AUDIT KEAMANAN LABORATORIUM 2 FASILKOM UNIVERSITAS SUBANG BERBASIS COBIT 5

Bambang Tjahjo Utomo
FakultasIlmu Komputer, Universitas Subang

bercahaya2019@gmail.com

Abstrak

Laborotarium komputer sebagai tempat mahasiswa melakukan praktek merupakan tempat yang penting bagi pembelajaran mahasiswa. Agar proses pembelajaran berjalan lancar maka keamanan laboratorim harus dijaga. Untuk itu perlu dilakukan proses audit untuk memeriksa apakah proses pengamanannya sudah berjalan sesuai dengan standar yang baik.

Standar yang dipakai dalam audit ini adalah cobit 5, yang dibuat oleh ISACA. Sedangkan metode yang digunakan dalam penelitian ini adalah metode self assessment dari ISACA.

Hasil dari audit Keamanan Laboratorim 2 Fasilkom Universitas Subang berbasis cobit ini , laboratorium Fasilkom Universitas subang ini ada pada Capability level 1, Performed, dimana proses pengamanan sudah tercapai, tetapi belum dikelola dengan baik.

Keywords: Audit, laboratorium , cobit 5.

Pendahuluan

Praktikum merupakan proses pembelajaran yang sangat penting bagi mahasiswa. Dengan melakukan praktikum , maka mahasiswa bisa lebih memahami tentang sebuah materi. Melalui praktikum mahasiswa bisa mengembangkan proses berpikirnya dengan lebih baik, yaitu dengan melakukan percobaan percobaan untuk membuktikan atau mempraktekkan sebuah teori atau menyelesaikan sebuah tujuan tertentu yang ingin dicapai

Laboratorium sebagai tempat mahasiswa melakukan praktikum terdiri dari beberapa komputer , yang terhubung dalam sebuah jaringan komputer. Jaringan komputer dibuat agar komputer komputer tersebut bisa saling berhubungan, saling berbagi sumber daya, dan agar bisa dilakukan pengelolaan dengan baik.

Keamanan komputer adalah hal yang sangat penting dalam sebuah jaringan komputer, terutama kalau jaringan computer tersebut terhubung dengan jaringan internet. Jaringan computer yang terkena virus, spyware dan lain, lain bisa menyebabkan jaringan computer tidak dapat berfungsi dengan baik, dan bahkan bisa tidak berfungsi sama sekali . Untuk itu pengaman sangat diperlukan dalam sebuah jaringan computer.

Audit keamanan dalam sebuah jaringan computer perlu dilakukan untuk melihat apakah proses pengamanan.sudah dilakukan dengan baik . Untuk melakukan proses audit terhadap sebuah jaringan computer diperlukan sebuah standar, yang dipakai sebagai acuan dalam melakukan proses audit tersebut. COBIT 5 adalah salah satu standar yang baik , yang dapat dipakai sebagai acuan dalam proses audit sebuah jaringan komputer

Kajian Teori

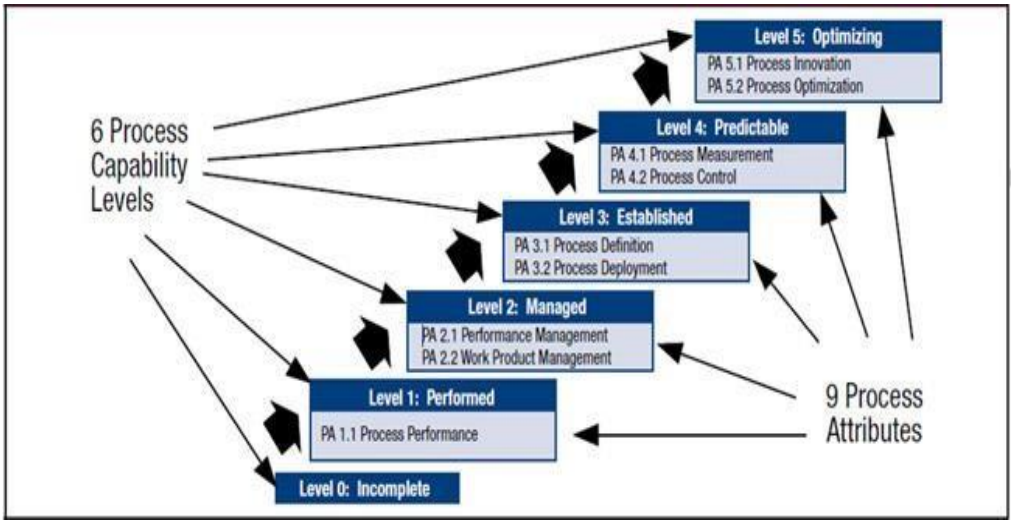
COBIT adalah kerangka kerja untuk manajemen dan tata kelola Teknologi Informasi [1] Ini adalah serangkaian praktik dan prosedur terbaik yang membantu organisasi untuk mencapai tujuan strategis melalui penggunaan sumber daya yang tersedia secara efektif dan meminimalkan risiko TI. Di sisi lain Cobit bisa dipakai sebagai sebuah standar untuk audit teknologi infomasi. Cobit dipakai untuk memeriksa berapa level capability suatu proses teknologi infomasi. Cobit 5 sebagai sebuah versi dari Cobit mememiliki 5 tingkat atau level capability sebuah proses.

