Audit Layanan Teknologi Informasi Berbasis *Information Technology Infrastructure Library* (ITIL)

Didin Herlinudinkhaji[1], April Firman Daru[2]
Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi Universitas Semarang
Jl. Soekarno Hatta Tlogosari Semarang 50196
e-mail : didin@usm.ac.id, firman@usm.ac.id

Abstract *– IT Service Management is one way to manage information technology services. Technology services need to be managed well in order to get the output in the form of information needed by management. To improve information technology services for the better, it required audits include audit of information technology services. Audit of information technology services made to determine the feasibility of the related denngan information technology, in this case the author focuses on information technology security issues. Information technology security audit was made to determine the level of security for information technology services, the extent to which such information can be up to those entitled to receive, whether the information is actually available, whether the information is confidential. To be able to measure the security level of information technology services, the authors chose to use the method of Information Technology Infrastructure Library Version 3 (ITIL V3). ITIL is a set that consists of Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. In this case the author focuses on the design service on the part of information security management, in this section explain how a service is said to be good if it meets the 8 points that have been standardized internationally.*

Keywords: ITSM; Auditof Information Technology; ITIL;InformationTechnologyServices

Abstrak - IT Service Management adalah salah satu cara untuk mengelola layanan teknologi informasi. Layanan teknologi perlu dikelola dengan baik untuk mendapatkan output dalam bentuk informasi yang dibutuhkan oleh manajemen. Untuk meningkatkan layanan teknologi informasi untuk lebih baik, diperlukan audit meliputi audit layanan teknologi informasi. Audit layanan teknologi informasi dilakukan untuk menentukan kelayakan teknologi informasi denngan terkait, dalam hal ini penulis berfokus pada isu-isu keamanan teknologi informasi. Audit keamanan teknologi informasi dibuat untuk menentukan tingkat keamanan untuk layanan teknologi informasi, sejauh mana informasi tersebut bisa sampai kepada yang berhak menerima, apakah informasi tersebut benar-benar tersedia, apakah informasi tersebut bersifat rahasia. Untuk dapat mengukur tingkat keamanan layanan teknologi informasi, penulis memilih untuk menggunakan metode InformationTechnologyInfrastructureLibraryVersi 3 (ITIL V3). ITIL adalah set yang terdiri dari Layanan Strategi, Jasa Desain, Jasa Transisi, Layanan Operasi, dan terus-menerus Peningkatan Pelayanan. Dalam hal ini penulis berfokus pada layanan desain pada bagian dari manajemen keamanan informasi, pada bagian ini menjelaskan bagaimana layanan dikatakan baik jika memenuhi 8 poin yang telah distandarisasi secara internasional.

Kata Kunci: ITSM; Auditof Information Technology; ITIL; Information Technology Services

PENDAHULUAN

Penelitian tentang *IT Service Management* (ITSM) menunjukkan bahwa ISO/IEC 20000, ITIL (V2 dan V3) dan CMMI-SVC adalah proses *IT Service Management* (ITSM) model referensi yang paling sering digunakan [10]. Sehingga service managemen tmenjadi lebih penting dalam bidang manajemen Teknologi Informasi (TI) tentang pengelolaan TI secara efisien dan mengatur layanan TI dengan perubahan sewaktu-waktu agar dapat menyesuaikan kebutuhan [11]).

Teknologi informasi telah menjadi kebutuhan dalam bisnis, konsekuensi dari sistem keamanan informasi adalah pelanggaran keamanan terhadap sistem menjadi barang mahal [11]. Kajian ini menunjukkan bahwa sistem informasi menjadi sarana utama bagi organisasi untuk mencapai tujuan. Oleh karena itu, tata kelola teknologi informasi sangat diperlukan untuk menghasilkan sistem informasi yang baik. Sehingga organisasi perlu melakukan penelitian pada strategi pelaksanaan, metode, pengukuran kinerja, keselarasan,dan tata kelola teknologi informasi yang menunjukkan kebutuhan untuk organisasi [6]. Dengan melakukan tata kelola teknologi informasi, organisasi dapat meningkatkan kualitas layanan teknologi informasi, mengurangi resiko, meningkatkan kinerja penghantaran nilai dan mengurangi biaya layanan teknologi informasi [18] .

Salah satu kerangka kerja untuk melakukan tata kelola TI adalah *Information Technology Infrastructure Library* (ITIL), ITIL dirancang khusus untuk pengelolaan pelayanan TI, selain itu ITIL juga dapat menjadi pedoman bagi organisasi untuk merancang dan menjalankan sistem tata kelola TI [18]. ITIL merupakan kerangka paling populer dan berpengaruh untuk menerapkan IT Service Management [9]. Pelaksanan ITIL tidak sulit jika memahami betul yang harus dilakukan, diprioritaskan, dan disesuaikan dengan pedoman ITIL. Pada pelaksanaannya organisasi seringkali tidak mematuhi pedoman ITIL akibatnya implementasi ITIL memakan waktu yang panjang, mahal, dan berisiko.

