JCOSIS (Journal Computer Science and Information Syetem)
E-ISSN : 3032-5676
Volume : 01 | Nomor : 01 | Tahun 2024 | Hal 08-13
DOI Article : https://doi.org/10.61567/jcosis.v1i1.174

Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (Studi Kasus : PT Bpr Xyz)

Fernando Simamora [1]*, Vieri Putra kartika[1]
[1]Program Studi Informasi, Fakultas Teknik,
Universitas Mercu Buana, Indonesia
[1]*41819110078@student.mercubuana.ac.id*; [2] *41819110075@student.mercubuana.ac.id*

Abstrak.
Tujuan : Penelitian ini dilakukan dengan tujuan untuk mengevaluasi keamanan sistem informasi yang ada di PT BPR XYZ yang merupakan sebuah bank pengkreditan rakyat yang bergerak di bidang perbankan. Sektor perbankan adalah salah satu yang paling sering menjadi sasaran serangan peretasan atau kejahatan cyber dibandingkan dengan bidang lainnya,kejadian insiden keamanan termasuk siaran broadcast dari salah satu web server perusahaan dan serangan terhadap server perusahaan sering kali terjadi di PT BPR XYZ
Metode/Design/Pendekatan: Diperlukan pengukuran dan evaluasi terhadap PT. BPR Prima Kredit Mandiri untuk mengetahui Capability Level pada tata kelola keamanan sistem informasi di PT BPR XYZ dengan menggunakan framework COBIT 5 domain proses APO13 dan DSS05
Hasil/Temuan: Data yang digunakan dalam penelitian ini diperoleh melalui serangkaian wawancara, pengisian kuesioner, dan observasi. Hasil penelitian menunjukan Capability Level pada domain proses APO13 berada pada level 3 dan domain proses DSS05 berada pada level 3,sedangkan level yang diinginkan pada kedua domain tersebut adalah 4,sehingga terjadi Gap sebesar 1 untuk kedua domain tersebut.
Kebaharuan/Originalitas/Nilai: Setelah mengetahui Capability Level saat ini dan level yang diinginkan maka diberikan beberapa rekomendasi perbaikan yang dapat dilakukan organisasi.

Keywords: level kapabilitas, cobit_5, keamanan

Abstract.
Purpose: This study was conducted with the aim of evaluating the security of the information system at PT BPR XYZ which is a people's crediting bank engaged in banking. The banking sector is one of the most frequently targeted by hacking attacks or cyber crimes compared to other fields, the occurrence of security incidents including broadcast broadcasts from one of the company's web servers and attacks on company servers often occur at PT BPR XYZ
Methods/Study design/approach: Measurement and evaluation of PT. BPR Prima Kredit Mandiri to determine the Capability Level of information system security governance at PT BPR XYZ using the COBIT 5 framework of the APO13 and DSS05 process domains
Result/Findings: The data used in this study were obtained through a series of interviews, questionnaire filling, and observation. The results showed that the Capability Level in the APO13 process domain was at level 3 and the DSS05 process domain was at level 3, while the desired level in both domains was 4, so there was a gap of 1 for both domains.
Novelty/Originality/Value: After knowing the current Capability Level and the desired level, several recommendations for improvements that can be made by the organization are given.

Keywords: Capability_Level, cobit_5, Security

Article history:

Received, 2023-11-04
Revised, 2023-11-05
Accepted, 2023-12-04

*Corresponding author.
Fernando Simamora.
Email addresses: 41819110078@student.mercubuana.ac.id

PENDAHULUAN

Kemajuan pesat dalam Teknologi Informasi (TI) telah mengubahnya menjadi aspek yang sangat penting dalam pemenuhan kebutuhan perusahaan saat ini. Perusahaan mengakui bahwa TI dapat memberikan solusi bagi berbagai proses bisnis yang mereka jalankan. Oleh karena itu, penerapan tata kelola TI menjadi suatu kebutuhan yang mendesak untuk memudahkan evaluasi dan monitoring sistem informasi [1].

