ANALISIS RISIKO OPERASIONAL TEKNOLOGI INFORMASI MENGGUNAKAN COBIT 5 FOR RISK PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA TANGERANG SELATAN

INFORMATION TECHNOLOGY OPERATIONAL RISK ANALYSIS USING COBIT 5 FOR RISK IN THE COMMUNICATION AND INFORMATICS DEPARTMENT OF SOUTH TANGERANG CITY

I Putu Yogi Nugraha[1], Rokhman Fauzi[2], Yuli Adam Prasetyo[3]

[1,2,3]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom

[1]iputuyoginugraha@student.telkomuniversity.ac.id, [2]rokhmanfauzi@telkomuniversity.ac.id, [3]adam@telkomuniversity.ac.id

Abstrak

Kebutuhan komunikasi yang instan menjadi hal yang sangat diperlukan dalam urusan pemerintahan guna menunjang banyaknya permintaan pelayanan. Selain itu, peningkatan keamanan informasi juga perlu dilakukan agar informasi dan data yang ada terjamin kerahasiaannya, keutuhannya, dan ketersediaannya. DISKOMINFO Tangerang Selatan merupakan unsur pelaksana otonom daerah yang salah satu tugasnya adalah menjaga keamanan asset informasi, dalam menjalankan tugasnya akan muncul risiko-risiko keamanan informasi yang mengancam keamanan asset informasi. Untuk menemukan risiko tersebut maka dilakukan evaluasi keamanan informasi. Tujuan penelitian ini adalah membuat rancangan evaluasi keamanan informasi di DISKOMINFO Tangerang Selatan dengan mengacu pada kerangka kerja COBIT 5 *for Risk* dan menggunakan proses COBIT 5 Domain EDM dan APO. Sistematika penelitian ini terdiri dari tahap analisis konteks, tahap analisis eksisting, tahap perancangan, dan tahap akhir. Hasil penelitian menunjukkan DISKOMINFO Tangerang Selatan sudah menerapkan prinsip COBIT 5 *for Risk* proses untuk menanggulangi beberapa risiko, penerapan domain APO dan EDM juga cukup baik namun harus ada yang diperbaiki. Penilaian proses pada kedua domain masih berada di tingkat 1 (*performed process*) dengan persentase EDM03 57% dan APO12 62% dan terasuk dalam kategori level *Largely achieved*. Ditemukan 10 kasus risiko di berbagai level kategori, kemudian dihasilkan tujuh usulan rekomendasi kebijakan yang dapat membantu DISKOMINFO Tangerang Selatan dalam menangani risiko yang ada.

Kata kunci : COBIT 5, DISKOMINFO, Kemanan Informasi, Teknologi Informasi.

Abstract

The need for instant communication is indispensable in government affairs to support the many requests for service. In addition, it is also necessary to increase information security so that the information and data that is available are guaranteed its confidentiality, integrity and availability. DISKOMINFO Tangerang Selatan is a regional autonomous implementing element whose duties are to maintain the security of information assets. In carrying out its duties, information security risks will arise that threaten the security of information assets. To find these risks, an information security evaluation is conducted. The purpose of this study is to design an information security evaluation at DISKOMINFO Tangerang Selatan by referring to the COBIT 5 for Risk framework and using the COBIT 5 Domain EDM and APO processes. The systematics of this research consists of the context analysis stage, the existing analysis stage, the design stage, and the final stage. The results showed that DISKOMINFO Tangerang Selatan has applied the COBIT 5 for Risk principle to overcome several risks, the application of the APO and EDM domains is also quite good, but there must be improvements. The assessment process in both domains was still at level 1 (performed process) with the percentage of EDM03 57% and APO12 62% and included in the Largely achieved level category. Found 10 risk cases at various level categories, then produced seven policy recommendations that can help DISKOMINFO Tangerang Selatan in dealing with existing risks.

Keywords: COBIT 5, DISKOMINFO, Information Security, Information Technology.

