PROTOTIP *SELF ASSESSMENT AUDIT* ISO 17799

Pujianto Yugopuspito, Susanti, Sutrisno
Fakultas Ilmu Komputer, Universitas Pelita Harapan
UPH Tower, Lippo Karawaci, TANGERANG 15811 Indonesia
e-mail: {yugopuspito,- ,sutrisno}@uph.edu

ABSTRACT

This paper presents a web-based application for a self assessment audit tool that is guided by ISO17799 guidelines.The ISO17799 is a code of practice for information security management as part of the information security standard, and provides a set of controls and procedure to achieve security information. This self assessment audit system shall indicate any security threats based on a pre-defined checklist, which is derived from the implemented audit program of information technology as guided by the ISO17799. Current state of this development is limited to Access Control, and System Development & Maintenance categories.

Keywords: *Web-based application, ISO 17799, IT Audit Program.*

1. PENDAHULUAN

Self assessment audit adalah audit yang dilakukan oleh kalangan internal perusahaan sendiri. Audit ini dilakukan berdasarkan pedoman-pedoman yang didapatkan dari proses-proses atau ketentuan tertentu yang sudah berhasil diterapkan di perusahaan pada umumnya. Pedoman tersebut kemudian disatukan dalam bentuk daftar butir-butir data (*checklist*) dan digunakan sebagai acuan dalam melakukan audit. Audit ini merupakan cara yang dapat digunakan perusahaan untuk mengetahui status sistem kontrol perusahaan mereka dan dapat juga dijadikan persiapan untuk melakukan audit yang lebih formal selanjutnya. Jenis alat bantu IT audit yang dibangun ini dikategorikan sebagai *self assessment audit tools.*

ISO17799 adalah suatu standar internasional yang memfokuskan diri pada manajemen keamanan teknologi informasi [8]. ISO17799 ini berisi serangkaian rekomendasi atau proses-proses praktikal dalam manajemen keamanan teknologi informasi. ISO17799 tidak mengharuskan untuk menerapkan seluruh rekomendasi yang diberikan, tetapi lebih menganjurkan untuk menerapkan rekomendasi yang sesuai dengan kondisi dan kebutuhan perusahaan untuk meningkatkan kinerja dan keamanan teknologi informasi perusahaan mereka.

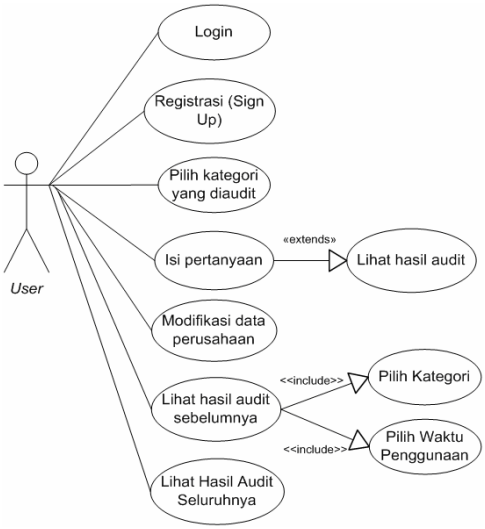
Prototip yang dikembangkan adalah suatu aplikasi berbasis web dengan bahasa script PHP dan database MySQL [3],[6]. Kategori yang digunakan dalam prototip sistem self-assessment audit ini adalah kategori *Access Control* dan *System Development and Maintenance*. Daftar pertanyaan dan rekomendasi serta audit program diturunkan dari [1], [2],[4], [7].

2. PERANCANGAN SISTEM *SELF-ASSESS-MENT AUDIT*

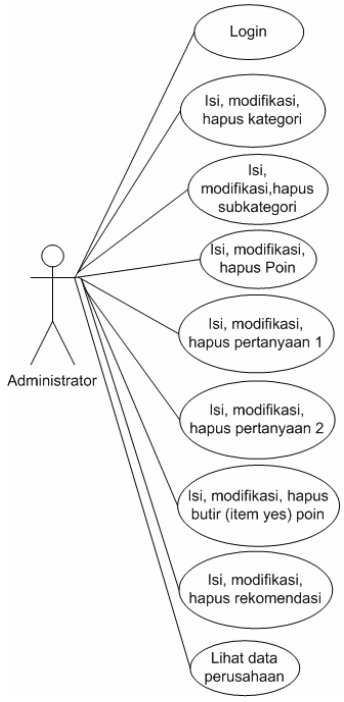
Sistem audit ini terdiri dari 2 (dua) pengguna yaitu administrator dan pengguna (*user*). Administrator dapat melakukan modifikasi ataupun penambahan kategori, subkategori, poin, pertanyaan tipe 1, pertanyaan tipe 2 dan rekomendasi apabila terjadi perubahan atau penambahan dari standar ISO17799 itu sendiri. Sedangkan *user* adalah perusahaan atau organisasi yang menggunakan sistem audit ini untuk melakukan *self asessment audit* terhadap perusahaan mereka.