Keamanan sistem informasi menjadi isu utama bagi perusahaan dan organisasi saat ini. Beberapa masalah yang dihadapi termasuk kurangnya evaluasi tingkat kematangan keamanan sistem, kekurangan dalam pendokumentasian laporan, pedoman, dan SOP terkait kebijakan keamanan sistem informasi. Evaluasi tingkat kematangan keamanan sistem informasi menjadi penting guna memastikan kelangsungan dan keberlanjutan proses bisnis serta meningkatkan keamanan sistem informasi yang telah ada [2].

Untuk mencapai keamanan sistem informasi yang memadai, perlu diterapkan seperangkat kontrol yang sesuai, termasuk kebijakan, proses, prosedur, struktur organisasi, serta perangkat lunak dan keras. Kontrol-kontrol ini perlu ditetapkan, dimonitor, direview, dan ditingkatkan guna memastikan bahwa tujuan bisnis dan keamanan yang spesifik bagi organisasi terpenuhi. Keamanan informasi bertujuan untuk mengatasi berbagai masalah dan tantangan, baik dari segi teknis maupun non-teknis, seperti ketersediaan, kerahasiaan, dan integritas data [3].

PT. BPR Prima Kredit Mandiri, salah satu bank perkreditan rakyat di Kota Tangerang, menyadari pentingnya informasi yang akurat dan terintegrasi dalam pengambilan keputusan. Oleh karena itu, perusahaan ini perlu menerapkan sistem informasi dan teknologi informasi yang tepat untuk memberikan pelayanan terbaik kepada stakeholder-nya. Data dan informasi yang dimiliki oleh PT. BPR Prima Kredit Mandiri sangatlah banyak dan penting, mulai dari data nasabah, data jaminan kredit, laporan keuangan, dan lain sebagainya. Oleh karena itu, pengelolaan data ini sangat penting untuk menjaga kelancaran operasional perbankan [4][5].

Namun, sektor perbankan juga menjadi sasaran serangan peretasan dan kejahatan siber yang tinggi. Data menunjukkan bahwa sektor perbankan sering menjadi target serangan phishing, serangan malware, dan serangan berbasis jaringan. Untuk itu, PT. BPR Prima Kredit Mandiri perlu melakukan evaluasi tingkat keamanan informasi guna mengidentifikasi kelemahan dan risiko keamanan yang ada serta mengembangkan rekomendasi untuk meningkatkan keamanan sistem informasi secara efektif [6].

Dalam rangka melakukan evaluasi tingkat kapabilitas tata kelola keamanan sistem informasi, PT. BPR Prima Kredit Mandiri dapat menggunakan framework COBIT 5. COBIT 5 menyediakan model proses yang relevan dengan aktivitas TI dalam lima domain proses yang terkait. Framework ini memungkinkan perusahaan untuk mengidentifikasi tanggung jawab dan akuntabilitas terkait keamanan sistem informasi serta memandangnya sebagai bagian integral dari strategi dan operasional perusahaan secara keseluruhan [7].

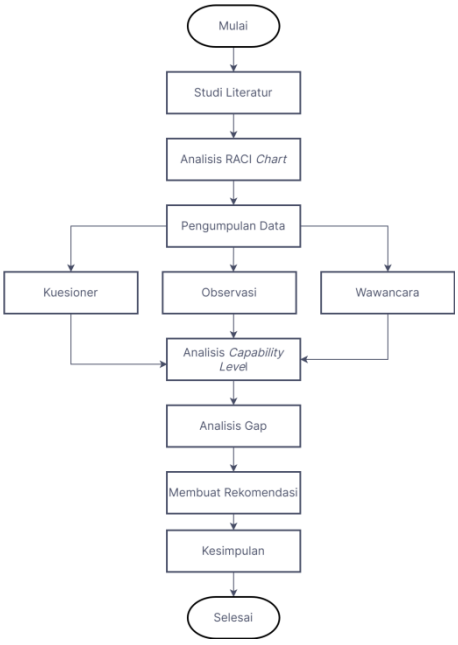
Penelitian ini bertujuan untuk memberikan evaluasi mengenai tingkat kapabilitas tata kelola keamanan sistem informasi pada PT. BPR Prima Kredit Mandiri dan memberikan rekomendasi perbaikan yang diperlukan. Dalam penelitian ini, fokus diberikan pada proses APO13 (Manage Security) dan DSS05 (Manage Security Services) dalam framework COBIT 5. Dengan menggunakan COBIT 5, diharapkan PT. BPR Prima Kredit Mandiri dapat mengembangkan strategi keamanan yang efektif melalui proses teknis, kontrol, dan alat yang relevan [8]-[10] .