Pendahuluan

1.1 Latar Belakang

Menurut Kusrini (2007) Informasi adalah data yang sudah diolah menjadi sebuah bentuk yang berguna bagi pengguna yang bermanfaat dalam pengambilan keputusan saat ini atau mendukung sumber informasi. Begitu pula menurut Jogiyanto (2005) Informasi diartikan sebagai data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi yang menerimanya. Seiring perkembangan teknologi informasi di dunia ini, kebutuhan komunikasi yang instan menjadi hal yang sangat diperlukan. Komunikasi yang dimaksud adalah terjadinya pertukaran data antar satu perangkat komputer dengan perangkat komputer lainnya. Dalam urusan pemerintahan, hal itu sangat diperlukan guna menunjang banyaknya permintaan pelayanan.

Keamanan informasi adalah perlindungan informasi, yang merupakan aset, dari kemungkinan bahaya yang diakibatkan oleh berbagai ancaman dan kerentanan. Peningkatan keamanan informasi di pemerintahan dilakukan dengan tujuan agar informasi dan data yang ada di pemerintahan terjamin kerahasiaannya (*confidentiality*), keutuhannya *(integrity*) dan ketersediaannya (*availability*). Salah satu pengimplementasian keamanan informasi yaitu dengan adanya tata kelola keamanan informasi agar resiko keamanan informasi dapat diminimalisir dan bahkan dapat dihindari.

Berdasarkan Perda Nomor 08 Tahun 2016 tentang Organisasi Perangkat Daerah, Dinas Komunikasi dan Informatika Kota Tangerang Selatan merupakan unsur pelaksana otonom daerah di bidang komunikasi dan informatika yang memiliki tugas pokok untuk membantu walikota dalam merencanakan, melaksanakan, mengawasi, dan mengendalikan kegiatan dibidang komunikasi dan informatika sesuai dengan kebijakan pemerintah daerah. Selain itu DISKOMINFO juga bertugas untuk menjaga keamanan aset informasi. Dalam menjaga keamanan aset informasi, maka akan muncul risiko keamanan informasi yang dapat mengancam keamanan asset informasi, sehingga perlu dilakukan evaluasi keamanan informasi.

COBIT 5 merupakan sebuah standar kerangka kerja yang disusun untuk membantu perusahaan dalam mengelola dan memanajemen aset atau sumber daya Informasi untuk mencapai tujuan perusahaan tersebut. Terdapat 5 domain pada kerangka COBIT 5 untuk mempraktekkan Tata Kelola TI yang efektif dan efisien. Pada penelitian ini akan menggunakan beberapa domain yaitu proses APO (*Align, Plan, Organise*), BAI (*Build, Acquire, Implement*), DSS (*Deliver, Service, Support*), MEA (*Monitor, Evaluate, Asses*), dan EDM (*Evaluate, Direct, Monitor*). Fokus untuk penelitian ini adalah menggunakan domain EDM dan APO dikarenakan Dinas Komunikasi dan Infomartika Tangerang Selatan merupakan suatu instansi pemerintahan yang berhubungan erat dengan layanan publik, maka apabila layanan tersebut mengalami sebuah masalah akan berdampak sangat besar terhadap Dinas Komunikasi dan Informatika itu sendiri.

COBIT 5 *for Risk* merupakan kerangka kerja bagian dari COBIT 5 *family* yang digunakan dalam membantu perusahaan untuk melakukan pengelolaan sumber daya teknologi informasi. Perancangan manajemen risiko yang dirancang berdasarkan proses *seven enabler* pada aspek *Services, Infrastructure, Applications and Information.* Sehingga

berdasarkan latar belakang yang telah dijelaskan, penulis menggunakan COBIT 5 *for Risk* sebagai kerangka kerja dalam penelitian ini. Berdasarkan Permasalahan di atas mendorong penulis membuat rancangan evaluasi keamanan informasi di DISKOMINFO Tangerang Selatan, evaluasi ini dibuat dengan mengacu pada kerangka kerja COBIT 5 *for Risk* dan menggunakan proses COBIT 5 dengan Domain EDM dan APO.