Desain dari system ditampilkan dengan mengunakan *Use case* dan *activity diagram* mengacu pada UML 2.0 [5]. Gambar 1 dan 2 menunjukan usecase diagram dari pengguna dan administrator. Untuk setiap use case digunakan activity diagram untuk mengambarkan kegiatan dari actor tersebut. Contoh dari activity diagram dapat seperti Gambar 3.

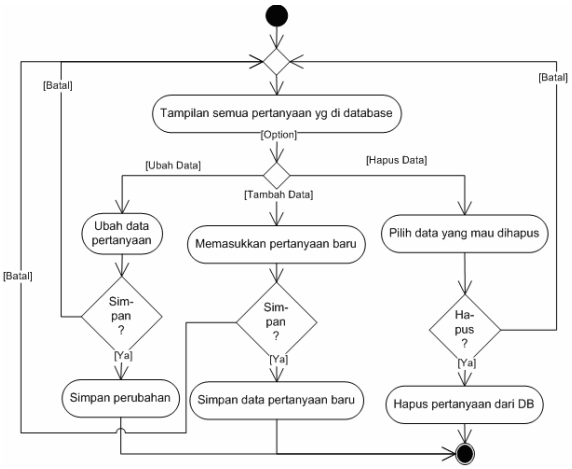
Sistem akan menampilkan pertanyaan dari kategori yang dipilih *user*. Tiap kategori terdiri dari beberapa subkategori yang memiliki beberapa poin di dalamnya. Tiap poin berisi pertanyaan tipe 1, pertanyaan tipe 2, dan butir poin. Pertanyaan tipe 1 merupakan pertanyaan umum mengenai poin yang diajukan pertama kali saat pertanyaan ditampilkan. Pertanyaan tipe 2 merupakan pertanyaan spesifik mengenai poin dan ditampilkan setelah *user* menjawab pertanyaan tipe 1 sebelumnya dan jawabannya adalah ”tidak”. Sedangkan butir poin merupakan pertanyaan yang juga ditampilkan setelah pertanyaan tipe 1 dijawab dan jawabannya adalah ”ya”. Pengguna memberikan jawaban mereka pada *field* yang telah tersedia. Berdasarkan jawaban-jawaban tersebut, sistem akan mendeteksi kelemahan yang ditemukan pada kategori yang telah dipilih dan memberikan rekomendasi perbaikan terhadap kelemahan tersebut. Selain itu, sistem akan menampilkan persentase kesesuaian dari kategori yang diaudit beserta seluruh persentase poin-poin di dalamnya. Gambar 4 mengilustrasikan *activity diagram* dari penggunaan sistem.



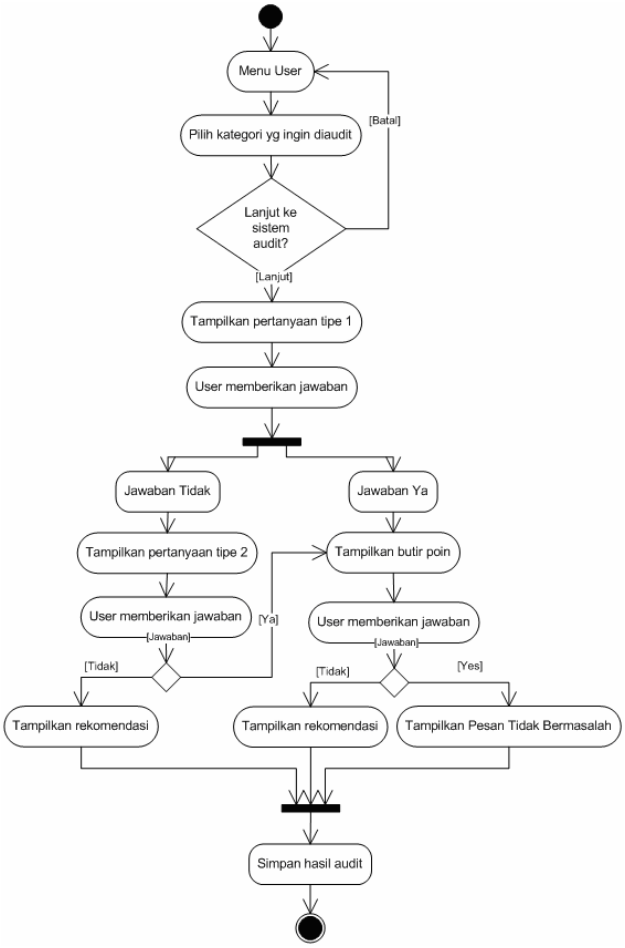
Gambar 1. Use Case Diagram untuk Pengguna



