ANALISIS KEAMANAN SISTEM PADA SISTEM INFORMASI AKADEMIK MENGGUNAKAN COBIT 5 FRAMEWORK PADA SUB DOMAIN DSS05

Miftahurrizqi[1], Ika S. Windiarti[1], Agung Prabowo[2]
[1] Department of Computer Science, Muhammadiyah University of Palangkaraya, Palangkaraya,73112, Indonesia
[2]Department of Information Systems, STMIK Palangkaraya, Palangkaraya, 73112, Indonesia
Emails: **miftahurrizqii@gmail.com , ikasafitri@gmail.com , agungdosen@gmail.com**

ABSTRAK

Dalam tata kelola teknologi informasi dengan Framework COBIT 5, Terdapat sub domain DSS05 yaitu *Deliver, Service, and Support* khususnya yang membahas tentang jaminan atau kepastian keamanan sistem. penelitian ini secara menyeluruh menginvestigasi proses yang terjadi pada biro administrasi akademik dengan fokus pada domain DSS. Dalam tulisan Ini yang akan dibahas adalah domain DSS05 tersebut. Dalam penelitian ini Perumusan masalahnya adalah bahwa Apakah proses sistem informasi akademik yang ada pada biro administrasi akademik universitas Muhammadiyah Palangkaraya telah menjamin adanya keamanan sistem bagi pengguna dan juga bagi sistem itu sendiri. Metode yang dilakukan pada penelitian ini adalah Pengukuran tingkat maturity berdasarkan indikator atau kriteria yang ada pada cobit 5. Dalam penelitian ini dilakukan serangkaian wawancara dan observasi terhadap keamanan sistem yang ada pada sistem informasi akademik. Dari penelitian yang dilakukan diperoleh hasil bahwa domain DSS05 pada sistem informasi akademik universitas Muhammadiyah Palangkaraya berada pada tingkat maturity level 2 yaitu *Repeatable but Intuitive*, dan diharapkan berada pada tingkat level maturity level 4. Hal yang dapat dilakukan untuk meningkatkan level maturity ini adalah meningkatkan sistem keamanan dengan memperhitungkan kondisi seiring Bertambahnya kompleksitas atas sistem yang ada.

Kata kunci: COBIT, manajemen, keamanan, sistem informasi, institusi akademik

ABSTRACT

In information technology governance with the COBIT 5 Framework, there is a DSS05 sub domain, namely Deliver, Service, and Support, especially which discusses system security assurance or certainty. This study thoroughly investigates the processes that occur in academic administration bureaus with a focus on the DSS domain. In this paper what will be discussed is the DSS05 domain. In this research, the problem formulation is that whether the academic information system process in the academic administration bureau of Muhammadiyah University of Palangkaraya guarantees the security of the system for users and also for the system itself. The method used in this research is measuring the level of maturity based on the indicators or criteria in COBIT 5. In this study, a series of interviews and observations were conducted on the security of the existing systems in the academic information system. From the research conducted, it is found that the DSS05 subdomain in the academic information system of Muhammadiyah University of Palangkaraya is at maturity level 2, namely Repeatable but Intuitive, and is expected to be at the maturity level 4. Things that can be done to increase this maturity level are to improve the security system considering the conditions as the increasing complexity of the existing system.

Keywords: COBIT, management, security, information system, academic institution

1. PENDAHULUAN

Dalam implementasi suatu sistem informasi perlu untuk mempertimbangkan faktor keamanan dari sistem informasi tersebut. Terlebih apabila sistem informasi tersebut berkaitan dengan hal-hal yang bersifat rahasia dan melibatkan adanya informasi pribadi di dalamnya (Bakri & Irmayana, 2017). Keamanan sistem informasi ini menjadi sangat penting karena apabila sistem informasi ini diakses oleh orang yang tidak berhak menggunakan asas tersebut maka keakuratan informasi tersebut akan menurun levelnya(Aini et al., 2018). Pada dasarnya suatu sistem informasi yang aman apabila terpenuhi kriteria-kriteria antara lain identifikasi pemakai, pembuktian keaslian pemakai, dan otorisasi pemakai.

