requests and incidents.*		
Tujuan Wawancara	*verify satisfactory incident resolution and/or request fulfilment, and close.*		
Aktivitas	Yes / No	Proses eksisting	keterangan
1. *Verify with the affected users (if agreed on) that the service request has been satisfactory fulfilled or the incident has been satisfactory resolved*	*No*	Aktivitas ini belum dilakukan	Hanya mengabarkan jika insiden telah selesai ditangani
2. *close service requests and incidents*	*Yes*	Sudah melakukan *close incident* dalam bentuk laporan	Namun tidak semua insiden dilakukan penutupan insiden

Tabel 6. subdomain DSS02.06

Nama Kontrol	*DSS02 Manage Service Requests and Incidents*		
Sub Kontrol	*DSS02.07 Track status and produce reports*		
Tujuan Wawancara	*Regularly track, analyse and report incident and request fulfilment trends to provide information for continual improvement.*		
Aktivitas	Yes / No	Proses eksisting	keterangan

1.	*Monitor and track incident escalations and resolutions and request handling procedures to progress towards resolution or completion.*	*No*	Aktivitas ini belum dilakukan	Tidak ada eskalasi insiden
2.	*identify information stakeholders and their needs for data or reports. Identify reporting frequency and medium.*	*No*	Aktivitas ini belum dilakukan	Belum ada mengidentifikasi pemangku kepentingan informasi dan kebutuhan mereka akan data atau laporan
3.	*Analyse incidents and service requests by category and type to establish trends and identify patterns of recurring issues, SLA breaches or inefficiencies. Use the information as input to continual improvement planning.*	*No*	Aktivitas ini belum dilakukan	Belum ada Menganalisis insiden berdasarkan kategori dan jenis
4.	*Produce and distribute timely reports or provide controlled access to online data*	*No*	Aktivitas ini belum dilakukan	Belum ada mendistribusikan laporan dengan akses terkontrol ke data online

Tabel 7. Subdomain DSS02.07

Berdasarkan hasil GAP Analisis diatas kondisi eksisting saat ini masih jauh ketinggaalan dengan kondisi ideal yang ada pada COBIT 5. Kondisi eksisting pada subdomain DSS02.01 hanya menjalankan satu aktivitas saja tetapi aktivitas tersebut tidak sepenuhnya dijalankan karena belum ada kategorisasi penanganan dan prioritas insiden. Pada subdomain DSS02.02 menjalankan satu aktivitas yaitu mencatat insiden yang terjadi tetapi hanya beberapa insiden saja. Pada subdomain DSS02.04 sudah menjalankan aktivitas tersebut dengan menggunakan tenaga ahli dari luar (external) tetapi hanya sekedar referensi. Pada subdomain DSS02.05 untuk resolusi yang dilakukan hanya melakukan semaksimal mungkin jika tidak terselesaikan maka insiden tidak dilanjutkan penanganannya. Pada DSS02.06 hanya menjalankan aktivitas penutupan insiden tetapi aktivitas tersebut belum sepenuhnya dilakukan padahal hal tersebut sangat penting. Jika terjadi insiden yang sama maka akan terpenuhi dengan cepat. Jadi dapat disimpulkan dari 24 aktivitas yanga ada pada domain DSS02 *Manage Service Requests and Incidents* hanya 4 aktivitas saja yang masih dilakukan walaupun masih belum seutuhnya. Untuk mendekati kondisi ideal sesuai dengan domain DSS02 *Manage Service Requests and Incidents* maka kebijakan yang akan dirancang adalah kebijakan penanganan insiden, kebijakan eskalasi insiden, dan kebijakan penutupan insiden.

