AUDIT KEAMANAN SISTEM INFORMASI MENGGUNAKAN *FRAMEWORK* COBIT 5 (APO13)

Ivana Junita Aritonang [a,*], Erika Devi Udayanti [a], Nur Iksan [b]
[a] Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[b]Fakultas Teknik, Universitas Negeri Semarang
[a,b] Semarang, Indonesia
Email Address*: 112201405196@mhs.dinus.ac.id

Abstract

Penelitian ini bertujuan untuk mengidentifikasi dan mengukur tingkat kematangan keamanan sistem informasi. Permasalahan yang sering dialami pada salah satu objek penelitian yaitu belum adanya evaluasi tingkat kematangan terhadap keamanan sistem informasi. Untuk menghindari permasalahan yang ada dimasa yang akan datang, maka diperlukannya audit keamanan sistem informasi. Audit ini menggunakan framework COBIT 5 dengan fokus pada proses APO13 (Manage Security) yang bertujuan untuk menjaga dampak dan kejadian insiden keamanan informasi dalam tingkat risiko yang dapat di selesaikan oleh perusahaan. Hasil dari penelitian ini diketahui tingkat kapabilitas dari proses APO13 yaitu Level 0 (*Incomplete Process*) dengan status L (*Largely Achieved*) yang artinya sudah mencapai sebagian besar pengelolaan keamanan sistem informasi. Level 1 (*Performed Process*) dengan pencapaian level sebesar 50% dengan status P (*partially achieved*) yang artinya keamanan sistem informasi sudah tercapai sebagian. Selanjutnya juga pada Level 2,3 dan 5 yang memperoleh hasil rata-rata diatas 60% dengan status L.

Keywords: COBIT 5, APO13, Audit Sistem Informasi, Keamanan Sistem Informasi.

I. PENDAHULUAN

Dalam meningkatkan proses bisnis saat ini, perusahaan ataupun organisasi tidak dapat tepisah dengan teknologi informasi. Teknologi informasi semakin memberikan banyak kemudahan kepada penggunanya. Kemudahan yang diberikan dikarenakan berkembangnya teknologi informasi yang semakin pesat dan luas di berbagai macam bidang kehidupan yang juga akan memberikan dampak positif dan negatif di dalamnya, agar penggunaannya dapat berjalan dengan maksimal maka diperlukannya tata kelola TI yang baik dan benar supaya keberadaannya dapat membantu mencapai tujuan bisnis perusahaan ataupun organisasi tersebut. Suatu perusahaan ataupun organisasi harus dapat mengatasi masalah yang ada. Tak hanya berfokus pada tata kelola TI semata, melainkan juga harus menjaga dan meningkatkan mutu keamanan sistem informasi perusahaan tersebut. Keamanan informasi meliputi perlindungan pada kerahasiaan (*confidentiality*), ketersediaan (*availability*) informasi dan integritas (*integrity*) [1].

Keamanan sistem informasi merupakan masalah yang utama bagi perusahaan, organisasi maupun pemerintahan. Beberapa masalah yang ada seperti belum pernah dilakukannya evaluasi tingkat kematangan terhadap keamanan sistem, kurangnya pendekomentasian laporan, pedoman dan SOP (*Standart Operasional System*) mengenai kebijakan terkait keamanan sistem informasi. Untuk itu, perlu dilakukan evaluasi tingkat kematangan keamanan sistem informasi untuk menjamin kelangsungan dan proses bisnis yang ada supaya dapat memberikan perbaikan yang memberikan peningkatan keamanan sistem informasi yang sudah ada saat ini [2].