Ketika kelola TI sudah dilakukan dengan baik, maka langkah yang paling penting bagi organisasi adalah menjamin keamanan sistem informasi [16]. Keamanan informasi merupakan aset yang bernilai sehingga informasi tersebut harus dijaga kerahasiaannya, integritasnya, dan ketersediaannya [20]. Oleh karena itu, organisasi perlu menerapkan sistem keamanan terhadap hardware dan softwarenya. Tujuan dari keamanan sistem ini adalah untuk menjamin keamanan sistem agar tercipta integritas, keberlanjutan, dan kerahasiaan dari pengolahan data [16].

Keamanan informasi menjadi bagian yang paling penting bagi perusahaan untuk mendapatkan keuntungan dalam bisnis [5]. Sehingga keamanan informasi harus dijaga dari ancaman yang berusaha merusak, memasukkan data dan mengganti data dengan yang lain, bahkan sampai menghilangkan data.

Untuk mendapatkan keamanan sistem informasi maka organisasi perlu melakukan evalusasi secara berkala terhadap keamanan sistem informasi. Evaluasi berkala dapat dilakukan dengan menggunakan audit internal terhadap keamanan sistem informasi tersebut. Audit internal maupun eksternal dapat menjadi salah satu cara untuk mengevaluasi keamanan informasi[11]. Audit sistem informasi dilakukan untuk dapat menilai apakah teknologi informasi

yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien [25]. Salah satu cara untuk mengevaluasi terhadap keamanan informasi adalah dengan mengujikeamanan entitas informasi, entitas informasi itu terdiri dari manusia, perangkat lunak, perangkat keras, multimedia, jaringan [11].

TINJAUAN PUSTAKA

Penelitian Terkait

Simple Information Security Audit Process (SISAP) dibuat untuk audit keamanan informasi berdasarkan prosesnya [12]. SISAP dibuat berdasarkan ISO 17799 dan BS 7799.2 yang terdiri dari 10 bukti keamanan informasi, 36 tujuan keamanan informasi, dan 127 persyaratan sebagaimana disesuaikan dengan ISO 17799. SISAP dibuat dengan menggunakan analisis model probabilitas dan *Fuzzy sets.*

Meningkatnya kompleksitas sistem informasi menyebabkan meningkatnya risiko terhadap pelanggaran bisnis, hal itu kemudian mendorong diciptakannya kebutuhan untuk alat audit secara *online* [1] . *On Line Audit Tools* (OLAT) dibuat untuk dapat mempermudah kegiatan audit perusahaan. Kegiatan audit umumnya dilakukan secara manual dengan mendatangkan seorang auditor dengan sedikit berbantuan komputer. OLAT dibuat dengan menggunakan *database*, hal ini dapat mempermudah kegiatan audit sehingga dapat mempercepat proses pengambilan kebijakan secara cepat.

Sistem dan proses auditor menjamin kebenaran pemrosesan informasi dan integritas data yang dikumpulkan untuk tujuan audit keuangan [7]. Audit ini berfokus pada pengendalian aplikasi untuk perusahaan yang memproses data keuangan dan menunjukkan bagaimana aplikasi tersebut dapat dibangun untuk memenuhi sistem dan prosesyang dipersyaratkan sesuai dengan desain auditor. Auditor menguji setiap objek bisnis keuangan untuk kepatuhan dengan empat sifat yaitu kelengkapan (*Completeness*), akurasi (*Accuracy*), validitas (*Validity*), danAkses terbatas (*Restricted access*) atau disebut dengan istilah CAVR model.

Menggunakan konsep keamanan informasi diperlukan untuk mengkategorikan temuan audit, mengidentifikasi isu-isu temuan dalam laporan, terutama keamanan, manajemen data center, fisik keamanan, dan perencanaan [8]. Penelitian ini menggunakan klasifikasi *common body of knowledge* (CBK) didasarkan pada keamanan yang terjadi pada pusat data yang menjadi masalah keamanan utama yang dihadapi pada era modern.

Layanan yang disediakan oleh organisasi dirancang dengan dukungan infrastruktur TI yang besar. Oleh karena itu untuk mendapatkan layanan yang terbaik adalah dengan menerapkan pengelolaan sumber daya yang membentuk infrastruktur TI [15]. Penelitian ini membahas tentang pengelolaan proses manajemen risiko berbasis manajemen TI dan kerja sistem.

ITIL adalah kerangka kerja umum yang menggambarkan *best practice* dalam manajemen layanan teknologi informasi [9]. Penelitian yang dilakukan oleh Mc Naughton menggunakan data wawancara sebagai data yang disesuaikan dengan ITIL dan ITSM.

Landasan Teori

1. Audit Sistem Informasi/Teknologi Informasi

Audit merupakan proses atau aktivitas yang sistematik, independen, dan terdoku-mentasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara objektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan yang ditetapkan [20].

Audit sistem informasi dilakukan untuk dapat menilai apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien [25]. Audit sistem informasi difungsikan sebagai alat evaluasi organisasi terhadap penggunaan teknologi informasi dan kemanfaatannya terhadap organisasi.