4.2 Usulan Rekomendasi

Setelah mendapatkan gap analisis maka berikut adalah usulan rekomendasi yang diberikan :

GAP ANALYSIS	ASPEK	*PROCEDURE IMPROVEMENT*
Belum ada penggategorian insiden	*process*	Membuat sebuah formulir penggategorian insiden

Tidak mencatatan semua insiden	*process*	Membuat formulir pencatatan insiden
Belum ada priotitas insiden	*process*	Membuat sebuah prioritas insiden
Kurang dalam membuat report penutupan insiden	*process*	Membuat report penutupan insiden
Belum ada tenaga ahli untuk penanganan insiden	*People*	Menambah SDM dibagian tenaga ahli

Tabel 8. usulan rekomendasi

5. Perancangan kebijakan

5.1 Kebijakan *Incident Management*

Bersadarkan hasil analisis yang dilakukan pada bab sebelumnya, maka terbentuklah sebuah draft kebijakan sebagai berikut :

1. Peristiwa yang dikatakan dengan insiden adalah kejadian yang tidak disengaja dengan permasalan yang sama.
2. Pelapor (*user)* insiden bertanggung jawab dalam melaporkan insiden, memberikan informasi yang jelas terhadap insiden tersebut.
3. ASN sebagai komunikasi utama dengan pelapor (*user)*
4. ASN bertanggung jawab melakukan penyelesaian masalah dengan pelapor (*user)*, melakukan eskalasi kepada pihak tenaga ahli Ketika tidak dapat melakukan penyelesaian masalah, dan melakukan pencatatan insiden.
5. Tenaga ahli bertanggung jawab dalam membantu melakukan penyelesaian masalah pelapor yang tidak dapat diselesaikan oleh ASN.
6. Insiden harus diselesaikan sesuai dengan kategori sebagai berikut :
   a) Aplikasi, untuk permasalahan yang terjadi di aplikasi.
   b) Integrasi, untuk permasalahan yang terjadi di integrasi.
   c) Database, untuk permasalahan yang terjadi di database.
7. Setiap laporan insiden yang masuk harus mendapat prioritas penanganan yang tepat dan dilakukan dalam waktu singkat.

   Berikut tabel prioritas penanganan insiden :

Priotitas Insiden	Keterangan
Tinggi	Waktu tersedia untuk menyelesaikan masalah $\leq$ 8 jam
	Menggangu proses bisnis utama

	Banyak user yang tidak dapat melanjutkan pekerjaannya
	Berpotensi kehilangan data
Menengah	Waktu tersedia untuk menyelesaikan masalah ≤ 24 jam
	Mengganggu beberapa proses bisnis
	Hanya satu atau beberapa user yang terhambat pekerjaannya secara personal
Rendah	Waktu tersedia untuk menyelesaikan masalah ≤ 48 jam
	Menghambat pekerjaan user secara personal

Tabel 9. prioritas insiden

8. Untuk memenuhi keputusaan user waktu penanganan insiden dilakukan seminimal mungkin.
9. Wajib menggunakan standar dan best practice TI dalam melaksanakan penanganan insiden.
10. Wajib melakukan eskalasi insiden jika penanganan insiden belum terpenuhi.
11. Jika penanganan insiden telah diselesaikan maka wajib melakukan penutupan insiden
12. Semua insiden harus dilaporkan dalam bentuk laporan sebagai bahan pembelajaran yang berguna untuk memperbaiki system agar dikemudian hari jika ada terjadi insiden yang sama akan terpenuhu dengan cepat

5.2 Prosedur *Incident Management*

1) Jika terjadi insiden si pelapor *(user)* menghubungi operator untuk melaporkan adanya insiden. Pelaporan dapat melalui email atau datang langsung dan ditulis dalam bentuk form pelaporan.
2) Operator memeriksa kesesuaian kategorisasi insiden yang dilaporkan dan melakukan kategorisasi ulang apabila belum sesuai.
3) Operator melakukan prioritasi terkait insiden yang dilaporkan.
4) Operator melakukan diagnosis awal dan mencari solusi insiden dengan melihat data historis penanganan insiden.
5) Dari diagnosis dan identifikasi, apakah operator dapat menangani sendiri insiden yang terjadi. Jika iya lanjut ke aktivitas 6. jika tidak, lanjut ke aktivitas 7 untuk melakukan eskalasi.
6) Melakukan penyelesaian masalah dengan solusi yang ditentukan, kemudian melanjutkan pada aktivitas no 11.
7) Menganalisis pihak yang dilakukan eskalasi pada setiap masing -masing kategori insiden
8) Operator menyerahkan form pelaporan insiden untuk dilakukan eskalasi kepada tenaga ahli.
9) Tenaga ahli memeriksa form pelaporan yang dikirmkan dan melakukan investigasi terkait eskalasi insiden.
10) Tenaga ahli melakukan penyelesaian insiden yang dieskalasi dan menginformasikan kepada pihak operator bahwa penanganan insiden telah selesai
11) Operator menginformasikan kepada pelapor (user) bahwa insiden telah selesai melalui email.