1.2 Rumusan Masalah

1. Bagaimana kondisi penerapan proses COBIT 5 domain EDM dan APO pada DISKOMINFO Tangerang Selatan?
2. Bagaimana analisis risiko pada proses COBIT 5 domain EDM dan APO menggunakan kerangka kerja COBIT-5 *for risk*?
3. Bagaimana opsi penanganan risiko pada proses COBIT 5 domain EDM dan APO menggunakan kerangka kerja COBIT-5 *for risk*?
4. Bagaimana prioritas penanganan risiko pada proses COBIT 5 domain EDM dan APO menggunakan kerangka kerja COBIT-5 *for risk*?

1.3 Tujuan Penelitian

1. Mengetahui kondisi penerapan proses COBIT 5 domain EDM dan APO pada DISKOMINFO Tangerang Selatan.
2. Menghasilkan peta risiko pada proses COBIT 5 domain EDM dan APO.
3. Memilih opsi penanganan risiko pada proses COBIT 5 domain EDM dan APO.
4. Menghasilkan rencana penanganan risiko pada proses COBIT 5 domain EDM dan APO.

2. Tinjauan Pustaka

2.1 Keamanan Informasi

Keamanan informasi menurut Garfinkel, Spafford, dan Schwatz (2003) adalah bagaimana usaha untuk dapat mencegah penipuan (*cheating*) atau bisa mendeteksi adanya penipuan pada sistem yang berbasis informasi, di mana informasinya sendiri tidak memiliki arti fisik. Aspek-aspek yang harus dipenuhi dalam suatu sistem untuk menjamin keamanan informasi adalah informasi yang diberikan akurat dan lengkap (*right information*), informasi dipegang oleh orang yang berwenang (*right people*), dapat diakses dan digunakan sesuai dengan kebutuhan *(right time),* dan memberikan informasi pada format yang tepat (*right form*).

2.2 Aspek Keamanan

Menurut Mahersmi, Muqtadiroh, dan Hidayanto (2016) organisasi keamanan informasi memiliki tiga aspek yang harus dipahami untuk bisa menerapkannya, aspek tersebut biasa disebut dengan CIA Triad Model, yaitu (1) Confidentiality ; menjamin kerahasiaan data yang harus di lindungi dalam berbagai aspek dan menjamin informasi yang hanya dapat di akses oleh pihak yang berwenang, (2) Integrity; menajaga agar informasi selalu akurat, menjaga kelengkapan informasi dan menjaga informasi dari kerusakan atau ancaman lain, dan (3) Availibility; menjamin bahwa data akan tersedia saat dibutuhkan kapanpun dan dimanapun, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait. Dengan terpenuhinya aspek dan prinsip dasar penyusunan program keamanan informasi tersebut, maka informasi terjamin dan terlindungi dari ancaman dan informasi dapat di gunakan dengan baik.

2.3 Pengertian *E-Government*

E-Government adalah penerapan teknologi berbasis internet dalam berbagai layanan pemerintahan untuk memberikan informasi dan layanan demi tata kelola yang efisien dan efektif, e-government sendiri dilakukan di sektor publik baik di negara maju maupun berkembang dengan cara yang disesuaikan dengan tingkat sumber daya yang optimal (Sharma, 2015). Tujuan pelaksanaan e-government bagi pemerintah yaitu agar dapat menjadi lembaga yang lebih dekat dengan masyarakat dan membangun partnership dengan beberapa komunitas yang memiliki kepentingan serta keahlian yang berbeda-beda.