Dari permasalahan yang ada, maka diperlukan evaluasi tingkat kematangan keamanan sistem informasi menggunakan COBIT 5. Karena COBIT 5 merupakan salah satu kerangka kerja yang banyak digunakan pada *IT Governance*. Pada pelaksanaannya, keamanan sistem informasi terdiri atas aspek teknis aspek non teknis. Framework COBIT memiliki kelebihan dengan adanya metrik, acuan dan pelaksanakan audit, serta adanya tata kelola dan manajemen yang menyeluruh yang dapat melandasi pemilihan COBIT 5

dalam audit keamanan sistem informasi [1]. Penelitian ini menggunakan COBIT 5 dengan domain proses APO13 sebagai framework untuk dapat mengukur secara teknik dan non teknis tingkat kematangan sistem keamanan informasi. Evaluasi yang dilakukan terkait keamanan data, jaringan dan server dengan mengukur kapabilitas proses keamanan sistem informasi yang relevan.

II. PENELITIAN TERKAIT

Terdapat beberapa penelitian mengenai audit tata kelola TI menggunakan COBIT 5, diantaranya adalah penelitian yang membahas mengenai tata kelola keamanan sistem informasi menggunakan COBIT 5 dengan fokus proses APO13 dan DSS05 [3]. Mekanisme pengamanan pada penelitian tersebut belum tertuang kedalam Standar Operasional Prosedur (SOP) perusahaan. Selain itu, belum memiliki unit khusus yang berfokus pada aktivitas pengamanan informasi dan belum pernah melakukan evaluasi menggunakan framework COBIT 5. Sehingga mengakibatkan *security incident* yang kerap muncul berupa *broadcast* dari salah satu *web server* perusahaan serta serangan yang mengarah ke server perusahaan. Hasil dari penelitian ini adalah tingkat kemampuan atau *capability level* domain APO13 dan DSS05 berada pada level 1 dan masing-masing proses menunjukkan bahwa proses implementasi sudah mencapai tujuan prosesnya, tetapi belum ada manajemennya.

Penelitian lainnya mengenai tata kelola TI menggunakan COBIT 5 yaitu pada audit keamanan sistem informasi [4]. Penelitian tersebut masih belum mampu mencapai level yang ditargetkan yaitu level 3 (*Established Process*). Penelitian dilakukan melalui 5 proses dalam COBIT 5 dan hanya mampu mencapai level 1 (*Incomplete Process*). Dengan rincian hasil sebagai berikut : proses EDM03 memiliki nilai sebesar 1,13 , proses APO12 memiliki nilai sebesar 1,24 , proses APO13 memiliki nilai sebesar 1,22 , proses BAI06 memiliki nilai sebesar 1,18 dan Proses DSS05 memiliki nilai sebesar 1,54.

Penelitian lain mengenai tata kelola TI menggunakan COBIT 5 yaitu pada analisis keamanan informasi data center [5] yang mengalami permasalahan terjadinya peretasan dan *shell injection* yaitu penyusupan *malware* kedalam sistem sehingga mengakibatkan beberapa domain tidak dapat berjalan dengan baik. Penelitian tersebut dilakukan melalui 5 proses dan hasil penelitian ini menunjukkan bahwa tingkat kapabilitas saat ini berada di level 2 (*Managed Process*). Hasil yang pencapaian masing-masing proses yaitu proses APO13 memiliki nilai sebesar 1,54 dan DSS05 memiliki nilai sebesar 1,70. Hasil kapabilitas berada di level 2 (*Managed Process*) maka ditetapkan nilai kapabilitas selanjutnya yang harus dicapai selanjutkan pada level 3 (*Estabilished Process*) dengan menutup gap dan membuat detail kebijakan, pengelolaan dengan standart yang jelas. Sehingga mampu mencapai tujuan dan dapat mengimplementasikan kebijakan dan standar yang dibuat.