Pada kerangka kerja COBIT 5, terdapat salah satu domain yaitu subdomain DSS05 Yang membahas tentang kepastian atau jaminan keamanan system (Nuraeni & Haryana, 2016). Pada subdomain DSS05 suatu sistem informasi membutuhkan adanya integritas dari informasi tersebut untuk melindungi aset teknologi informasi (Zainuddin et al., 2020). Perlindungan

terhadap sistem informasi ini bertujuan agar dalam proses bekerjanya sistem informasi tersebut tidak mengalami kendala yang serius yang kaitannya dengan keamanan data dan juga keamanan sistem itu sendiri (Krisdiyawan & Kuswantoro, 2017). Keamanan data berkaitan dengan melindungi identitas pengguna, melindungi proses input data yang sudah dilakukan oleh para pengguna sistem serta melindungi data yang dimiliki oleh setiap pengguna sistem. Sedangkan keamanan sistem meliputi adanya perlindungan identitas operator, perlindungan terhadap data yang ada di sistem secara menyeluruh, perlindungan terhadap kode pemrograman yang ada di dalam sistem serta keamanan dari keseluruhan sistem tersebut.

Perlindungan integritas dan perlindungan akses teknologi informasi dilakukan dengan adanya proses manajemen keamanan (*security management*) (Imany et al., 2019). Proses manajemen keamanan ini meliputi adanya pemeliharaan peran, tanggung jawab, kebijakan, standar dan prosedur keamanan teknologi informasi. ada tiga bagian penting dari suatu manajemen keamanan yaitu:

1. penyelenggaraan pengawasan keamanan (*Security monitoring*)
2. pengujian berkala (*periodic testing*)
3. pengimplementasian tindakan koreksi

Permasalahan dalam penelitian ini adalah apakah proses sistem informasi akademik yang ada pada biro administrasi akademik Universitas Muhammadiyah Palangkaraya telah menjamin adanya keamanan sistem informasi yang meliputi keamanan sistem bagi pengguna dan bagi sistem itu sendiri penelitian ini bertujuan untuk mendapatkan hasil pengukuran tingkat maturity level pada subdomain DSS05 dengan serangkaian pertanyaan wawancara dan observasi terhadap keamanan sistem. Hasil dari penelitian ini nantinya akan didapatkan rekomendasi pada tingkat maturity level berapa yang diinginkan secara ideal yang seharusnya ada di dalam sistem informasi akademik pada biro administrasi akademik Universitas Muhammadiyah Palangkaraya.

2. TINJAUAN PUSTAKA

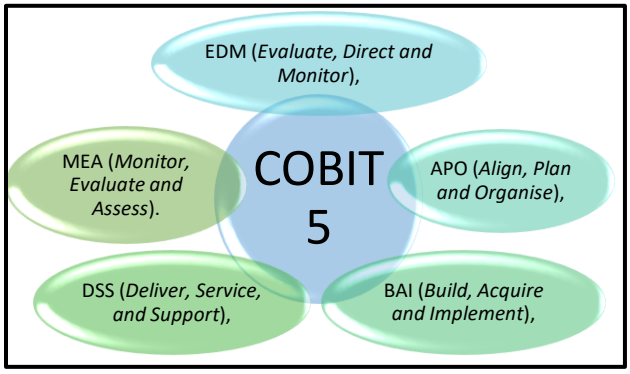
Tata kelola teknologi informasi yang baik dikelola secara sistematis terkontrol, efektif, efisien dan bisa mengurangi biaya operasional dari suatu sistem. Untuk membangun suatu tata kelola teknologi informasi yang baik diperlukan komitmen dari berbagai pihak termasuk *stakeholders* dan juga pengguna sistem (Swastika et al., 2016). Untuk mencapai suatu standar dalam tata kelola teknologi informasi secara internasional maka diterapkan adanya Control Objective for Information and Related Technology (COBIT). COBIT adalah standar pengendalian pada teknologi informasi secara umum dan COBIT ini memberikan suatu format kerangka kerja pada manajemen pengelolaan teknologi informasi (Sulaeman, 2017).

Apabila dalam suatu teknologi pengelolaan sistem teknologi informasi menggunakan COBIT dalam melaksanakan kegiatan auditnya maka akan menghasilkan suatu pengukuran level *maturity* dalam proses sistem informasi yang pada akhirnya dapat dijadikan sebagai bahan rekomendasi untuk peningkatan dan pengembangan sistem itu sendiri (De Haes et al., 2013).