Gambar 2. Use Case Diagram dari Administrator



Gambar 3. *Activity Diagram* untuk Isi dan Modifikasi Pertanyaan



Gambar 4. *Activity Diagram* Untuk Penggunaan Sistem Audit

3. PEMBANGUNAN SISTEM *SELF ASSESS-MENT AUDIT*

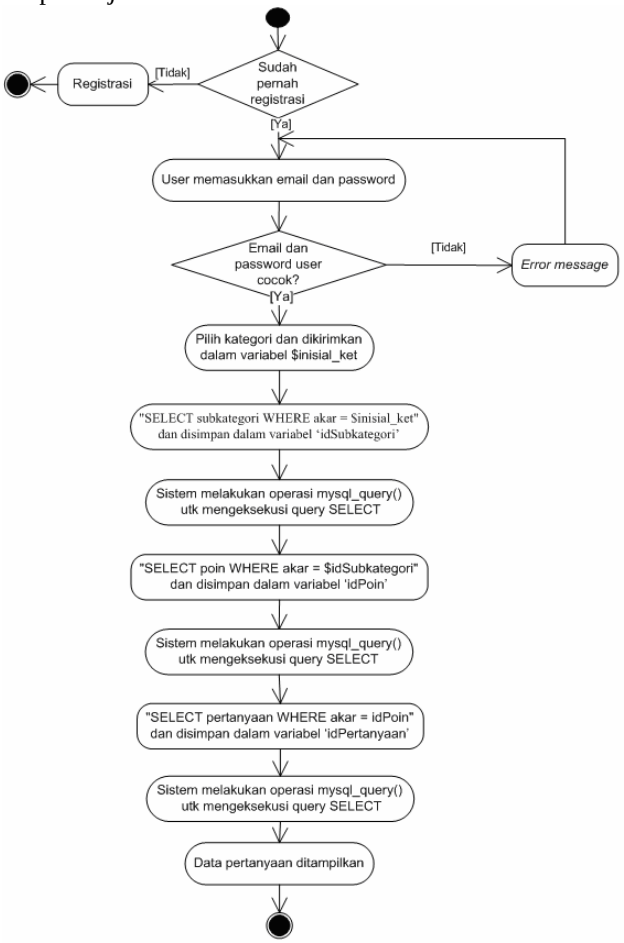
Pembangunan sistem audit ini terdiri dari empat tahap penting yaitu tahap pembangunan menu pertanyaan, tahap penyimpanan jawaban proses audit, tahap pembangunan sistem penyaringan hasil jawaban audit, dan tahap pembangunan sistem pemberian rekomendasi keamanan.

3.1 Tahap Pembangunan Menu Pertanyaan

Menu pertanyaan merupakan menu yang menampilkan pertanyaan audit berdasarkan kategori yang dipilih *user*, pertanyaan berdasarkan panduan ISO17799. Pertanyaan yang ditampilkan adalah jenis pertanyaan tipe 1 yaitu pertanyaan umum mengenai poin yang bersangkutan. Sebelum masuk ke menu ini, *user* diharuskan memilih data kategori yang ditampilkan dalam bentuk menu *list* sesuai dengan data kategori yang ada di database. menggunakan *query*, lihat Gambar 5.

Sistem akan mengambil data pertanyaan berdasarkan kategori yang dikirimkan secara bertahap mulai dari subkategori, poin, lalu pertanyaan. Data-data subkategori, poin, pertanyaan tipe 1, pertanyaan tipe 2, dan rekomendasi disimpan

dalam dua tabel yang berbeda. Untuk itu, dibutuhkan operasi *join* antara dua tabel.



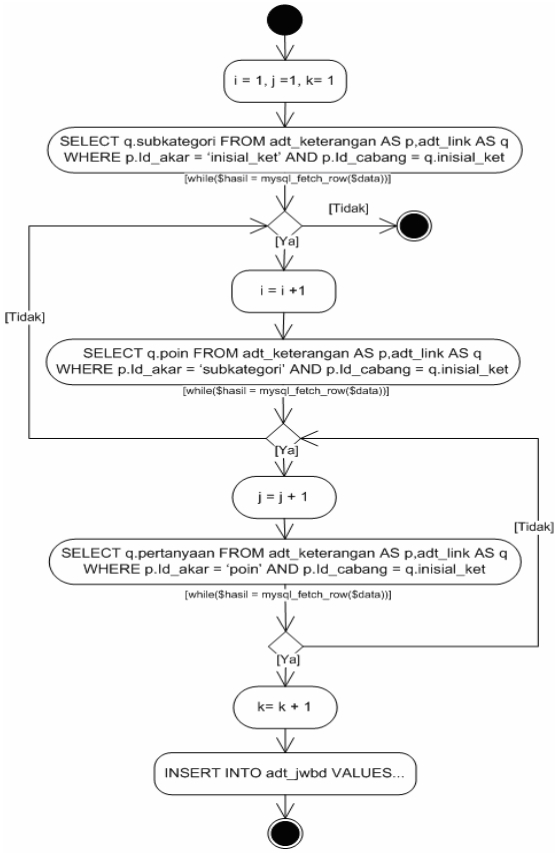
Gambar 5. *Activity Diagram* Pembangunan Menu Pertanyaan