Kegiatan audit dilakukan untuk mengevaluasi terhadap bukti atau temuan dan melaporkan ketidak sesuaian tersebut dengan aturan yang sudah ditentukan [21] serta pengevaluasian bukti-bukti atas informasi untuk menentukan dan melaporkan tingkat kesesuaian informasi tersebut dengan kriteria-kriteria yang telah ditentukan.

Audit teknologi informasi merupakan serangkaian pengawasan, evaluasi, dan pengendalian dari infrastruktur teknologi informasi secara menyeluruh. Audit teknologi informasi dapat juga diterapkan bersama dengan audit internal maupun audit eksternal.

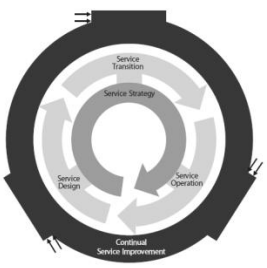
2. ITSM (IT Service Management)

ITSM *(Information Technology Service Management)* merupakan metode pengelolaan sistem teknologi informasi yang terpusat pada pelanggan, layanan TI, perjanjinan tentang layanan TI, dan penanganan fungsi TI [6]. ITSM atau manajemen layanan teknologi informasi menitikberatkan pada layanan terhadap pelanggan, pelanggan diberi fasilitas kenyamanan dan kemudahan dalam transaksi bisnis melalui teknologi informasi.

IT Service Management didefinisikan sebagai pengelolaan dari semua proses yang bekerja sama untuk memastikan bahwa kualitas layanan yang diberikan sudah sesuai dengan kebutuhan pelanggan (Menken, 2009).

3. Information Technology Infrastructure Library (ITIL)

ITIL adalah kerangka kerja umum yang menggambarkan *best practice* dalam manajemen layanan teknologi informasi [9] . ITIL menyediakan kerangka kerja bagi tata kelola teknologi informasi, "membungkus layanan", dan berfokus pada pengukuran terus-menerus dan perbaikan kualitas layanan teknologi informasi yang diberikan, baik dari sisi bisnis dan perspektif pelanggan [23][24]. Fokus ini merupakan faktor utama dalam keberhasilan ITIL dan telah memberikan kontribusi untuk penggunaan produktif dan memberikan manfaat yang diperoleh organisasi dengan pengembangan teknik dan proses sepanjang organisasi ada [23][24]. Gambar 1 menunjukkan siklus hidup ITIL yang terdiri dari 5 tahap yang meliputi *Service Strategy, Service Design, Service Transition, Service Operation, dan Continual Service Improvement* [23][24].



Gambar 1. Siklus hidup ITIL

Siklus hidup ITIL dimulai dari *service strategy,* pada proses ini organisasi menganalisa kebutuhan bisnis. Pada proses *service design* organisasi melakukan perubahan terhadap pola bisnis dengan mendesain infrastruktur Teknologi Informasi, kualitas layanan Teknologi Informasi, melakukan kebijakan terhadap keamanan Teknologi Informasi, dan melakukan pengukuran terhadap layanan. *Service transition* berfokus untuk memberikan layanan terbaik pada semua layanan. Fokus dari s*ervice operation* adalah memberikan nilai kepada bisnis dan memastikan bahwa nilai ini disampaikan. *Continual service improvement* melakukan evaluasi terus menerus untuk meningkatkan kualitas layanan pada siklus di bawahnya.

Pada siklus hidup ITIL ini, hanya dilakukan pada tahapan *service design* yang fokus penelitian pada proses *information security management. Service design* adalah sebuah tahap dalam siklus layanan dan elemen yang penting di dalam proses perubahan bisnis (Cartlidge, 2007).

A. Tujuan keamanan informasi

Tujuan dari manajemen keamanan informasi adalah untuk menyelaraskan keamanan TI dengan keamanan bisnis dan memastikan bahwa keamanan informasi dikelola dengan efektif pada seluruh layanan dan Manajemen Layanan[23][24]

B. Lingkup area

Lingkup area manajemen keamanan informasi harus jelas sesuai dengan kerja dalam bidang teknologi informasi [23][24]. Proses manajemen keamanan informasi harus menjadi titik fokus untuk semua masalah keamanan IT, dan harusmemastikan bahwa kebijakan keamanan informasi diproduksi, dipelihara dan ditegakkanyang mencakup penggunaan dan penyalahgunaan dari semua sistem dan layanan TI[23][24].

C. Nilai Bisnis

Information Security Management (ISM) memberikan jaminan proses bisnis dengan menegakkan keamanan yang sesuaikontrol dalam semua bidang TI dan mengelola risiko TI sejalan dengan bisnis danproses manajemen risiko perusahaan[23][24].

Perusahaan dalam mencapai tujuan bisnisnya tidak terlepas dari nilai bisnis perusahaan tersebut. Keterjamninan bisnis menjadi penting manakala organisasi ingin eksis dalam bisnisnya, bisnis dapat berjalan dengan baik jika informasi yang disampaikan sesuai dengan tujuan perusahaan. Oleh karena itu, manajemen keamanan informasi diperlukan untuk menjamin proses bisnis dengan menegakkan kontrol dalam semua bidang TI dan mengelola risiko.