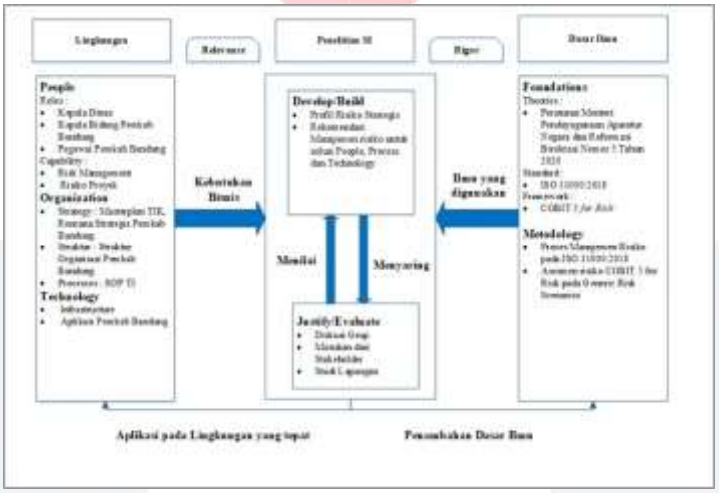
2.4 COBIT 5 *for Risk*

COBIT 5 for Risk di buat berdasarkan kerangka kerja COBIT 5 dengan berfokus kepada risiko dan menyediakan berbagai panduan rinci dan praktis untuk pada profesional dan pihak terkait mengenai risiko di suatu perusahaan. COBIT 5 for Risk membahas mengenai risiko TI yang terkait dan panduan ini juga memiliki 2 pandangan mengenai cara COBIT 5 dalam menangani risiko yaitu risk function dan risk management. Pandangan risk function berfokus kepada apa yang dibutuhkan untuk membangun dan mempertahankan fungsi risiko di dalam perusahaan. Sedangkan pandangan risk management berfokus kepada inti dari risiko tata kelola dan manajemen proses terhadap bagaimana cara untuk

mengoptimasi risiko dan bagaimana mengidentifikasi, menganalisa, dan menanggapi sampai melaporkan risiko setiap harinya (ISACA, 2013).

3. Metodologi Penelitian

Model konseptual merupakan model yang berisi hubungan antara factor-faktor utama yang akan memetakan permasalahan dan menghubungkan dengan teori yang ada untuk mempermudah dalam pemecahan masalah. Model konseptual dalam penelitian tugas akhir ini mengacu pada Hevner et al (2004) *design research* yang digambarkan melalui gambar 1 di bawah ini.



Gambar 1 Model Konseptual

4. Hasil dan Pembahasan

4.1 Identifikasi Teknologi Eksisting

Teknologi menjadi dukungan dalam mengerjakan setiap proses bisinis yang ada pada perusahaan atau organisasi. DISKOMINFO Tangerang Selatan memiliki beberapa aset seperti database, database server, PC, hub, switch, dan router.

4.2 Analisis *Capability Level*

Analisis penilaian capability level dilakukan untuk mengukur kondisi organisasi saat ini, analisis dilakukan menggunakan kerangka kerja COBIT 5 khususnya domain proses EDM03 dan APO12. Berdasarkan hasil observasi dan wawancara pada pihak DISKOMINFO Tangerang Selatan didapatkan nilai *capability level* kedua domain berada pada level 1. Tabel 1 memaparkan hasil perhitungan *capability level.*

Tabel 1 Capability Level

Proses	Level Kapabilitas	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 2.3	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
EDM03	1	57%	L	N	N	N	N	N	N	N	N	N
Proses	Level Kapabilitas	Persentase	PA 1.1	PA 2.1	PA 2.2	PA 2.3	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
APO12	1	62%	L	N	N	N	N	N	N	N	N	N

4.3 Analisis Risiko

Penilaian risiko dilakukan dengan menentukan level kemungkinan, dampak, dan risiko yang dari setiap paint point yang ada di DISKOMINFO Tangerang Selatan. Tabel 2 di bawah ini memaparkan analisis risiko dari setiap paint point.