COBIT 5 sendiri adalah merupakan kumpulan dari dokumentasi dan panduan untuk mengimplementasikan tata kelola teknologi informasi. Dan selain itu COBIT 5 juga membantu auditor dan pihak manajemen untuk menjembatani hal-hal seperti resiko dalam berbisnis, pengendalian proses dan juga permasalahan teknis di dalam penerapan teknologi informasi. COBIT 5 memiliki dua area utama yaitu area tata kelola dan juga area manajemen(Youssfi et al., 2014).

Area pertama yaitu area tata kelola berhubungan dengan peraturan yang mengikat pada penerapan teknologi informasi dan juga tentang bagaimana mengatur strategi dan pengendalian dari infrastruktur teknologi informasi. Sedangkan yang kedua adalah area manajemen, area ini berhubungan dengan bagaimana tata kelola yang baik diimplementasikan pada ranah manajemen dan dilakukan dengan cara perencanaan secara taktis.

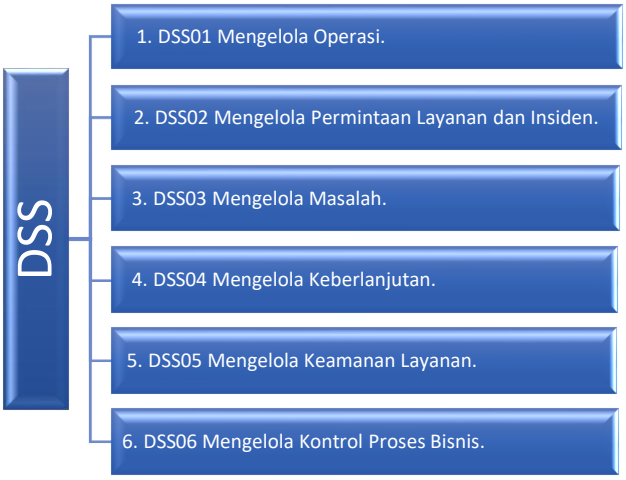
Di dalam kerangka kerja COBIT 5 sendiri memiliki 5 domain yaitu EDM (*Evaluate, Direct and Monitor*), APO (*Align, Plan and Organise*), BAI (*Build, Acquire and Implement*), DSS (*Deliver, Service, and Support*), MEA (*Monitor, Evaluate and Assess*) (Oktarina, 2017). Di dalam artikel ini akan dibahas adalah domain DSS05, yaitu terkait tentang jaminan keamanan sistem.



Gambar 1. Domain dalam COBIT 5

Domain DSS terdiri dari 6 *control objective*, yakni sebagai berikut:

1. DSS01 Mengelola Operasi.
2. DSS02 Mengelola Permintaan Layanan dan Insiden.
3. DSS03 Mengelola Masalah.
4. DSS04 Mengelola Keberlanjutan.
5. DSS05 Mengelola Keamanan Layanan.
6. DSS06 Mengelola Kontrol Proses Bisnis.



Gambar 2. 6 Sub Domain pada Domain *Deliver, Service, and Support (DSS)*

Jaminan keamanan sistem pada ada sesuatu yang salah struktur teknologi informasi berkaitan erat dengan perlindungan terhadap ancaman terhadap sistem baik secara fisik maupun non fisik serta metode untuk mendeteksi dan memperbaiki kerusakan yang terjadi pada sistem (Umar et al., 2019). Keamanan sistem ini juga berkaitan dengan adanya kebijakan, prosedur serta mekanisme yang terjadi pada pengelolaan sistem dan infrastruktur teknologi informasi.

Sebuah infrastruktur teknologi informasi terutama yang berkaitan dengan sistem sangat penting untuk dijaga keamanannya meskipun sebagian dari pengelola infrastruktur teknologi informasi lebih mementingkan efisiensi biaya dan peningkatan kinerja dari sistem. Apabila sudah terjadi kerusakan yang ditimbulkan dari ancaman yang terjadi pada keamanan sistem maka perbaikan sistem tersebut akan lebih besar biayanya Dibandingkan dengan apabila dilakukan penjagaan dan pengamanan terhadap sistem tersebut.

3. METODE

Metode yang digunakan dalam penelitian ini adalah dengan cara pengukuran *level maturity* pada setiap kriteria yang mendukung kesimpulan pada domain DSS05 (De Haes et al., 2013). Untuk mendapatkan penilaian kriteria maka dilakukan wawancara dan observasi terhadap para pengelola sistem, pemangku kebijakan dan sistem itu sendiri.