Dengan meningkatnya kepuasan pelanggan, maka dapat mengakibatkan jumlah pelanggan meningkat hal ini akan mempengaruhi nilai bisnis itu sendiri. Pelanggan mendapatkan pelayanan sesuai dengan kebutuhan pelanggan, pelanggan merasa nyaman dalam bertransaksi, dan pelanggan merasa dihargai selayaknya sebagai pelanggan.

D. Kebijakan

Semua organisasi penyedia layanan TI harus dapat memastikan bahwa organisasi memiliki kebijakan dan kontrol keamanan yang diperlukan untuk memantau dan menegakkan kebijakan [23][24].Kebijakan organisasi meliputi :

1) Kerangka kerja keamanan

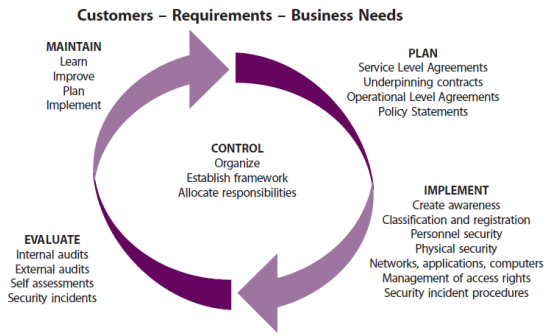
Kerangka keamanan yang membahas aspek strategi, kontrol, dan regulasi. Kontrol keamanan informasi berkaitan dengan standar keamanan, prosedur keamanan, dan pedoman yang mendukung kebijakan keamanan informasi.

2) Kebijkan keamanan informasi

Semua bidang keamanan informasi yang meliputi keamanan data; keamanan password; user; akses kontrol; keamanan email; antivirus dan sebagainya semuanya harus mematuhi kebijakan tentang keamanan informasi.

Sistem manajeman keamanan informasi

Pada bagian ini melibatkan 4 komponen penting diantaranya *people, proses, product and technology, partner and supplier*.Gambar 2 menunjukkan kerangka kerja untuk mengelola keamanan informasi.



Gambar 2. Kerangka kerja untuk mengelola informasi

E. Proses kegiatan, metode, dan teknik

Tujuan dari proses *Information Security Management* (ISM) adalah untuk memastikan bahwa aspek keamanan layanan teknologi informasi dan semua kegiatan manajemen layanan dikelola dengan tepatdan dikendalikan sesuai dengan kebutuhan bisnis dan risiko[23][24].

F. Masukan, keluaran, dan antarmuka

Pada tahapan ini dipicu banyak peristiwa sehingga langkah yang paling penting adalah melakukan perubahan disetiap masukan, proses, dan keluaran.Perubahan kebijakan-kebijakan tersebut dapat mempengaruhi semua aspek, termasuk aspek keamanan terhadap layanan teknologi informasi.

G. Manajen informasi

Semua informasi yang diperlukan mencakup semua kontrol keamanan, risiko, pelanggaran, proses, dan laporan yang diperlukan untuk mendukung dan memelihara kebijakan keamanan informasi dan sistem manajemen keamanan informasi [23][24].

H. Tantangan, CSF (critical success factor), dan risiko

Keamanan teknologi informasi merupakan tanggungjawab di semua lini dan keamanan taknologi informasi harus dilindungi dengan baik.

4. Uji validitas

Uji validitas berhubungan dengan seberapa aktual dapat dikatakan valid [18]. Pengukuran dikatakan valid jika mengukur tujuannya dengan nyata atau benar dan pengukuran dikatakan tidak valid jika pengukurannya menyimpang dari tujuannya [18]

Uji validitas didapatkan dari membandingkan nilai r tabel dibandingkan dengan r hitung. Jika r tabel lebih besar dari r hitung maka dinyatakan valid, begitu juga sebaliknya. r tabel diperoleh berdasarkan persamaan (1)

$$r = \frac{t}{\sqrt{dt + t^2}} \qquad (1)$$

Untuk mendapatkan nilai r tabel, harus mengetahui terlebih dahulu nilai dari t tabel. t tabel didapatkan dengan melihat lampiran yang terdapat pada buku statistika.

5. Uji reliabilitas

Uji reabilitas berhubungan dengan seberapa akurat dapat diandalkan [18] . Pengukuran yang reliabel (dapat diandalkan) adalah pengukurannya dapat dipercaya. Pengukuran yang dapat dipercaya adalah pengukuran yang akurat dan konsisten [18] terhadap beberapa subjek yang sama dan diperoleh hasil yang tidak berbeda.