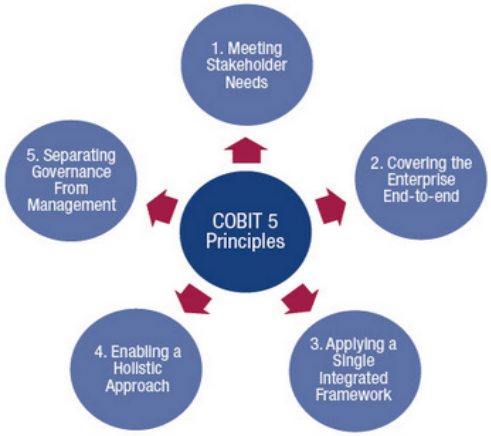
Dari beberapa penelitian terkait tersebut maka framework COBIT 5 khususnya domain APO (*Align, Plan, and Organize*) pada domain proses APO13 (*Manage Security*) dapat membantu perusahaan dalam mengaudit tata kelola informasi khususnya dalam mengevaluasi tingkat kematangan keamanan sistem informasi pada perusahaan.

III. AUDIT DAN TATA KELOLA COBIT 5

Audit tata kelola TI dapat diartikan sebagai aktifitas pengumpulan dan mengevaluasi dari bukti-bukti yang ada untuk proses penentuan apakah proses TI yang berlangsung dalam organisasi tersebut telah dikelola sesuai dengan standar dan dilengkapi dengan objek kontrol untuk mengawasi penggunannya serta apakah telah memenuhi tujuan bisnis organisasi secara efektif dengan menggunakan sumber daya yang efektif [6]. Keamanan informasi digunakan untuk melindungi kerahasiaan, integritas dan ketersediaan asset informasi, baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, dan teknologi [5]. Keamanan

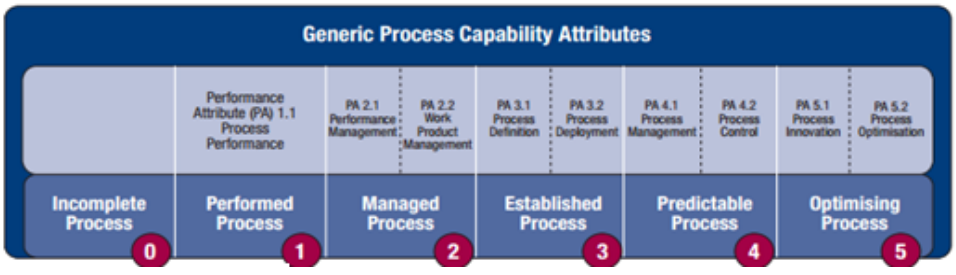
informasi berkembang dalam tiga konsep utama yang menjadi standar utama dalam industri keamanan yang sering disebut dengan *CIA triangle* yaitu: *Confidentiality*,*Integrity*, dan *Availability*. Ancaman informasi dapat merugikan perusahaan ataupun organisasi terkait yang sedang membutuhkan informasi tersebut. Ada beberapa bentuk ancaman informasi yang dapat mengganggu proses bisnis perusahaan yaitu [7] *interruption, interception, modification, fabrication.*

COBIT (Control Objective for Information and related Technology) merupakan sekumpulan berbagai dokumentasi-dokumentasi dan sebagai panduan dalam proses implementasi tata kelola teknologi informasi (*IT Governance*), COBIT sebagai framework penting dalam membantu pengguna,auditor dan manajemen untuk menjadi jembatan pemisah (gap) untuk kebutuhan control, risiko bisnis,dan berbaga macam masalah teknis yang berkaitan dengan TI. COBIT 5 merupkan kerangka kerja untuk memanajemen dan mengelola semua yang berkaitan dengan teknologi informasi mulai dari pemenuhan kebutuhan para *stakeholder* akan teknologi informasi. COBIT 5 memiliki prinsip dasar untuk tata kelola dan manajemen TI. Kelima prinsip ini diharapkan dapat membangun tata kelola perusahaan atau organisasi yang dapat mengoptimalkan tingkat resiko daan memberikan keuntungan bagi perusahaan atau organisasi sebagaimana ditunjukkan pada Gambar 1 [6].