3.2 Tahap Penyimpanan Jawaban Proses Audit

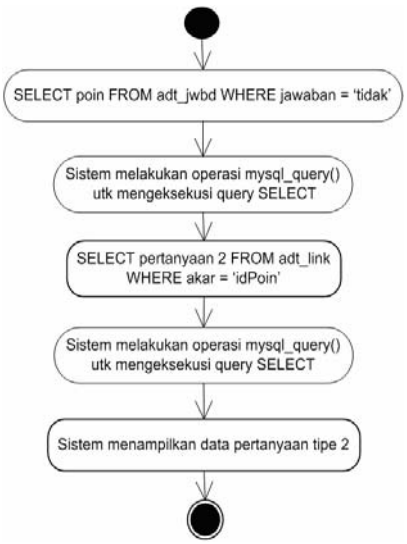
Tahap penyimpanan jawaban merupakan tahap lanjutan setelah tahap pembangunan menu pertanyaan. Pada tahap ini, jawaban dari pertanyaan tipe 1 yang sudah diisi disimpan ke dalam database. Tiap pertanyaan memiliki dua pilihan jawaban yaitu ”ya” dan ”tidak”. Jawaban-jawaban dari *user* akan disimpan ke tabel jawaban. Proses penyimpanan ini dimulai dengan pengambilan data subkategori berdasarkan kategori yang dipilih sebelumnya dan dilanjutkan dengan pengambilan poin berdasarkan subkategori yang didapatkan. Jawaban tersebut akan disimpan dalam database dan digunakan untuk menentukan hasil audit pada tahap selanjutnya. Gambar 6 menunjukan activity diagram dari tahap penyimpanan jawaban proses audit.

3.3 Tahap Pembangunan Sistem Penyaringan Hasil Jawaban Audit

Tahap penyaringan hasil audit merupakan tahap pengelompokkan jawaban hasil audit menjadi dua bagian yaitu jawaban “ya” dan tidak”. Untuk tiap jawaban “ya”, *user* akan diarahkan ke pertanyaan untuk memeriksa kesesuaian lebih lanjut yaitu dengan menampilkan butir-butir poin yang harus diterapkan dari poin yang bersangkutan. Sedangkan untuk jawaban “tidak”, *user* akan diarahkan ke pertanyaan tipe 2 yaitu pertanyaan yang lebih spesifik dari poin yang bermasalah tersebut. Dari jawaban-jawaban terhadap pertanyaan di atas, sistem akan menampilkan rekomendasi yang sesuai. Activity Diagram untuk kasus jawaban ’tidak’ ditunjukan pada Gambar 7.



Gambar 6. *Activity Diagram* Penyimpanan Jawaban Proses Audit

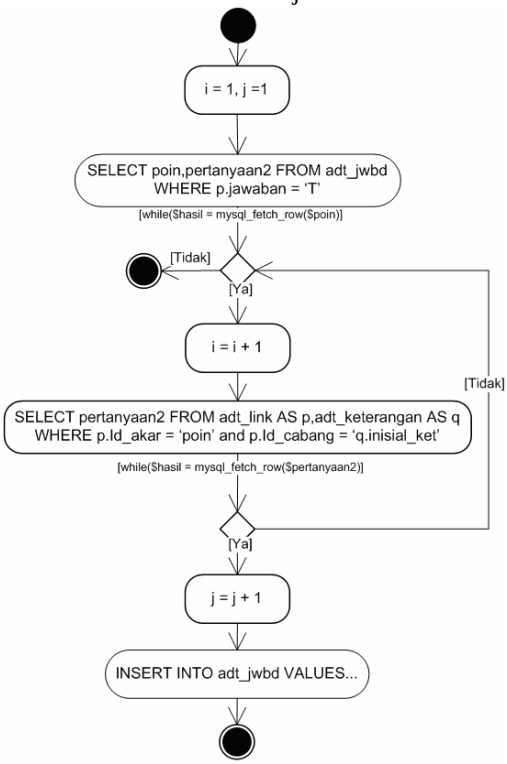


Gambar 7. *Activity Diagram* Penyaringan Jawaban “Tidak”

 ISSN: 1907-5022

3.4 Tahap Pembangunan Sistem Pemberian Rekomendasi

Tahap ini merupakan tahap terakhir dari serangkaian proses audit. Pada tahap ini, jawaban-jawaban dari pertanyaan tipe 2 dan butir poin dari *user* disaring sehingga didapatkan rekomendasi yang sesuai. Lihat Gambar 8 untuk jawaban 'Tidak'.