Reliabilitas yang digunakan dengan menghitung korelasi total antaritem [18] dan *cronbach's alpha*. Perhitungan reliabilitas korelasi total antaritem terlebih dahulu mencari korelasi antaritem kemudian menjumlahkan total korelasi semua item yang diuji dibagi jumlah item.Nilai *cronbach's alpha* yang dapat diterima tergantung dari penelitiannya. Tabel 1 menunjukkan batasan skor reliabilitas *cronbach's alpha* [18]. Koefisien *cronbach's alpha* ditunjukkan oleh persamaan (2).

$$\alpha = \frac{k}{k-1}\left(\frac{\sum \sigma_{xi}^2}{\sigma_x^2}\right) \quad (1)$$

Tabel 1. Batasan skor *cronbach's alpha* [18]

Skor	Reliabilitas
< 0,50	Rendah
0,50 – 0,60	Cukup
0,61 – 0,80	Tinggi
0,81 – 1,00	Sangat Tinggi

6. Uji korelasi

Uji korelasi digunakan untuk mengetahui hubungan antar variabel [18], apakah hasil dari korelasi tersebut bernilai negatif atau positif. Jika hasil dari korelasi tersebut bernilai positif maka hubungan tersebut searah dan jika hasil dari korelasi tersebut bernilai negatif maka hubungan tersebut tidak searah.

Uji korelasi digunakan untuk mengetahui koefisien korelasi untuk masing-masing item. Uji korelasi yang digunakan dengan bantuan microsoft excel dan SPSS.

METODE PENELITIAN

Bahan penelitian

Bahan penelitian adalah hasil survei kuesioner kepada pengguna layanan TI dan pengambil kebijakan TI.

A. Kuesioner

Kuesioner dari pelanggan TI sebanyak 19 pertanyaan yang berhubungan dengan layanan yang diberikan oleh pihak pengelola TI ke pelanggan.

B. Wawancara

Wawancara ini dilakukan untuk mendapatkan data yang berhubungan dengan kebijakan TI, teknik wawancara ini penulis lakukan dengan menyebarkan pertanyaan ke bagian pengambil kebijakan TI. Pertanyaan terdiri dari 8 bagian atau 8 kebijakan yang disusun berdasarkan standar ITIL V3.

Bagian 1 tentang kebijakan tujuan organisasi, bagian 2 tentang ruang lingkup manajemen keamanan TI, bagian 3 tentang nilai bisnis manajemen keamanan TI, bagian 4 tentang kebijakan dan konsep dasar terhadap teknologi informasi, bagian 5 tentang antifitas proses dan metode, bagian 6 tentang perubahan kebijakan keamanan teknologi informasi, bagian 7 tentang model standar penilaian TI, dan bagian 8 tentang tanggungjawab manajemen terhadap keamanan TI. Kedelapan bagian tersebut masing-masing bagian dilengkapi dengan tujuan audit yang bertujuan untuk mendapatkan hasil audit sesuai dengan standar ITIL V3.

C. Observasi

Observasi ini dilakukan dengan mengamati perangkat teknologi informasi. Perangkat teknologi informasi berupa perangkat keras, perangkat lunak, dan sumber daya manusia.

Alat penelitian

Alat penelitian yang digunakan adalah sebagai berikut :

A. Perangkat keras

Mencakup perangkat keras yang digunakan untuk mengelola sistem informasi dengan spesifikasi : Prosesor minimal speed

2.00 GHz; RAM minimal 512 MB; dan Hardisk minimal free space 1 GB.

B. Perangkat lunak

Perangkat lunak yang digunakan berupa sistem operasi windows 7, microsoft office 2007, adobe reader, microsoft visual basic 6.0, Sql, dan SPSS.

HASIL DAN PEMBAHASAN

Hasil penelitian

Hasil penelitian tentang audit layanan teknologi informasi berbasis *Information Technology Infrastructure Library* (ITIL) versi 3 berupa tool audit layanan TI berbasis ITIL Versi 3 yang dapat digunakan untuk mengevaluasi terhadap layanan teknologi informasi terutama pada proses *service design* yang mengacu pada keamanan teknologi informasi.

Penelitian ini juga sebagai ukuran untuk melakukan proses awal dalam membangun keamanan teknologi informasi berbasis ITIL Versi 3. Penelitian ini didasarkan pada survei pelanggan, survei pelanggan digunakan untuk mengukur tingkat kepuasan pelanggan terhadap layanan teknologi informasi. Berdasarkan survei pelanggan, kemudian dilakukanlah proses audit layanan teknologi informasi berbasis ITIL Versi 3. Audit ini dilakukan untuk mengevaluasi terhadap kebijakan-kebijakan manajemen yang berkaitan dengan layanan teknologi informasi.

A. Uji validitas

Dari hasil pengukuran validitas dapat dikatakan bahwa item yang digunakan valid atau tidak. Tabel 2 menunjukkan hasil dari pengukuran validitas untuk kuesioner pelanggan dengan jumlah responden sebanyak 130 dan taraf signifikansi 5%.