Melalui evaluasi dan perbaikan yang dilakukan, diharapkan PT. BPR Prima Kredit Mandiri dapat meningkatkan tata kelola dan keamanan sistem informasi mereka, serta memastikan kepatuhan terhadap standar keamanan yang berlaku.

METODE PENELITIAN

Penelitian ini menggunakan dua metode penelitian, yaitu metode kualitatif melalui studi kasus dan metode kuantitatif dengan penggunaan kuesioner untuk mengumpulkan data dalam bentuk angka yang nantinya akan digunakan untuk menghitung Capability Level. Adapun tahapan penelitian ditunjukkan oleh gambar 1.

JCOSIS (Journal Computer Science and Information Syetem)
E-ISSN : 3032-5676
Volume : 01 | Nomor : 01 | Tahun 2024 | Hal 08-13
DOI Article : https://doi.org/10.61567/jcosis.v1i1.174



Gambar 1 Alur Tahapan Penelitian

Studi Literatur

Studi literatur tentang framework COBIT 5 untuk melaksanakan Evaluasi Tata Kelola Keamanan Sistem Informasi. Fokus yang dipelajari adalah domain APO untuk proses APO13 dan domain DSS05 yang akan digunakan sebagai fokus penelitian.

Analisis RACI *chart*

Analisis RACI Chart melibatkan empat peran utama dalam sebuah proses : responsible (bertanggung jawab), accountable (bertanggung jawab utama), consulted (yang dikonsultasikan), dan informed (yang diberitahu). Konsep ini diperkenalkan oleh framework COBIT 5 untuk menggambarkan tingkatan tanggung jawab dalam sebuah proses, berdasarkan peran dan struktur yang berbeda. Untuk menentukan responden yang tepat untuk mengisi kuesioner sesuai dengan peran mereka, diperlukan pemetaan antara RACI Chart setiap proses dengan sumber daya manusia yang tersedia.

Pengumpulan Data

Proses pengumpulan data dalam penelitian ini melibatkan penggunaan beberapa metode, yaitu kuesioner, observasi, wawancara, dan studi pustaka. Kuesioner digunakan untuk mengukur tingkat kemampuan dalam mengelola tata kelola sistem informasi berdasarkan kerangka kerja COBIT 5 contoh kuesioner bisa dilihat pada gambar 2. Observasi dilakukan melalui pengamatan langsung terhadap kegiatan yang terkait dengan tata kelola teknologi informasi di PT BPR XYZ. Wawancara dilakukan untuk memperoleh informasi yang lebih mendalam mengenai visi, misi, pengelolaan TI, struktur organisasi, program kerja, peraturan/kebijakan, serta kendala yang terkait dengan tata kelola teknologi informasi. Studi pustaka dilakukan untuk mengumpulkan data dari jurnal-jurnal terkait evaluasi keamanan, COBIT 5, dan metodologi yang digunakan, serta penelitian-penelitian yang mendukung penelitian ini. Dengan menggunakan berbagai metode pengumpulan data tersebut, penelitian ini bertujuan untuk memperoleh informasi yang komprehensif dan akurat mengenai tata kelola sistem informasi di PT BPR XYZ.

Analisis Capability Level

Dalam kuesioner untuk mengetahui Capability Level, terdapat 4 pilihan skala penilaian yang terdiri dari N (Not Achieved) dengan pencapaian 0-15%, P (Partially Achieved) dengan pencapaian >15%-50%, L (Largely Achieved) dengan pencapaian >50%-85%, dan F (Fully Achieved) dengan pencapaian >85%-100%. Dari hasil kuesioner ini, akan diperoleh Capability Level dari process practice yang dipilih

Analisis Gap

Setelah mengevaluasi kondisi tata kelola sistem keamanan teknologi informasi saat ini berdasarkan hasil perhitungan Capability Level, langkah selanjutnya adalah melakukan analisis gap. Analisis gap ini bertujuan

JCOSIS (Journal Computer Science and Information Syetem)
E-ISSN : 3032-5676
Volume : 01 | Nomor : 01 | Tahun 2024 | Hal 08-13
DOI Article : https://doi.org/10.61567/jcosis.v1i1.174

untuk mengidentifikasi perbedaan antara Capability Level yang telah tercapai dengan level target yang ingin dicapai.