12) Melakukan pengecekan kategorisasi dan kelengkapan pencatatan insiden yang ditulis pada form pencatatan insiden.
13) Melakukan penutupan insiden. Lalu operator membuiat report dalam bentuk laporan.

Untuk SOP alur penanganan i*ncident management* dapat dilihat pada bab lampiran.

5.3 Verifikasi Dan Validasi

Setelah melakukan perancangan tahap selanjutnya adalah verfikasi dan validasi. Tahap ini dilakukan untuk mengetahui ketepatan dan kesesuian aktivitas kebijakan dan SOP yang telah dirancang. Verifikasi dan validasi dilakukan sesuai dengan pedoman yang ada pada COBIT 5, khususnya pada process subdomain *DSS02.01 Define incident and service request classification schemes, DSS02.02 Record, classify and prioritise requests and incidents, DSS02.04 Investigate, diagnose and allocate incident, DSS02.05 Resolve and recover from incidents* dan *DSS02.06 Close service requests and incidents.*

6. Kesimpulan dan saran

6.1 Kesimpulan

Hasil dari perancangan kebijakan *incident management* menggunakan Cobit 5 dapat diperoleh kesimpulan sebagai berikut :

1. Dari 24 aktivitas yang ada pada domain DSS02 hanya 4 aktivitas yang dapat diterapkan untuk perancangan kebijakan *incident management* pada instansi Diskominfotik DKI Jakarta.
2. Kebijakan *incident management* yang berbasis *framework Cobit 5* menghasilkan kebijakan menegenai kebijakan penanganan insiden, kebijakan eskalasi insiden, dan kebijakan penutupan insiden.
3. Kebijakan dan SOP yang telah dirancang sudah memenihi pedoman *incident management* yang ada pada cobit khususnya pada process subdomain *DSS02.01 Define incident and service request classification schemes, DSS02.02 Record, classify and prioritise requests and incidents, DSS02.04 Investigate, diagnose and allocate incident, DSS02.05 Resolve and recover from incidents* dan *DSS02.06 Close service requests and incidents*

6.2 Saran

Draft kebijakan *incident management* sudah mencakup proses penanganan insiden, tetapi untuk lebih mengoptimalkan pelaksanaan penanganan insiden, perlu dibuatkan sebuah aplikasi pendukung agar pelaksanaan *incident management* bisa lebih otomatis. Selain itu untuk mencapai kondisi yang ideal maka dapat menerapkan semua aktivitas yang pada domain DSS02.

referensi

[1] Jayusman, Yus, dan Tarmin Abdulghani. 2018. Evaluasi Tata Kelola Teknologi Informasi Dan Perancangan Kebijakan Sistem Manajemen Keamanan Informasi Berdasarkan Kerangka Kerja Cobit 5 Dan Sni Iso/Iec 27001. Bangkit Indonesia, 2(8)1-9.

[2] Tiatama, Adi. 2016. Perencanaan Tata Kelola Manajemen Keamanan Informasi Menggunakan Information Technology Infrastructure Library (Itil) V3. Pada D~Net Surabaya.

[3] Fitriana, Lailatul, Bambang Setiawan, dan Andre Parvian A. Pembuatan Panduan Tata Kelola Pada Bidang Keamanan Informasi Dan Pemulihan Bencana Berbasis Cobit 4.1 Dan Iso 27002 . Seminar Nasional Sistem Informasi Indonesia, 22 September 2014.

[4] Ciptangingrum, Dewi, Eko Nugroho, Dan Dani Adhipta. Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5. Seminar Nasional Teknologi Informasi dan Komunikasi 2015 (SENTIKA 2015).

[5] Lenawati, M., Winarno, W. W., & Amborowati, A. (2017). *Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5.* Yogyakarta.

[6] Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis *Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity.* Yogyakarta.