Gambar 1. Lima Prinsip Dasar COBIT 5

Proses APO13 merupakan proses pendefinisian, pengoprasian dan pengawasan sistem yang diterapkan perusahaan untuk memanajemen keamanan informasi yang dimiliki. Proses ini bertujuan untuk menjaga kejadian dan dampak atas insiden keamanan informasi tidak boleh lebih dari level resiko yang ditentukan perusahaan. Indikator kapabilitas proses adalah kemampuan proses dalam meraih tingkat kapabilitas yang dibentuk oleh atribut proses. Bukti atas indikator kapabilitas proses akan mendukung penilaian atas pencapaian atribut proses [8]. Dimensi kapabilitas dalam model penilaian proses mencakup enam tingkat kapabilitas sebagaimana ditunjukkan pada Gambar 2.



Gambar 2. Model proses kapabilitas pada COBIT 5

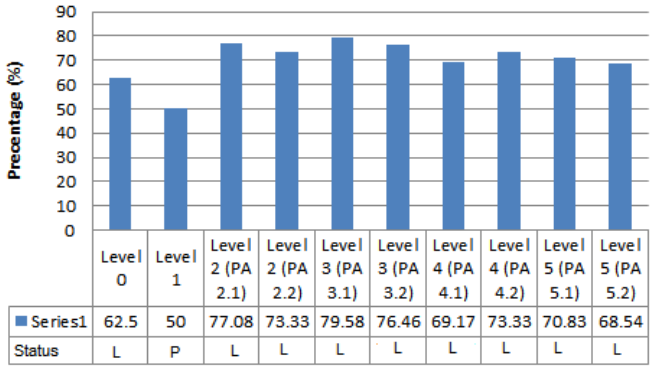
IV. HASIL DAN PEMBAHASAN

Penelitian ini berfokus pada permasalahan terkait masalah keamanan pada tata kelola sistem informasi pada suatu perusahaan. Hasil dari penelitian ini digunakan untuk merancang strategi perbaikan yang diharapkan agar dapat mendukung perusahaan dalam mencapai tujuan bisnisnya. Studi dokumen berupa SOP dilakukan terkait manajeman keamanan yang mencakup SOP *troubleshooting* internet, SOP *active directory* (manajemen user), SOP *storage* (web based), SOP *storage server* (operasional), SOP *streaming server*. Selanjutnya juga dilakukan wawancara kepada beberapa narasumber yang memiliki peran dan tanggung jawab pada manajeman keamanan. Tabel 1 berikut membahas hasil wawancara terhadap beberapa narasumber.

Tabel 1. Hasil Wawancara Terkait Manajeman Keamanan Sistem Informasi

Topik Pertanyaan	Hasil Pembahasan
APO13.1 (membang`un dan memelihara sistem manajemen keamanan informasi)	
Bentuk keamanan sistem informasi yang ada	Sistem *service*, akses user password dan *firewall*
Keberadaan devisi khusus untuk keamanan sistem informasi	Hanya ada devisi IT
SOP (standar operasional prosedur) mengenai keamanan sistem informasi	SOP khusus keamanan informasi belum ada
APO13.2 (mendefinisikan dan mengelola rencana penanganan keamanan informasi)	
Prosedur penyelesaian jika terjadi permasalahan keamanan sistem informasi	Dilakukan pengamatan terhadap log penggunaan.
Rencana perbaikan dan peningkatan keamanan sistem informasi	Peningkatan dilakukan jika ditemukan celah keamanan dan jika tidak ditemukan maka hanya dilakukan maintenance saja.
Manajeman hak akses sistem informasi	Manajeman hak akses diatur disetiap unit-unit kerja
APO13.3 (mengawasi dan mengkaji sistem manajemen keamanan informasi)	
Cara melakukan pemantauan untuk keamanan sistem informasi	Pemantauan dilakukan melalui log sistem dan password serta melalui CCTV pada beberapa titik
Enkripsi pada sistem informasi	Hanya ada beberapa sistem informasi yang terenkripsi

Pengisian kuesioner dilakukan terhadap beberapa responden untuk melihat pencapaian level serta penilaia proses dari setiap atribut. Gambar 3 berikut adalah hasil rincian dari setiap level sesuai dengan proses atribut dan rincian perhitungan kuesionernya.