Tabel 2 Paint Point

No	***Paint Point***	Kategori	Risiko	Level	***Risk Response***
1	Ada kekurangan atau ketidakcocokan antara keterampilan TIK dengan kebutuhan SPBE	*IT expertise and skills*	11	Sedang	Mengurangi Resiko (*Risk Reduction*)
2	Kurangnya pemahaman bisnis oleh staf IT yang mempengaruhi pemberian layanan / kualitas proyek.	*IT expertise and skills*	7	Rendah	Mengurangi Resiko (*Risk Reduction*)
3	Tidak ada keterampilan yang cukup untuk memenuhi kebutuhan pemerintahan.	*IT expertise and skills*	3	Sangat Rendah	Mengurangi Resiko (*Risk Reduction*)
4	Adanya kesalahan oleh staf TI (selama backup, upgrade sistem, pemeliharaan sistem, dll.).	*Staff operations (human error and malicious intent)*	11	Sedang	Mengurangi Resiko (*Risk Reduction*)
5	Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah).	*Information (data breach: damage, leakage and access)*	16	Tinggi	Mengurangi Resiko (*Risk Reduction*)
6	Aplikasi SPBE yang belum stabil telah diimplementasikan	*Software*	10	Rendah	Mengurangi Risiko (*Risk Reduction*)
7	Adanya kebijakan nasional/internasional yang membatasi kemampuan layanan SPBE.	*Geopolitical*	16	Tinggi	Mengurangi Resiko (*Risk Reduction*)
8	Pengguna yang tidak sah mencoba membobol sistem.	*Logical attacks*	12	Sedang	Mengurangi Resiko (*Risk Reduction*)

9	Situs web dirusak.	*Logical attacks*	12	Sedang	Mengurangi Resiko (*Risk Reduction*)
10	Terjadi *hacktivisme*	*Logical attacks*	12	Sedang	Mengurangi Resiko (*Risk Reduction*)

Berdasarkan hasil analisis risiko yang sudah dilakukan didapatkan jumlah risiko berdasarkan level risiko yang sudah diperhitungkan, kemudian di kelompokkan sesuai levelnya. Sehingga didapatkan hasil sebagai berikut, terdapat satu *paint point* dengan level risiko sangat rendah, dua *paint point* dengan level risiko rendah, lima *paint point* dengan level risiko sedang, dua *paint point* dengan level risiko tinggi, dan tidak ada satu pun *paint point* dengan level risiko sangat tinggi.

4.4 Rekomendasi Kontrol Risiko dan Rekomendasi Kebijakan

Risiko adalah hal yang tidak pasti dan memiliki dampak negatif terhadap tujuan atau keinginan yang akan dicapai (Yap, 2017). Kontrol risiko dilakukan untuk meminimalisir atau mengurangi risiko terjadi kembali. Menurut Handoyo (2012) kebijakan berkaitan dengan rencana tindakan yang diarahkan untuk mewujudkan tujuan tertentu. Perancangan rekomendasi kontrol risiko dan rekomendasi kebijakan dibuat menggunakan framework COBIT 5 *for risk* berdasarkan hasil analisis risiko menggunakan metode COBIT 5 yang bertujuan sebagai saran dalam menangani risiko yang ada. Tabel 3 di bawah ini memaparkan perancangan rekomendasi kontrol risiko dan rekomendasi kebijakan.

Tabel 3 Rekomendasi Kontrol Risiko dan Rekomendasi Kebijakan

Paint Point	**COBIT 5 For Risk**	**Rekomendasi Kontrol**	**Rekomendasi Kebijakan**
Ada kekurangan atau ketidakcocokan antara keterampilan TIK dengan kebutuhan SPBE	APO07.03 *Maintain the skills and competencies of personnel.*	Menetapkan keterampilan dan kompetensi yang dibutuhkan SDM kemudian memberikan program pelatihan untuk mencapai tujuan perusahaan. Selanjutnya, perusahaan melakukan monitoring dan evaluasi program pelatihan keterampilan dan kompetensi SDM secara teratur.	Kebijakan pengelolaan sumber daya manusia
Kurangnya pemahaman bisnis oleh staf IT yang mempengaruhi pemberian layanan / kualitas proyek.	APO07.03 *Maintain the skills and competencies of personnel*		
Tidak ada keterampilan yang cukup untuk memenuhi kebutuhan pemerintahan.	APO07.03 *Maintain the skills and competencies of personnel*		