Pertanyaan yang di sampaikan pada saat wawancara antara lain sebagai berikut:

A. Untuk Pemangku Kebijakan

1. Apakah sudah ada kebijakan Institusi dalam penyelenggara infrastruktur teknologi informasi?
2. Apakah kebijakan tersebut meliputi pengadaan, standar kinerja dan juga mengenai pemeliharaan dan keamanan sistem?
3. Apakah institusi menyadari bahwa keamanan sistem juga merupakan hal yang penting dalam infrastruktur teknologi informasi?
4. Apakah ada dalam kebijakan insitusi terkait perlindungan Informasi pribadi dari pengelola dan pengguna sistem?
5. Apakah ada pengaturan tertentu dalam manajemen password pada pengelolaan sistem dan teknologi informasi?

B. Untuk Pengelola Sistem

1. Apakah ada pembagian tugas yang jelas dalam pengelolaan sistem dan teknologi informasi?
2. apakah otorisasi penggunaan *password* pada sistem dan teknologi informasi sudah ada panduan atau aturannya?
3. apakah para pengelola sudah memahami bahwa

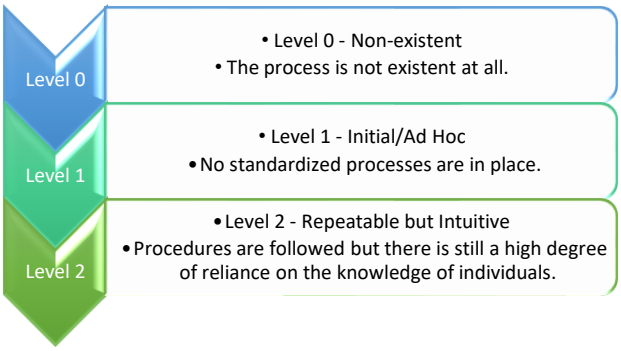
keamanan sistem adalah hal yang penting dalam infrastruktur teknologi informasi?

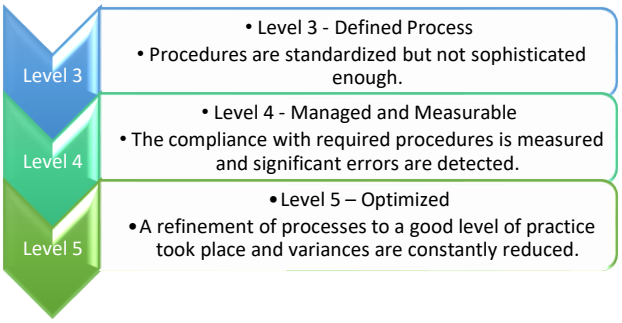
4. apakah para pengelola menyadari bahwa biaya yang timbul dari kerusakan keamanan sistem akan lebih besar daripada pemeliharaannya?
5. apakah para pengelola sistem sudah mengatur adanya pengelolaan privasi data personal dari pengelola dan juga pengguna sistem?
6. Teknik apa yang digunakan dalam meningkatkan privasi pengguna sistem, Apakah dilakukan teknik seperti teknologi kriptografi?
7. Apakah di terapkan teknis *two-steps authorisation* Dalam penggunaan sistem informasi dengan tujuan untuk mengurangi kemungkinan sistem diakses oleh pihak-pihak yang tidak berhak mengakses?
8. Apakah hal-hal terkait dengan integritas data dan sistem sudah disosialisasikan kepada para pengguna sistem?

4. HASIL DAN PEMBAHASAN

Dengan menerapkan metode penelitian tersebut, maka akan diperoleh hasil penelitian. Hasilnya berupa data kualitatif dari pertanyaan yang sudah disiapkan sebelumnya. Jawaban dari pertanyaan tersebut dianalisa dan kemudian diberikan bobot terhadap level maturity dari COBIT 5. Selain itu dilakukan juga pengukuran terhadap fitur umum COBIT 5 dalam menerapkan key process area yaitu terhada 5 hal: komitmen untuk melakukan, kemampuan untuk melakukan, kegiatan yang dilakukan, analisis pengukuran, dan verifikasi implementasi

Adapun level maturity yang dimaksud adalah dari rentang level 0-5.