Membuat Rekomendasi

Membuat rekomendasi dari hasil evaluasi tata kelola keamanan sistem informasi. Rekomendasi tersebut diharapkan dapat membantu PT BPR XYZ untuk mencapai level capability yang diharapkan.

HASIL DAN PEMBAHASAN

Seteleah menentukan responden menggunakan RACI Chart dan memberikan kuesioner kepada 3 responden,ditentukan penilaian tingkat kemampuan tiap domain proses yang bisa di lihat pada tabel di bawah ini.

Tabel 1. Penilaian Proses APO 13

Responden	Penilaian Proses APO 13								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Manager		100	100	100	100	83,3	16,6	0	0	0
Head Programmer		100	100	100	80	83,3	16,6	0	0	0
Supervisor Infrastructure		100	100	100	80	66,6	16,6	0	0	0
Rata Rata		100	100	100	86,6	77,7	16,6	0	0	0
Nilai		F	F	F	F	L	N			

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori Fully achieved (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai false jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses APO13 berada pada level 3 (Established), yang artinya proses telah teretapkan dan ada pendekatan yang terstruktur dalam menjalankan dan mengawasi sistem manajemen keamanan informasi. Prosedur keamanan yang mengatur penggunaan aset dan sumber daya keamanan TI di perusahaan telah ditetapkan dan diterapkan sesuai dengan tujuan. Meskipun belum mencapai tingkat prediktabilitas penuh, perusahaan telah membangun fondasi yang kuat untuk menjalankan proses keamanan yang terukur dan terkelola dengan baik.

Berdasarkan Tabel diatas, hasil pencapaian PA 3.1 Process Definition menunjukkan nilai 86,6 (Fully Achieved), yang mengindikasikan bahwa perusahaan telah berhasil mendefinisikan proses dengan baik. Hal ini berarti tujuan kinerja sistem keamanan telah diidentifikasi dan ditetapkan dengan jelas.

Sementara itu, hasil pencapaian PA 3.2 Process Deployment menunjukkan nilai 77,7 (Largely Achieved), yang menggambarkan bahwa perusahaan telah mencapai sebagian besar dari pencapaian penuh pada proses implementasi. Proses keamanan yang telah didefinisikan telah diimplementasikan secara memadai dengan batasan yang telah ditentukan.

Tabel 2. Penilaian Proses DSS 05

Responden	Penilaian Proses DSS 05									
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Manager		100	100	100	100	80	20	0	0	0
Head Programmer		100	100	100	80	80	20	0	0	0
Supervisor Infrastructure		100	100	80	80	80	20	0	0	0
Rata Rata		100	100	93,3	86,6	80	20	0	0	0
Nilai		F	F	F	F	L	P			

Berdasarkan prinsip model penilaian proses maka suatu proses harus meraih kategori Fully achieved (F) untuk dapat melanjutkan penilaian ke level kapabilitas selanjutnya, level 0 bernilai false jika level 1 terpenuhi (ISACA, 2012).

Nilai tingkat kapabilitas untuk proses DSS05 berada pada level 3 (Established), yang artinya proses pengelolaan layanan keamanan telah didirikan dan ada pendekatan yang terstruktur dalam menjalankan dan mengoperasikannya. Meskipun belum mencapai tingkat prediktabilitas penuh, perusahaan telah berhasil membangun fondasi yang kokoh dalam mengelola layanan keamanan dengan baik.

Dalam level ini, proses DSS05 telah berjalan dan dioperasikan dengan batasan yang ditentukan untuk mencapai hasil yang diharapkan dari pengelolaan layanan keamanan. Perusahaan telah mengimplementasikan langkah-langkah yang diperlukan dan telah mengenali pentingnya pengelolaan layanan keamanan. Meskipun masih ada ruang untuk peningkatan dan penyesuaian, perusahaan telah mencapai tingkat yang memadai dalam memastikan keamanan sistem sesuai dengan tujuan yang telah ditetapkan.