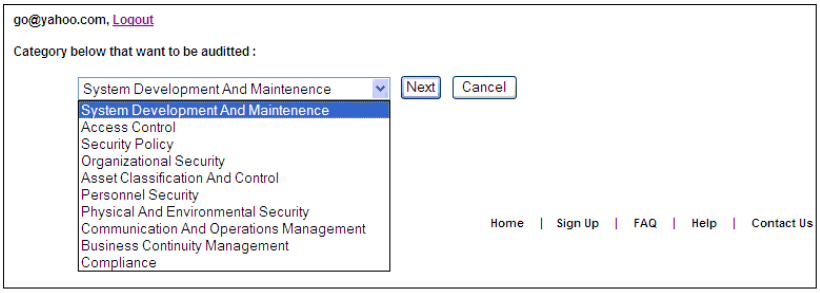
Gambar 8. *Activity Diagram* Penyimpanan Data Jawaban "Tidak' Pertanyaan Tipe 2 dan Poin

Jawaban dari pertanyaan tipe 2 yang bernilai 'tidak' artinya memiliki masalah, dan sistem akan menampilkan rekomendasi yang bersesuaian. Demikian pula untuk semua jawab bernilai 'ya' akan menampilkan klarifikasi poin dari jawaban tersebut.

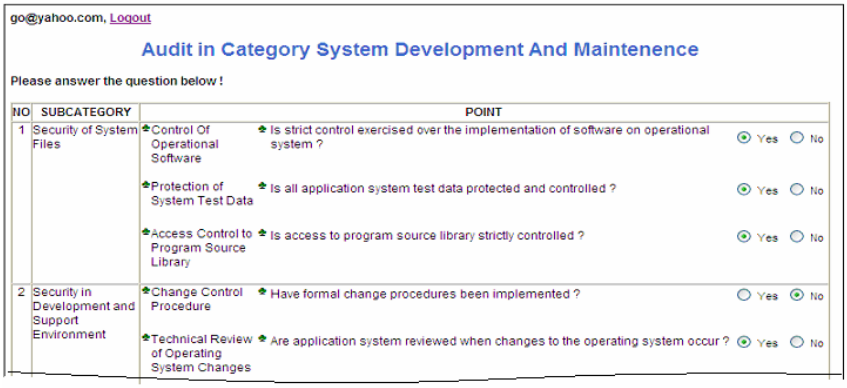
4. PROSES AUDIT DALAM SISTEM

Berikut akan ditampilkan bagaimana sistem *self assessment audit* ini dijalankan dalam proses audit:

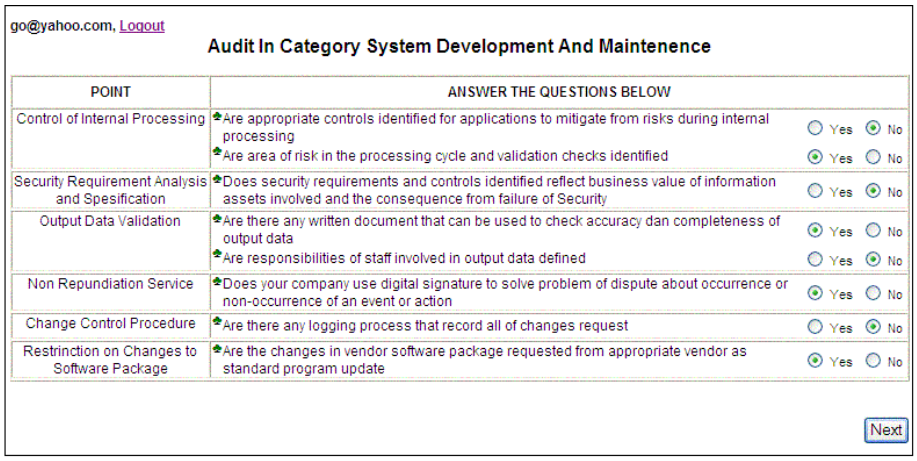
1. *User* memilih kategori yang ingin diaudit, Gambar 9.
2. Sistem menampilkan daftar pertanyaan umum (pertanyaan tipe 1) dari kategori yang telah dipilih. Terdapat 2 (dua) pilihan jawaban yang harus dijawab *user*, Gambar 10
3. Sistem menampilkan pertanyaan spesifik (pertanyaan tipe 2) berdasarkan hasil penyaringan jawaban pada pertanyaan tipe 1 yang diajukan sebelumnya. Terdapat 2 (dua) pilihan jawaban juga yang harus dijawab *user*, Gambar 11.
4. Sistem menampilkan pertanyaan berisi butir poin berdasarkan hasil penyaringan jawaban pada pertanyaan tipe 1 yang diajukan sebelumnya. Terdapat 2 (dua) pilihan jawaban juga yang harus dijawab *user*, Gambar 12.
5. Sistem menampilkan hasil audit dan rekomendasi dari hasil proses audit yang dilakukan, Gambar 13.
6. Sistem menampilkan persentase dari hasil penerapan berdasarkan proses audit yang dilakukan, Gambar 14.