Tabel 2. Validitas kuesioner pelanggan

Variabel	Item	r hitung	r tabel	Keterangan
Layanan Internet	LI1	0,505	0,171	Valid
	LI2	0,478	0,171	Valid
	LI3	0,642	0,171	Valid
	LI4	0,586	0,171	Valid
	LI5	0,592	0,171	Valid
	LI6	0,520	0,171	Valid
Layanan Hosting	LH1	0,570	0,171	Valid
	LH2	0,612	0,171	Valid
	LH3	0,603	0,171	Valid
REPOSITORY	REPO1	0,633	0,171	Valid
	REPO2	0,654	0,171	Valid
	REPO3	0,631	0,171	Valid
Digital Library	DIGI1	0,617	0,171	Valid
	DIGI2	0,614	0,171	Valid
	DIGI3	0,501	0,171	Valid
Sistem Informasi	SI1	0,563	0,171	Valid
	SI2	0,758	0,171	Valid
	SI3	0,624	0,171	Valid
	SI4	0,639	0,171	Valid

B. Uji reliabilitas

Pengujian reliabilitas diperlukan untuk mengetahui reliabilitas masing-masing variabel. Tabel 3 menunjukkan hasil pengujian. Tabel 4 menunjukkan hasil tanggapan responden.

Tabel 3. Hasil pengujian reliabilitas pelanggan

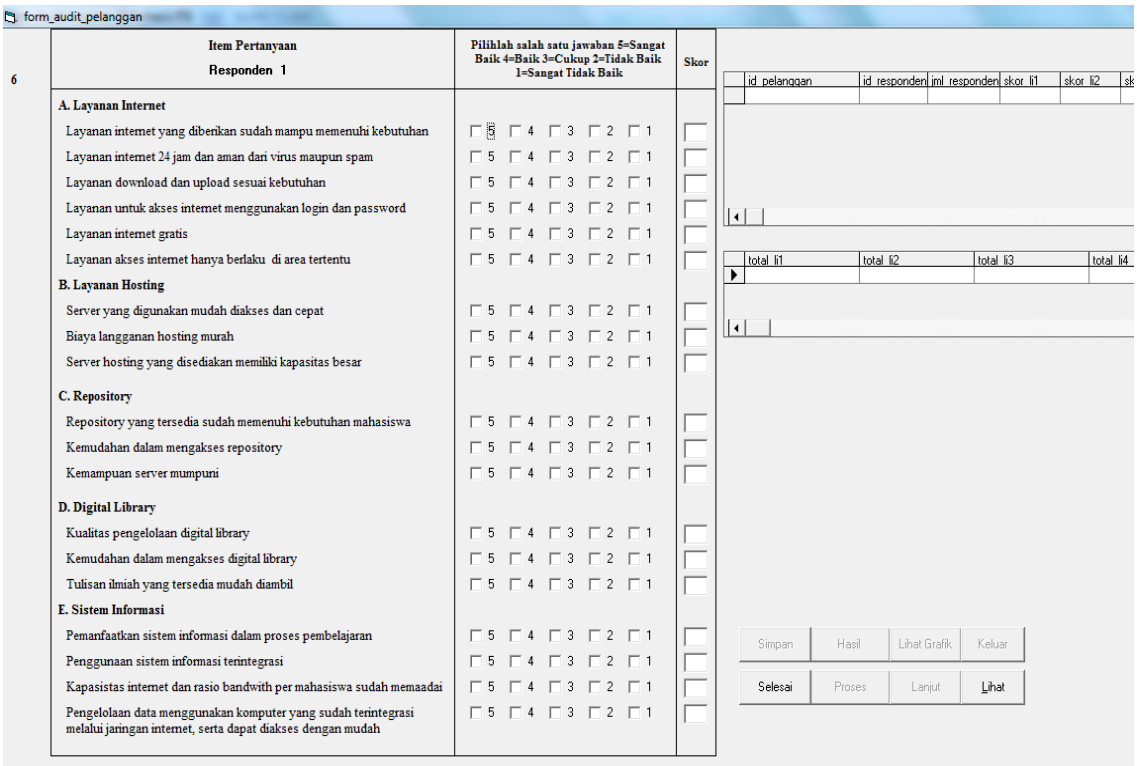
Variabel	Cronbach's alpha	r tabel	Keterangan
Layanan internet	0,712	0,171	Reliabel
Layanan hosting	0,726	0,171	Reliabel
Repository	0,767	0,171	Reliabel
Digital library	0,790	0,171	Reliabel
Sistem informasi	0,784	0,171	Reliabel