Berdasarkan Tabel diatas, hasil pencapaian PA 3.1 Process Definition menunjukkan nilai 86,6 (Fully Achieved), yang mengindikasikan bahwa perusahaan telah berhasil mendefinisikan proses dengan baik. Hasil ini menunjukkan bahwa perusahaan telah mengenal sejauh mana hasil pengukuran dapat digunakan untuk memastikan bahwa performa proses mendukung tujuan perusahaan.

Sementara itu, hasil pencapaian PA 3.2 Process Deployment menunjukkan nilai 80 (Largely Achieved), yang menunjukkan bahwa perusahaan telah mencapai sebagian besar dari pencapaian penuh pada proses implementasi. Proses yang telah didefinisikan termasuk dalam pengelolaan keamanan dan pelayanan aplikasi di dalam proses TI telah diimplementasikan dengan cukup baik, dan memberikan dukungan yang lebih efektif dan efisien dalam pelaksanaan proses TI.

Dengan demikian, perusahaan telah mencapai tingkat kapabilitas yang memadai untuk PA 3.1 dan PA 3.2 dalam konteks DSS05. Meskipun masih ada ruang untuk perbaikan dan peningkatan, perusahaan telah berhasil dalam mendefinisikan dan mengimplementasikan proses pengelolaan layanan keamanan dengan baik.

Berdasarkan hasil evaluasi yang menunjukkan nilai capability level 3 untuk domain APO13 dan DSS05 dan terdapat Gap sebesar 1 pada setiap proses nya,berikut adalah beberapa rekomendasi yang dapat dipertimbangkan untuk meningkatkan level capability ke level 4 :

Rekomendasi untuk Proses APO13 :

- Membentuk Unit Keamanan Informasi (Information Security Unit) unit khusus yang bertanggung jawab atas pengelolaan keamanan informasi secara menyeluruh. Unit ini akan fokus pada pengembangan, implementasi, dan pemantauan kebijakan, prosedur, dan kontrol keamanan yang relevan dengan APO13. Tim ini akan melibatkan spesialis keamanan informasi yang memiliki pengetahuan dan keahlian yang diperlukan untuk meningkatkan kemampuan pengelolaan keamanan.
- Peningkatan Rencana Pengelolaan Kinerja: Perkuat rencana pengelolaan kinerja terkait dengan keamanan sistem. Sertakan indikator kinerja yang relevan, target kinerja yang realistis, dan jadwal pengukuran yang teratur. Pastikan rencana mencakup langkah-langkah tindakan perbaikan yang jelas.
- Peningkatan Monitoring dan Pelaporan Kinerja: Tingkatkan mekanisme pemantauan dan pelaporan kinerja sistem keamanan. Pastikan ada sistem yang mengumpulkan data kinerja secara akurat dan menyajikan laporan terstruktur. Hal ini akan membantu mengidentifikasi tren kinerja dan mengambil tindakan perbaikan yang tepat.
- Peningkatan Tindakan Perbaikan: Perbaiki respons terhadap hasil pengukuran yang tidak mencapai target. Identifikasi akar penyebab masalah, ambil tindakan perbaikan yang efektif, dan pastikan pemantauan untuk memverifikasi keberhasilan tindakan tersebut.

Rekomendasi untuk Proses DSS05 :

- Membentuk Tim Pengembangan Produk Keamanan (Security Product Development Team) tim khusus yang bertanggung jawab untuk pengembangan dan pengelolaan produk keamanan yang terkait dengan DSS05. Tim ini akan berfokus pada pengembangan produk keamanan yang sesuai dengan kebutuhan perusahaan, melakukan pengujian yang memadai, dan memastikan integrasi yang baik dengan infrastruktur yang ada.
- Peningkatan Identifikasi Produk dan Layanan Keamanan: Identifikasi produk dan layanan keamanan yang sesuai dengan kebutuhan perusahaan. Pastikan kebijakan dan pedoman terkait pengelolaan produk keamanan ditetapkan dan diterapkan dengan baik.
- Peningkatan Proses Pengembangan dan Penerapan Produk Keamanan: Perbaiki proses pengembangan, pengujian, dan penerapan produk keamanan. Pastikan produk dan layanan keamanan terintegrasi dengan infrastruktur dan sistem yang ada secara efektif.