	Level 0	Level 1	Level 2 (PA 2.1)	Level 2 (PA 2.2)	Level 3 (PA 3.1)	Level 3 (PA 3.2)	Level 4 (PA 4.1)	Level 4 (PA 4.2)	Level 5 (PA 5.1)	Level 5 (PA 5.2)
Series1	62.5	50	77.08	73.33	79.58	76.46	69.17	73.33	70.83	68.54
Status	L	P	L	L	L	L	L	L	L	L

Gambar 3. Perhitungan rating pada tiap level

Hasil dari penelitian ini ingin meningkatkan pengelolaan keamanan sistem informasi secara bertahap maka level target yang akan di capai selanjutnya yaitu berada pada level 2 yang memungkinkan peningkatan keamanan sistem informasi akan berlanjut sampai pada peningkatan level tertinggi yaitu pada level 5. Level 0 (*Incomplete Process*) dengan status L (*Largely Achieved*) yang artinya sudah mencapai sebagian besar pengelolaan keamanan sistem informasi. Level 1 (*Performed Process*) dengan pencapaian level sebesar 50% dengan status P (*partially achieved*) yang artinya keamanan sistem informasi sudah tercapai sebagian. Selanjutnya juga pada Level 2,3 dan 5 yang memperoleh hasil rata-rata diatas 60% dengan status L.

V. KESIMPULAN

Berdasarkan hasil kegiatan pengabdian yang dilakukan, maka dapat disimpulkan bahwa Tingkat keamanan pada sistem informasi pada perusahaan X dengan menggunakan perhitungan tingkat kapabilitas pada saat ini telah mencapai level 1 (*Performed Process*) sebesar 50% dengan tingkat *Managed Process* yang memiliki status P (*Partially Achieved*) yang menunjukkan bahwa pengelolaan keamanan sistem informasi yang ada secara garis besar belum tercapai dengan baik dikarenakan target yang ingin dicapai yaitu 80 % hingga 90% maka diperlukan peningkatan dalam keamanan sistem informasi.

REFERENCES

[1] E. N. D. A. Dewi Ciptaningrum, “COBIT 5 Sebagai Metode Alternatif Bagi Audit Keamanan Sistem informasi (Sebuah Usulan Untuk Diterapkan di Pemerintah Kota Yogyakarta),” Seminar Nasional Teknologi Informasi dan Multimedia 2015, July 2015.

[2] P. s. sukanto, “PERANCANGAN SISTEM MONITORING PERANGKAT JARINGAN BERBASIS ICMP DENGAN NOTIFIKASI TELEGRAM,” ITEJ (INFORMATION TECHNOLOGY ENGINEERING JOURNALS), vol. 2, no. 2, 2017.

[3] S. Y. T. M. Raja Gantino Mufti, “Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses APO13 dan DSS05 (Studi Pada PT. Martina Berto Tbk),” Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, vol. 1, pp. 1622-1631, July 2017.

[4] E. N. D. A. Dewi Ciptaningrum, “Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5,” Seminar Nasional Teknologi Informasi dan Komunikasi 2015, pp. 65-74, 12 July 2015.

[5] A. L. K. W. Iik Muhamad Malik Matin, “Analisis Keamanan Informasi Data Center Menggunakan COBIT 5,” Jurnal teknik informatika, vol. 10, pp. 119-128, 2017.

[6] R. Sarno, Audit Sistem dan Teknologi Informasi, Surabaya: ITS press, 2009.

[7] R.T.Asmono, Proteksi Aset Informasi, Semarang, 2014.

[8] ISACA, COBIT 5 Enabling Processes, USA: IT Governance Institute, 2012.