Tabel 4. Hasil tanggapan responden

ITEM	Tanggapan Responden										Jml	SKOR	HASIL
	5	%	4	%	3	%	2	%	1	%			
LI1	0	0.00	50	38.46	63	48.46	14	10.77	3	2.31	130	420	BAIK
LI2	3	2.31	24	18.46	64	49.23	35	26.92	4	3.08	130	377	CUKUP
LI3	2	1.54	29	22.31	64	49.23	32	24.62	3	2.31	130	385	CUKUP
LI4	12	9.23	31	23.85	47	36.15	24	18.46	16	12.31	130	389	CUKUP
LI5	40	30.77	46	35.38	35	26.92	7	5.38	2	1.54	130	505	BAIK
LI6	1	0.77	40	30.77	66	50.77	17	13.08	6	4.62	130	403	CUKUP
LH1	4	3.08	43	33.08	61	46.92	19	14.62	3	2.31	130	416	BAIK
LH2	7	5.38	37	28.46	70	53.85	15	11.54	1	0.77	130	424	BAIK
LH3	6	4.62	37	28.46	67	51.54	20	15.38	0	0.00	130	419	BAIK
REPO1	6	4.62	41	31.54	61	46.92	20	15.38	2	1.54	130	419	BAIK
REPO2	5	3.85	44	33.85	63	48.46	17	13.08	1	0.77	130	425	BAIK
REPO3	3	2.31	24	18.46	64	49.23	35	26.92	4	3.08	130	377	CUKUP
DIGI1	6	4.62	45	34.62	60	46.15	17	13.08	2	1.54	130	426	BAIK
DIGI2	10	7.69	52	40.00	57	43.85	11	8.46	0	0.00	130	451	BAIK
DIGI3	9	6.92	47	36.15	59	45.38	15	11.54	0	0.00	130	440	BAIK
SI1	10	7.69	68	52.31	42	32.31	10	7.69	0	0.00	130	468	BAIK
SI2	18	13.85	46	35.38	53	40.77	13	10.00	0	0.00	130	459	BAIK
SI3	2	1.54	23	17.69	59	45.38	35	26.92	11	8.46	130	360	CUKUP
SI4	4	3.08	52	40.00	63	48.46	10	7.69	1	0.77	130	438	BAIK

A. Desain input pelanggan

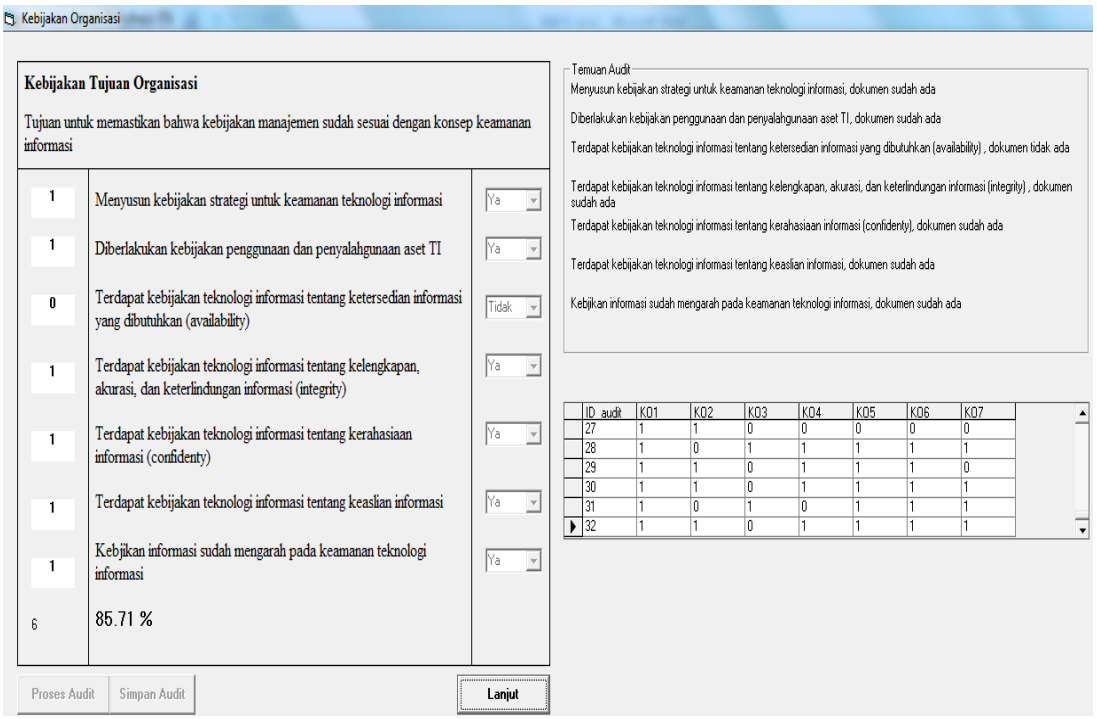
Tahap pertama dari audit layanan teknologi informasi adalah mendesain tampilan input dari pelanggan. Gambar 3 menunjukkan desain input pelanggan.



Gambar 3 desain input pelanggan

B. Desain output pelanggan

Input sudah didesain dengan rapi, langkah berikutnya adalah mendesin output dari pelanggan. Gambar 4 menunjukkan desain outpun dari pelanggan.



Gambar 4 Desain output pelanggan

KESIMPULAN DAN SARAN

Pada penelitian audit layanan teknologi informasi berbasis ITIL dapat diambil kesimpulan bahwa audit terhadap pelanggan akan menghasilkan kategori berupa sangat baik (skor > 502) , baik (skor 417 – 502), cukup (skor 313 – 416), tidak baik (skor 209 – 312), dan sangat tidak baik (skor 104 – 208) untuk jumlah responden sebanyak 130.