Gambar 9. Pilihan Kategori



Gambar 10. Tampilan Pertanyaan Umum



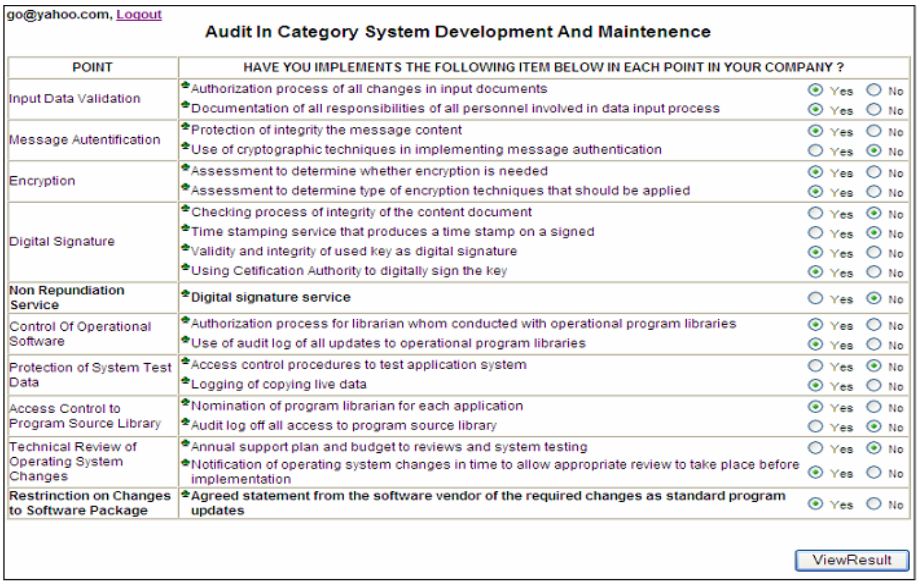
go@yahoo.com, Logout

Audit In Category System Development And Maintenence

POINT	ANSWER THE QUESTIONS BELOW	
Control of Internal Processing	Are appropriate controls identified for applications to mitigate from risks during internal processing	Yes / No
	Are area of risk in the processing cycle and validation checks identified	Yes / No
Security Requirement Analysis and Spesification	Does security requirements and controls identified reflect business value of information assets involved and the consequence from failure of Security	Yes / No
Output Data Validation	Are there any written document that can be used to check accuracy dan completeness of output data	Yes / No
	Are responsibilities of staff involved in output data defined	Yes / No
Non Repundiation Service	Does your company use digital signature to solve problem of dispute about occurrence or non-occurrence of an event or action	Yes / No
Change Control Procedure	Are there any logging process that record all of changes request	Yes / No
Restrinction on Changes to Software Package	Are the changes in vendor software package requested from appropriate vendor as standard program update	Yes / No