Gambar 3. Maturity Level COBIT 5

Hasil pengukuran observasi terhadap Fitur Umum untuk menerapkan key process, adalah sebagaimana pada table 1 di bawah ini:

Tabel 1. Pengukuran Fitur Umum

No.	Fitur	Score Skala 0-5	Keterangan
1.	Komitmen	3,2	Komitmen dari organi-sasi/ institusi untuk implementasi sudah ada tetapi belum kuat
2.	Kemampuan	3,1	Kemampuan hardware, software dan brainware ada tetapi belum men-cukupi
3.	Kegiatan	2,3	Kegiatan yang dilakukan untuk keamanan sistem belum terencana dengan baik, belum ada struktur yang baik.
4.	Analisis	1,0	Baru akan dimulai ana-lisis terhadap keamanan sistem
5.	Verifikasi Implementasi	1,0	Penerapan keamanan sudah diverifikasi teta-pi masih di tahap awal
Score Rata-rata		2,14	

Selain mempertimbangkan penilaian pada fitur Umum COBIT 5, tentu saja dilakukan pembobotan terhadap pertanyaan yang disusun pada saat akan melakukan interview dan observasi. Tabel 2 dan 3 berturut-turut adalah hasil pengukuran terhadap instrument yang diukur data wawancara dengan pemangku kebijakan dan pengelola sistem.

Tabel 2. Hasil Wawancara kepada Pemangku Kebijakan

No	Pertanyaan	Kesimpulan
1.	Apakah sudah ada kebijakan institusi dalam penye-lenggaraan infrastruktur teknologi informasi?	Belum ada dokumen kebijakan dalam penyelenggaraan infrastruktur Teknologi

		Informasi, baik berupa SOP maupun panduan
2.	Apakah kebijakan tersebut meliputi pengadaan, standar kinerja dan juga mengenai pemeliharaan dan keamanan sistem?	Untuk kebijakan terkait pengadaan terdapat pada biro lain yaitu Biro Administrasi Umum, sedangkan untuk pemeliharaan sistem belum ada
3.	Apakah institusi menyadari bahwa ke-amanan sistem juga merupakan hal yang penting dalam infrastruktur teknologi informasi?	Sudah ada kesadaran terkait keamanan sitem akan tetapi belum dirancang prosedur keamanan sistem
4.	Apakah ada dalam kebijakan insitusi terkait perlindungan Informasi pribadi dari pengelola dan pengguna sistem?	Tidak ada kebijakan institusi terkait perlindungan informasi pribadi dari pengelola maupun pengguna sistem
5.	Apakah ada pengaturan tertentu dalam manajemen password pada pengelolaan sistem dan teknologi informasi?	Tidak ada pengaturan password, semua password dipegang oleh satu orang pengelola yaitu kepala BAA

Tabel 2. Hasil Wawancara kepada Pengelola Sistem

No	Pertanyaan	Kesimpulan
1.	Apakah ada pembagian tugas yang jelas dalam pengelolaan sistem dan teknologi informasi?	Hanya ada admin utama, 2 staff yang lain hanya sebagai operator saja.
2.	apakah otorisasi penggunaan *password* pada sistem dan teknologi informasi sudah ada panduan atau aturannya?	Belum ada panduan atau SOP terkait pembagian password
3.	apakah para pengelola sudah memahami bahwa keamanan sistem adalah hal yang penting dalam infrastruktur teknologi informasi?	Sudah ada pemahaman bahwa keamanan sistem adalah hal yang penting
4.	apakah para pengelola menyadari bahwa biaya yang timbul dari kerusakan keamanan sistem akan lebih besar daripada pemeliharaannya?	Sudah ada kesadaran bahwa biaya yang timbul dari kerusakan keamanan sistem akan lebih besar daripada pemeliharaannya
5.	apakah para pengelola sistem sudah mengatur adanya pengelolaan privasi data personal dari pengelola dan juga pengguna sistem?	Belum ada pengaturan pengelolaan privasi data personal dari pengelola dan juga pengguna sistem
6.	Teknik apa yang digunakan dalam meningkatkan privasi pengguna sistem, Apakah dilakukan teknik seperti teknologi kriptografi?	Belum ada Teknik tertentu terkait privasi pengguna.
7.	Apakah di terapkan teknik *two-steps authorisation* dalam penggunaan sistem informasi dengan tujuan untuk mengurangi kemungkinan sistem diakses oleh pihak-pihak yang tidak berhak mengakses?	Tidak ada penerapan Teknik *two-steps authorisation* Dalam penggunaan sistem informasi
8.	Apakah hal-hal terkait dengan integritas data dan sistem sudah disosialisasi-kan kepada para pengguna sistem?	Belum ada sosialisasi terkait dengan integritas data

Kemudian dari hasil penghitungan Maturity Level yang telah dilakukan pembobotan, maka diperoleh di angka 2,34.