Peningkatan Evaluasi dan Peningkatan Produk Keamanan: Lakukan evaluasi dan perbaikan produk keamanan secara berkala. Pastikan ada mekanisme evaluasi yang memadai untuk meningkatkan produk keamanan sesuai dengan kebutuhan perusahaan.

KESIMPULAN

Hasil terhadap tata kelola sistem keamanan teknologi informasi di PT. BPR PRIMA KREDIT MANDIRI menunjukkan tingkat kemampuan atau Capability Level sebagai berikut. Pada domain APO, tingkat kemampuan atau Capability Level pada proses APO13 (manage security) berada pada level 3, yaitu established process. Hal ini mengindikasikan bahwa proses yang terimplementasi telah mencapai tujuan prosesnya dan telah dikelola dengan baik. Pada domain DSS, tingkat kemampuan atau Capability Level pada proses DSS05 (manage security

services) juga berada pada level 3, yaitu established process. Hasil ini menunjukkan bahwa proses yang terimplementasi telah mencapai tujuan prosesnya dan telah dikelola dengan baik hasil evaluasi.

REFERENSI

[1] A. Habiba, "Evaluasi Tata Kelola Keamanan Sistem Informasi Menggunakan Framework COBIT 5 pada PT. Tsabita Cake," JATISI (Jurnal Teknik Informatika Dan Sistem Informasi), vol. 8, no. 2, 2021. [Online]. Available: https://doi.org/10.35957/jatisi.v8i2.838.

[2] I. J. Aritonang, E. D. Udayanti, and N. Iksan, "Audit Keamanan Sistem Informasi Menggunakan Framework Cobit 5 (APO13)," ITEJ (Information Technology Engineering Journals), vol. 3, no. 2, 2018. [Online]. Available: https://doi.org/10.24235/itej.v3i2.2.

[3] E. Handoyo, "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55," Jurnal CoSciTech (Computer Science and Information Technology), vol. 1, no. 2, 2020. [Online]. Available: https://doi.org/10.37859/coscitech.v1i2.2199.

[4] I. G. Y. Shamgita, I. G. L. A. Raditya, and I. G. J. E. Putra, "Analisis Dan Evaluasi Tata Kelola Teknologi Informasi USSI Software Menggunakan Framework COBIT 5 Pada PT . BPR Naga," Jurnal Ilmiah Teknik Informatika Dan Sistem Informasi, vol. 9, no. 1, pp. 67-74, 2020.

[5] A. Andrianti and S. Assegaf, "Analisis dan Perancangan IT Governance Menggunakan Framework COBIT Pada Pengelolaan Data PT. BPR US," Jurnal Manajemen Sistem Informasi, vol. 3, no. 2, 2018.

[6] ISACA, "Process Assessment Model: Using COBIT 5," USA: ISACA, 2013.

[7] M. A. Wicaksono, Y. Rahardja, and H. P. Chernovita, "Analisis Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Domain EDM," JSiI (Jurnal Sistem Informasi), vol. 7, no. 1, 2020. [Online]. Available: https://doi.org/10.30656/jsii.v7i1.2027.

[8] M. F. A. Effendi, A. R. Perdanakusuma, and B. T. Hanggara, "Evaluasi Kapabilitas Keamanan Teknologi Informasi pada Proses APO13 dan DSS05 berdasarkan Framework COBIT 5 (Studi pada Dinas Komunikasi dan Informatika Kota Malang)," Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer, vol. 4, no. 2.

[9] U. Cahyani, I. Aknuranda, and others, "Evaluasi Layanan BPJSTK Mobile Dengan Menggunakan Domain Deliver, Service and Support Berdasarkan Framework COBIT 5 (Studi Kasus: BPJS …. … Teknologi Informasi Dan …," vol. 2, no. 8, 2018.

[10] M. Noveri and Z. Musliyana, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Evaluation of Information Technology Governance Using COBIT 5 Framework)," Journal of Informatic and Computer Science, vol. 6, November.