Next

Gambar 11. Tampilan Pertanyaan Spesifik



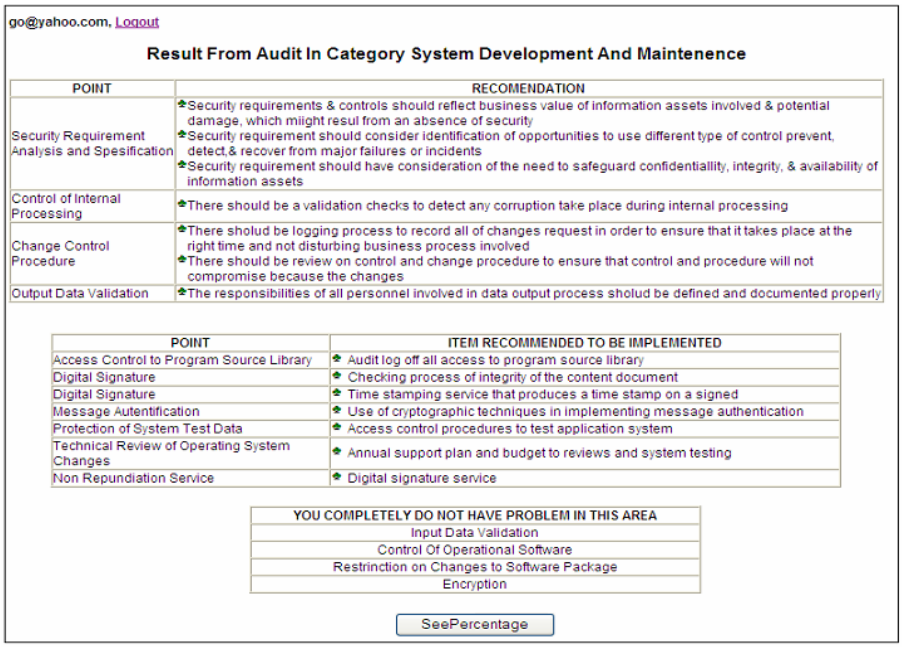
go@yahoo.com, Logout

Audit In Category System Development And Maintenence

POINT	HAVE YOU IMPLEMENTS THE FOLLOWING ITEM BELOW IN EACH POINT IN YOUR COMPANY ?	
Input Data Validation	Authorization process of all changes in input documents	Yes / No
	Documentation of all responsibilities of all personnel involved in data input process	Yes / No
Message Autentification	Protection of integrity the message content	Yes / No
	Use of cryptographic techniques in implementing message authentication	Yes / No
Encryption	Assessment to determine whether encryption is needed	Yes / No
	Assessment to determine type of encryption techniques that should be applied	Yes / No
Digital Signature	Checking process of integrity of the content document	Yes / No
	Time stamping service that produces a time stamp on a signed	Yes / No
	Validity and integrity of used key as digital signature	Yes / No
	Using Cetification Authority to digitally sign the key	Yes / No
Non Repundiation Service	**Digital signature service**	Yes / No
Control Of Operational Software	Authorization process for librarian whom conducted with operational program libraries	Yes / No
	Use of audit log of all updates to operational program libraries	Yes / No
Protection of System Test Data	Access control procedures to test application system	Yes / No
	Logging of copying live data	Yes / No
Access Control to Program Source Library	Nomination of program librarian for each application	Yes / No
	Audit log off all access to program source library	Yes / No
Technical Review of Operating System Changes	Annual support plan and budget to reviews and system testing	Yes / No
	Notification of operating system changes in time to allow appropriate review to take place before implementation	Yes / No
Restrinction on Changes to Software Package	**Agreed statement from the software vendor of the required changes as standard program updates**	Yes / No

ViewResult

Gambar 12. Tampilan Pertanyaan Butir Poin



go@yahoo.com, Logout

Result From Audit In Category System Development And Maintenence

POINT	RECOMENDATION
Security Requirement Analysis and Spesification	Security requirements & controls should reflect business value of information assets involved & potential damage, which miight resul from an absence of security Security requirement should consider identification of opportunities to use different type of control prevent, detect,& recover from major failures or incidents Security requirement should have consideration of the need to safeguard confidentiallity, integrity, & availability of information assets
Control of Internal Processing	There should be a validation checks to detect any corruption take place during internal processing
Change Control Procedure	There sholud be logging process to record all of changes request in order to ensure that it takes place at the right time and not disturbing business process involved There should be review on control and change procedure to ensure that control and procedure will not compromise because the changes
Output Data Validation	The responsibilities of all personnel involved in data output process sholud be defined and documented properly