Adanya kesalahan oleh staf TI (selama backup, upgrade sistem, pemeliharaan sistem, dll).	APO01.02 *Establish roles and responsibilities.*	Menetapkan, menyetujui, dan mengomunikasikan peran dan tanggung jawab terkait TI untuk semua personel di perusahaan yang sejalan dengan kebutuhan dan tujuan bisnis dengan cara memasukan uraian peran dan tanggung jawab dalam kebijakan, prosedur manajemen, kode etik, dan praktik profesional yang sesuai dengan persyaratan perusahaan dan kesinambungan layanan TI. Selain itu perusahaan perlu melakukan pengawasan yang ketat untuk memastikan peran dan tanggung jawab dilaksanakan dengan benar, pengawasan juga dilakukan agar dapat menilai kinerja personel, menentukan akuntabilitas, dan mengurangi kemungkinan peran tunggal.	Kebijakan peran dan tanggung jawab
Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah).	DSS04.03 Develop and implement a business continuity response.	Mengembangkan dan memelihara BCP operasional yang berisi prosedur pengaturan kelanjutan operasi proses bisnis. Perusahaan perlu menetapkan kondisi dan prosedur pemutakhiran dan rekonsiliasi basis data informasi, kemudian menentukan dan mendokumentasikan SDM, fasilitas, infrastruktur TI, dan persyaratan cadangan informasi untuk mendukung prosedur pemulihan. Perusahaan juga perlu menentukan keterampilan yang dibutuhkan personelnya yang terlibat dalam pelaksanaan rencana dan prosedur, dan membagikan dokumentasi pendukung kepada pihak berkepentingan yang berwenang dan memastikan semuanya dapat diakses dalam skenario bencana.	Kebijakan komunikasi dan tindakan terhadap insiden

Aplikasi SPBE yang belum stabil telah diimplementasikan	BAI07.05 Perform acceptance test	Meninjau log kesalahan yang ditemukan dalam proses pengujian dan memastikan semua kesalahan telah diperbaiki, mengevaluasi kriteria keberhasilan hasil pengujian akhir, pastikan hasil pengujian akhir disetujui oleh pemangku kepentingan TI sebelum di produksi.	Kebijakan kelola perubahan penerimaan dan transisi
Adanya kebijakan nasional/internasional yang membatasi kemampuan layanan SPBE.	MEA03.02 Optimise response to external requirements.	Secara teratur meninjau dan menyesuaikan kebijakan, prinsip, standar, prosedur, dan metodologi yang efektif untuk menangani risiko dengan menggunakan tenaga ahli internal dan eksternal. Kemudian mengkomunikasikan perubahan-perubahan yang terjadi kepada semua personil yang relevan.	Kebijakan, prinsip, prosedur, dan standar yang diperbarui
Pengguna yang tidak sah mencoba membobol sistem.	DSS05.02 Manage network and connectivity security	Menetapkan dan memelihara kebijakan keamanan konektivitas dengan hanya mengizinkan perangkat tertentu untuk mengakses informasi perusahaan, gunakan konfigurasi menggunakan kata sandi untuk perangkat-perangkat yang diizinkan masuk. Kemudian menerapkan mekanisme penyaringan jaringan seperti *firewall* dan perangkat lunak pendeteksi intrusi, mengenkripsi informasi sesuai klasifikasinya, menerapkan protokol keamanan yang disetujui ke konektivitas jaringan, dan mengkonfigurasi peralatan jaringan dengan cara yang aman.	Kebijakan keamanan dan konektivitas
Situs web dirusak.	DSS05.01 Protect against malware.	Menginstal dan mengaktifkan alat pelindung perangkat lunak berbahaya menggunakan konfigurasi secara terpusat dan memfilter lalu lintas masuk untuk melindungi dari informasi yang tidak diminta. Kemudian melakukan monitoring dan evaluasi informasi tetang potensi ancaman baru,	Kebijakan pencegahan perangkat lunak berbahaya
Terjadi *hacktivisme*	DSS05.01 Protect against malware.		

		selanjutnya perlu juga pelatihan secara berkala tentang malware dalam penggunaan email dan internet agar dapat menerapkan prosedur pencegahan perangkat lunak berbahaya.	