Proses proses pada Cobit 5 bisa dibagi menjadi 2 bagian , yaitu bagian tata kelola dan bagian manajemen. Pada bagian manajemen proses dibagi menjadi 4 domain, yaitu Domain Align,Plan and Organise (APO) , Build, Acquire and Implement (BAI) , Decision Support and Service (DSS) dan Monitor,Evaluation and Asses (MEA). Dalam Domain DSS terdapat 5 proses yaitu Manage Operations (DSS01), Manage Service,Request and Incident (DSS02), Manage Problems (DSS03),Manage Continuity(DSS04) dan Manage security service (DSS05).

Proses Manage security service (DSS05) memiliki sub proses / praktek manajemen : melindungi dari malware, mengelola keamanan jaringan dan konektifiti nya, mengelola keamanan end point, mengelola identitas user dan akses logical, mengelola akses fisik asset Teknologi informasi, mengelola dokumen dokumen sensitive dan piranti output, memonitor infrastruktur untuk memastikan kejadian kejadian yang membahyakan.

Pada setiap proses bisa dilakukan audit , untuk mengetahi berapa level capability (kemampuan) nya. capability setiap proses yang dinilai dinyatakan sebagai tingkat capability dari 0 hingga 5 [2] . level 0 adalah Proses tidak diimplementasikan atau gagal mencapai tujuan prosesnya. Pada tingkat ini, hanya ada sedikit atau tidak ada bukti adanya sistematik pencapaian tujuan proses. Pada level 1 (Peformed) ,Proses yang diterapkan mencapai tujuan prosesnya. Pada level 2 (Managed), Proses yang dilakukan s diimplementasikan dengan cara yang terkelola (direncanakan, dipantau dan disesuaikan) dan hasil kerjanya mapan (Establish), terkontrol, dan terpelihara(Maintened) dengan tepat. Pada level 3 (Established), Proses yang dikelola diimplementasikan menggunakan proses yang ditentukan (defined) yang mampu mencapai hasil prosesnya. Pada level 4 (Predicted), Proses yang ditetapkan beroperasi dalam batas yang ditentukan untuk mencapai hasil prosesnya. Pada level 5 (Optimized), Proses yang dapat diprediksi terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan saat ini dan yang diproyeksikan.

Dalam COBIT, ukuran kapabilitas didasarkan pada sembilan atribut proses, seperti yang ditunjukkan pada gambar 1. Setiap atribut berlaku untuk kemampuan proses tertentu. Atribut proses digunakan untuk menentukan apakah suatu proses telah mencapai kemampuan yang diberikan.



Gb 1. 9 atribut proses[2]

Metode

Metode audit yang dipakai dalam penelitian ini adalah metode self assessment process ISACA. Metode ini dapat dilihat pada gambar 2 dibawah ini.

Gb 2. Self Assesment Process[2]

Suatu proses dikatakan mencapai level kapabilitas bila atribut pada level tersebut bernilai *"fully achieved"* (F) dengan *range* nilai 85% sampai dengan 100%" atau *"largely achieved"* (L)

dengan *range* nilai 50% sampai dengan 85%, tetapi bila nilai keseluruhan tidak mencapai F, maka proses tidak dapat naik ke level berikutnya.

Hasil dan Pembahasan

Hasil audit diperoleh dari kuesioner yang telah di jawab oleh 3 responden yang mengelola laboratorium Fasilkom 2 komputer. Dari jawaban ketiga responder tersebut, ketiganya menjawab F(Fully), nilai 85 – 100 % , pada pertanyaan pada level 0, dan menjawab L(large), nilai 50-85 % pada pertanyaan level 1. Sehingga Dapat diketahui bahwa pengelolaan layanan keamanan komputer pada laboraturium komputer berada pada level capability 1 (performed).

Tabel 1
Rekapitulasi *Capability Leve*l DSS05
laboratorium Komputer 2 Fasilkom

DSS05		*Mengelola Layanan Keamanan (Manage services security)*									
		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
Rating dari kriteria	R1	F	L	N	N	N	N	N	N	N	N
	R2	F	L	N	N	N	N	N	N	N	N
	R3	F	L	N	N	N	N	N	N	N	N
Capability level yang dicapai			1								

Dari data diatas dapat diketahui bahwa pengelolaan layanan keamanan komputer pada laboratorium komputer 2 Fasilkom sudah mencapai tujuannya, sehingga praktikum dilaboratorium komputer 2 Fasilkom berjalan dengan cukup baik.
Harapan dari pimpinan fakultas ilmu komputer, bahwa layanan keamanan komputer dapat dikelola dengan baik, atau berada di level 2 (Managed).
Agar dapat berada di level 2 (Managed), maka atribut kinerja dan produk kerja harus dapat dikelola dengan baik.

Penutup

Audit , self assesment assessment , keamanan laboratorium Fasilkom 2 telah dilakukan pada penelitian ini . Dengan audit self assessment terhadap keamanan laborotarium diharapkan dapat diketahui capability dar proses layanan keamanan komputer laboratorium komputer 2 Fakultas illmu komputer, sehingga dapat diperoleh keamanan sistem komputer yang lebih baik.

Daftar Pustaka

[1] ISACA, COBIT® 5, USA, 2012
[2] ISACA, Self assessment guide using COBIT® 5 , USA, 2012