5. KESIMPULAN DAN SARAN

Kesimpulan

Beberapa kesimpulan yang dapat diambil dari hasil penelitian ini adalah sebagai berikut:

1. Berdasarkan hasil penghitungan maturity level yang diuraikan pada bagian 4, maka dapat disimpulkan bahwa untuk COBIT 5 Domain DSS05 terkait keamanan sistem ada pada level 2,34, yang termasuk dalam skala level maturity 2 yaitu *repeatable but intuitive*.
2. Kepedulian dan kesadaran terhadap pentingnya keamanan sistem sudah terbangun tetapi tidak didukung oleh pengaturan kebijakan berupa panduan atau SOP yang terkait.
3. Strategi untuk perlindungan terhadap keamanan informasi berupa pengaturan password belum dilaksanakan.

Saran

Beberapa saran yang diajukan berdasarkan hasil penelitian ini adalah sebagai berikut:

1. Dari hasil penghitungan maturity level yang diperoleh pada penelitian ini, yaitu pada level 2, maka diharapkan Domain DSS05 terkait keamanan sistem berada pada level 4 yaitu *managed and measurable.*
2. Untuk mencapai level 4 perlu diadakan perbaikan pada keseluruhan pengelolaan infrastruktur teknologi informasi terutama dalam hal kebijakan yang dimulai dengan penyusunan panduan dan SOP terkait hal-hal seperti pengadaan sarana, pengaturan password, pengaturan wewenang, Teknik *two-steps verifications* dan sosialisasi kepada pengguna sistem.
3. Perlu diadakan audit secara menyeluruh terhadap tata kelola teknologi informasi yang meliputi semua domain yang ada pada COBIT 5 yaitu lan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS) dan Monitor and Evaluate (ME), untuk mendapatkan hasil evaluasi yang lebih lengkap.

Pustaka Acuan

Aini, Q., Rahardja, U., Madiistriyatno, H., & Setiaji, Y. D. M. (2018). Pengamanan Pengelolaan Hak Akses Web Berbasis Yii Framework. *Syntax: Jurnal Informatika*, *7*(1), 52-63.

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi SIMHP BPKP Menggunakan Standar ISO 27001. *Jurnal Tekno Kompak*, *11*(2), 41-44.

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307-324.

Imany, Y. D., Putra, W. H. N., & Herlambang, A. D. (2019). Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer e-ISSN*, *2548*, 964X.

Krisdiyawan, R. D., & Kuswantoro, R. H. (2017). AUDIT KEAMANAN SISTEM INFORMASI PADA RS MATA DR. YAP YOGYAKARTA MENGGUNAKAN FRAMEWORK COBIT 5. *Jurnal Ilmiah Manajemen Informasi dan Komunikasi*, *1*(1), 8-15.

Nuraeni, A., & Haryana, K. S. (2016). Penilaian Tata Kelola Teknologi Informasi Dengan Menambahkan Unsur Keamanan Menggunakan Framework Cobit 5 Pada Domain DSS. *Jurnal Computech & Bisnis*, *10*(2), 89-105.

Oktarina, T. (2017). Tata kelola teknologi informasi dengan Cobit 5. *J. Informanika*, *3*(2), 30-38.

Sulaeman, F. S. (2017). Audit Sistem Informasi Framework Cobit 5. *Media Jurnal Informatika*, *7*(2).

Swastika, I. P. A., Kom, M., & Putra, I. G. L. A. R. (2016). *Audit Sistem Informasi dan Tata Kelola Teknologi Informasi: Implementasi dan Studi Kasus*. Penerbit Andi.

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, *1*, 47-53.

Youssfi, K., Boutahar, J., & Elghazi, S. (2014). IT governance implementation: a tool design of COBIT 5 roadmap. 2014 Second World Conference on Complex Systems (WCCS),

Zainuddin, N., Winarno, W. W., Ningsi, N., Pasrun, Y. P., & Muliyadi, M. (2020). IT governance evaluation at the population and civil registry office in Kolaka district using COBIT 5 framework. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *6*(2), 86-95.

.