5. Kesimpulan

Hasil penelitian ini menunjukkan bahwa DISKOMINFO Tangerang Selatan sudah menerapkan beberapa prinsip COBIT 5 for Risk seperti prinsip proses untuk menanggulangi beberapa risiko yang ada, penerapan domain APO dan EDM juga cukup baik namun harus ada yang diperbaiki. Penilaian proses pada kedua domain masih berada tingkat 1 (performed process) dengan persentase EDM03 57% dan APO12 62% yang terasuk dalam kategori level *Largely achieved*. Selain itu, ditemukan sepuluh kasus risiko dengan satu risiko pada level sangat rendah, dua risiko pada level rendah, lima risiko pada level sedang, dua risiko pada level tinggi, dan dan tidak ditemukan risiko pada level sangat tinggi. Kemudian, dihasilkan tujuh usulan rekomendasi kebijakan yang dibuat sesuai dengan kebutuhan kontrol risiko yang ada. Rekomendasi kebijkan yang dibuat yaitu kebijakan pengelolaan sumber daya manusia, kebijakan peran dan tanggung jawab, kebijakan komunikasi dan tindakan terhadap insiden, kebijakan kelola perubahan, penerimaan dan transisi, kebijakan prinsip, prosedur, dan standar yang diperbarui, kebijakan keamanan dan konektivitas, kebijakan pencegahan perangkat lunak berbahaya.

Referensi

[1] Garfinkel, S., Spafford, G., & Schwartz, A. (2003). *Practical Unix and Internet Security,* Third Ed. O'Relly Media, Inc.

[2] Handoyo, E. (2012). *Kebijakan Publik*. Semarang (ID): Widya Karya.

[3] Hevner, A. R., March. S. T., Park, J., & Ram, S. (2004). Design svience in information systems research. *MIS Quarterly, vol 28*(1), 75-105. Doi: https://doi.org/10.2307/25148625.

[4] ISACA. (2013). *COBIT 5 for Risk. IT Operation and Service Delivery Rolling Meadows:* ISACA.

[5] Jogiyanto. (2005). Sistem teknologi Informasi, Andi, Yogayakarta.

[6] Kusrini. (2007). Strategi Perancangan dan Pengelolaan Basis Data, Amikom, Yogyakarta.

[7] Mahersmi, B. L., Muqtadiroh, F. A., & Hidayanto, B. C. (2016). Analisis risiko keamanan informasi dengan menggunakan metode octave dan kontrol Iso 27001 pada Dishubkominfo Kabupaten Tulungagung. *Seminar Nasional Indonesia, vol 2016*, 181-194. Retrieved 3 Dec 2019 from http://is.its.ac.id/pubs/oajis/index.php/home/detail/1663/ANALISIS-RISIKO-KEAMANAN-INFORMASI-DENGAN-MENGGUNAKAN-METODE-OCTAVE-DAN-KONTROL-ISO-27001-PADA-DISHUBKOMINFO-KABUPATEN-TULUNGAGUNG.

[8] Sharma, S. K. (2015). Adoption of e-government services: The role of service quality dimensions and demographic variables. *Transforming Government: People, Process and Policy Journal*, *9*(2), 207-223. Doi: https://doi.org/10.1108/TG-10-2014-0046.

[9] Yap, P. (2017). *Panduan Praktis Manajemen Risiko Perusahaan*. Growing Publishing.