Audit layanan teknologi informasi berbasis ITIL terdapat 8 bagian yang diambil dari proses *service design* yang akan menghasilkan persentase terhadap masing-masing bagian.

Audit layanan teknologi informasi dapat menghasilkan evaluasi terhadap layanan keamanan teknologi informasi yang didasarkan pada kerangka kerja ITIL.

DAFTAR PUSTAKA

[1] Aalst, Wil, van Der, Hee, Kees, van, Werf, Martijn, Jan van der, Kumar, Akhil, Verdonk, Marc, 2011, Conceptual Model for Online Auditing, *Decision Support Systems 50*, 636–647.

[2] Bernroider, Edward W.N., dan Ivanov, Milen, 2010, IT Project management control and the Control Objectives for IT and Technology (CobiT) framework, *International Journal of Project Management 29*, 325–336.

[3] Champlain, Jack J., 2003, *Auditing Information Systems Second Edition*, John Wiley & Sons, Inc., Hoboken, Canada.

[4] Chang, Hangbae, 2012, Is ISMS for financial organizations effective on their business?, *Mathematical and Computer Modelling*, 212.

[5] Huang, Shi-Ming, Shen, Wei-Cheng, Yen, David, C., Chou, Ling-Yi, 2011, IT Governance : Objectives and assurances in internet banking, *Journal Advance in International Acounting 27*, 406–414.

[6] Idena, J, dan Eikebrokk, T.T., 2013, Implementing IT Service Management: A systematic literature review, *International Journal of Information Management 33*, 512–523.

[7] Julisch, Klaus, Suter, Christophe, Woitalla, Thomas, Zimmermann, Olaf, 2011, Compliance By Design Bridging The Chasm Between Auditors And IT Architects, *Computer and Security 30*, 410-426.

[8] Knapp, J. Kenneth, Denney, D. Gary, Barner, E. Mark, 2011, Key Issues in Data Center Security : An Investigation of Government Audit Reports, *Government Information Quarterly 28*, 533–541.

[9] McNaughton, Blake, Ray, Pradeep, dan Lewis, Lundy, 2010, Designing an evaluation framework for IT service management, *Information and Management 47*, 219 –225.

[10] Mesquida, Antoni, Lluís, Mas, Antonia, Amengual, Esperança, Manzano, Calvo, Jose, A., 2012, IT Service Management Process Improvement based on ISO/IEC 15504: A systematic review,*Information and Software Technology 54*, 239–247.

[11] Nan, Feng, Wang, Jiannan, Harry, Li, Minqiang, 2013, A security risk analysis model for information systems : Causal relationships of risk factors and vulnerability propagation analysis, *Information Sciences xxx*, xxx–xxx.

[12] Raggad, G. Bell dan Collar, Emilio, Jr, 2006, The Simple Information

Security Audit Process : SISAP, *International Journal of Computer Science and Network Security*, VOL. 6 No. 6.

[13] Stantchev, Vladimir, Petruch, Konstantin, dan Tamm, Gerrit, 2013, Assessing and governing IT-staff behavior by performance-based simulation, *Computers in Human Behavior 29*, 473–485.

[14] Wang, Wei, Wang, Hao, Yang, Bo, Liu, Liang, Liu, Peini, Zeng, Guosun, A Bayesian Network-Based Knowledge Engineering Framework for IT Service Management, *IEEE Transactions On Services Computing* , *Vol. 6 No. 1*.

[15] Wickboldt, Juliano, Araujo, Bianchin, Armando, Luís, Lunardi, Roben, Castagna, Granville, Lisandro, Zambenedetti, Gaspary, Paschoal, Luciano, Bartolini, Claudio, 2011, A framework for risk assessment based on analysis of historical information of workflow execution in IT systems, *Computer Networks 55*, 2954–2975.

[16] IBISA, 2011, *Keamanan Sistem Informasi*, ANDI Offset, Yogyakarta.

[17] Jogiyanto, 2008, Metodologi Penelitian Sistem Informasi, ANDI Offset, Yogyakarta.

[18] Jogiyanto, 2011, *Pedoman Survey Kuesioner*, BPFE, Yogyakarta.

[19] Jogiyanto dan Abdillah, Willy, 2011, *Sistem Tata Kelola Teknologi Informasi*, ANDI Offset, Yogyakarta.

[20] Sarno, Riyanarto dan Tiffano, Irsyat, 2009, *Sistem Manajemen Keamanan Informasi berbasis ISO 27001*, ITS Press, Surabaya.

[21] Singleton, Tommie dan Hall, James, 2009, *Audit Teknologi Informasi dan Assurance*, Salemba Empat, Jakarta.

[22] Sutabri, Tata, 2012, *Konsep Sistem Informasi*, ANDI OFFSET, Yogyakarta.

[23] OGC, 2007, *The Official Introduction to the ITIL Service Lifecycle*, TSO, London.

[24] OGC, 2007, *Service Design*, TSO, London.

[25] Weber, Ron, 2000, *Informatioin System Control and Audit*, The University of Queensland, Prentice Hall Inc.