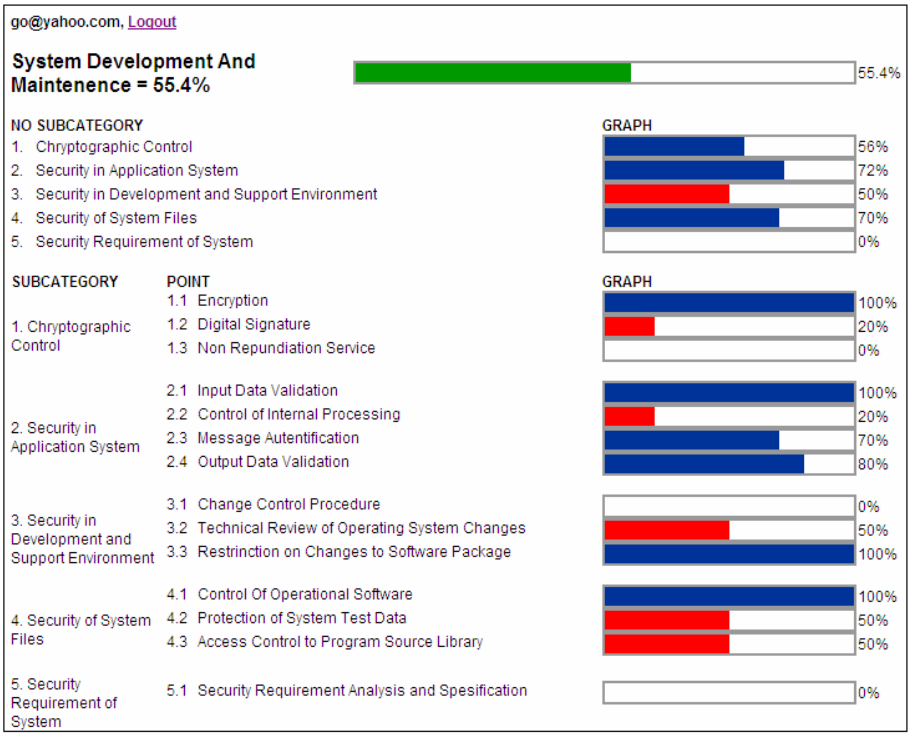
POINT	ITEM RECOMMENDED TO BE IMPLEMENTED
Access Control to Program Source Library	Audit log off all access to program source library
Digital Signature	Checking process of integrity of the content document
Digital Signature	Time stamping service that produces a time stamp on a signed
Message Autentification	Use of cryptographic techniques in implementing message authentication
Protection of System Test Data	Access control procedures to test application system
Technical Review of Operating System Changes	Annual support plan and budget to reviews and system testing
Non Repundiation Service	Digital signature service

YOU COMPLETELY DO NOT HAVE PROBLEM IN THIS AREA
Input Data Validation
Control Of Operational Software
Restrinction on Changes to Software Package
Encryption

SeePercentage

Gambar 13. Hasil Audit dan Rekomendasi

 ISSN: 1907-5022



Gambar 14. Hasil Persentase Proses Audit

Prototip sistem *self assessment audit* ini hanya mampu mengidentifikasi semua masalah yang telah dimasukan dalam daftar pertanyaan-pertanyaan melalui tahap pembangunan menu pertanyaan. Sistem ini dibuat terbuka sehingga pertanyaan dapat diedit sesuai dengan kebutuhan dan tuntutan kepatuhan.

5. SIMPULAN

Pembuatan prototip sistem *self assessment audit* ini telah memenuhi tujuan penulisan ini yaitu untuk memeriksa kelemahan keamanan dalam pengimplementasian teknologi informasi dan memberikan rekomendasi yang sesuai dengan standar ISO17799 yang ada. Secara umum proses audit pada sistem *self assessment audit* ini terbagi atas empat tahap, yaitu tahap pemberian pertanyaan sesuai dengan kategori yang dipilih, tahap penyaringan jawaban, tahap pemberian pertanyaan yang lebih spesifik, dan tahap penentuan hasil audit dan rekomendasi yang sesuai. Pengembangan sistem audit ini diharapkan dapat digunakan oleh perusahaan-perusahaan untuk melakukan audit teknologi informasi secara internal tanpa mengeluarkan biaya yang besar tetapi sudah memenuhi pedoman atau standar keamanan internasional yaitu ISO17799.

Sistem ini memiliki potensi yang besar untuk dikembangkan lebih lanjut yaitu dengan penambahan fasilitas audit pada kedelapan kategori dalam ISO17799 yang belum dikembangkan dalam sistem ini yaitu pada kategori *Security Policy*, *Organizational Security*, *Asset Classification & Control*, *Personel Security*, *Physical & Environmental Security*, *Communication & Operations Management*, *Business Continuity Management*, dan *Compliance*.

PUSTAKA

[1] Hubton, Bryant, *Core Concept of Information Technology Auditing*, John Wiley and Sons Inc. 2004.
[2] Krammer, John, *Preparation Guide For Audit Exam*, Willey Publishing, Canada, 2003.
[3] Madcoms, Andi, *Aplikasi Program PHP dan MySQL Untuk Membuat Website Interaktif*, Andi Offset, Yogyakarta, 2004.
[4] Pfleeger, Charles, Security in Computing, Prentice Hall, USA, 2003.
[5] Pender, Tom, *UML Bible*, John Willey & Sons, 2003.
[6] Sidik, Betha, *Pemograman Web Dengan PHP*, Penerbit Informatika, Bandung, Agustus 2004.
[7] Marianne, Swanson, *Security Self Assessment Guide for Information Technology System*, NIST, USA, 2004.
[8] Whitman, Mattord, *Management of Information Security*, Thompson Learning Inc, Canada, 2004.