UNIVERSITAS INDONESIA

DECISION SUPPORT SYSTEM PADA AUDIT KEAMANAN SISTEM INFORMASI RUMAH SAKIT "X" TAHUN 2009

TESIS

Nama : SUMARYANTO

NPM : 0706193265

PROGRAM PASCA SARJANA

PROGRAM STUDI TEKNOLOGI BIOMEDIS

SALEMBA

JULI 2010

UNIVERSITAS INDONESIA

DECISION SUPPORT SYSTEM PADA AUDIT KEAMANAN SISTEM INFORMASI RUMAH SAKIT "X" TAHUN 2009

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains

Nama : SUMARYANTO

NPM : 0706193265

PROGRAM PASCA SARJANA

PROGRAM STUDI TEKNOLOGI BIOMEDIS

KEKHUSUSAN INFORMATIKA BIOMEDIS

SALEMBA

JULI 2010

SURAT PERNYATAAN BEBAS PLAGIARISME

Saya yang bertanda tangan di bawah ini dengan sebenarnya menyatakan bahwa tesis ini saya susun tanpa tindakan plagiarisme sesuai dengan peraturan yang berlaku di Universitas Indonesia.

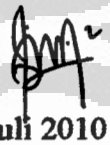
Jika di kemudian hari ternyata saya melakukan tindakan Plagiarisme, saya akan bertanggung jawab sepenuhnya dan menerima sanksi yang dijatuhkan oleh Universitas Indonesia kepada saya.

Jakarta, Juli 2010

SUMARYANTO

HALAMAN PERNYATAAN ORISINALITAS

Tesis ini adalah hasil karya saya sendiri, dan semua sumber baik yang dikutip maupun dirujuk telah saya nyatakan dengan benar.

Nama	: SUMARYANTO
NPM	: 0706193265
Tanda Tangan	: 
Tanggal	: Juli 2010

HALAMAN PENGESAHAN

Tesis ini diajukan oleh :

Nama : SUMARYANTO

NPM : 0706193265

Program Studi : Teknologi Biomedis

Judul Tesis : ***DECISION SUPPORT SYSTEM*** **PADA AUDIT KEAMANAN SISTEM INFORMASI RUMAH SAKIT "X" TAHUN 2009**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Sains pada Program Studi Teknologi Biomedis Program Pascasarjana Universitas Indonesia.

DEWAN PENGUJI

Pembimbing : Dr. dr. H. Boy S. Sabarguna MARS (.....)

Penguji 1 : Drs. Anwar S. Ibrahim, M.Eng. (.....)

Penguji 2 : dr. Aria Kekalih, MTI (.....)

Ditetapkan di : Jakarta

Tanggal : Juli 2010

Oleh

Ketua Program Studi Teknologi Biomedis
Program Pascasarjana Universitas Indonesia

Prof. Dr. dr. Cholid Badri, Sp.Rad

KATA PENGANTAR

Puji syukur saya panjatkan kepada Tuhan Yang Maha Esa, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan tesis ini. Penulisan tesis ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Sains, Program Pasca Sarjana, Program Studi Teknologi Biomedis, Universitas Indonesia. Saya menyadari bahwa tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan tesis ini, sangatlah sulit bagi saya untuk menyelesaikan tesis ini, oleh karena itu saya mengucapkan terima kasih nama-nama berikut.

1. Prof. Dr. dr. Cholid Badri, selaku Ketua Program Studi yang telah memberikan arahan dan bimbingan selama saya menjadi mahasiswa di Program Studi Teknologi Biomedis
2. Dr. dr. H. Boy Sabarguna MARS, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan tesis ini.
3. Pihak Rumah Sakit "X" yang telah banyak membantu dalam usaha memperoleh data yang saya perlukan.
4. Orang tua saya yang telah memberikan bantuan dukungan material dan moral.
5. Saudara saya (Mas Ano STKIP Purnama, Mbak Tik STIE Ahmad Dahlan, Mbak Tini Universitas Mercu Buana, Mas Hoho UTY Yogyakarta) yang telah memberikan bantuan dukungan material dan moral.
6. Ibu Sita Resmi, S.Pd, selaku Ketua Yayasan Pendidikan Makarya yang telah memberikan kesempatan untuk mengikuti perkuliahan di UI.
7. Bapak Saryanta, S.Pd, selaku Kepala Sekolah SMP Makarya Jakarta dan Bapak H. Abdullah Hasan, SH, selaku Kepala Sekolah SMIP Makarya Jakarta yang telah memberikan dukungan dan izin dalam mengikuti perkuliahan di UI.
8. Para sahabat (Mas Joko TBM UI, Dyah Sari Utami FKM UI, Keysa I.Z CitiBank, Mbak Citra Bank BNI, Mbak Nana Akbid, Mas Eko, Mas Gean, Mas Jay) yang telah memberikan semangat dan bantuan dalam menyelesaikan tesis ini.

Akhir kata, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tesis ini membawa manfaat bagi pengembangan ilmu.

Jakarta, Juli 2010

Penulis

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama : SUMARYANTO

NPM : 0706193265

Program Studi : Teknologi Biomedis

Fakultas : Program Pasca Sarjana

Jenis Karya : Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif (*Non-Exclusive Royalty-Free Right)*** atas karya ilmiah saya yang berjudul:

***DECISION SUPPORT SYSTEM* PADA AUDIT KEAMANAN SISTEM INFORMASI RUMAH SAKIT "X" TAHUN 2009**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalimedia/ formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : Juli 2010

Yang menyatakan

SUMARYANTO

ABSTRAK

Nama : SUMARYANTO
NPM : 0706193265
Program Studi : Teknologi Biomedis
Judul : **Sistem Bantu Keputusan pada Audit Keamanan Sistem Informasi Rumah Sakit "X" Tahun 2009**

Permasalahan: sistem informasi secara nyata membantu upaya peningkatan mutu suatu rumah sakit. Orientasi pada mutu pelayanan harus terus dikembangkan, sejalan tuntutan masyarakat yang terus bertambah karena masyarakat akan dengan mudah membandingkan pelayanan yang didapat. Peran alat bantu berupa DSS (*Decision Support System*) akan sangat berguna dalam menetapkan dan membantu adanya keputusan yang unggul. Rumah Sakit "X" sebagai salah satu rumah sakit terbesar di Jakarta mempunyai sistem informasi yang mengintegrasikan seluruh data. Selama ini sistem telah berjalan dengan memenuhi fungsinya dalam memproses informasi-informasi yang ada, tetapi hal tersebut belum menjamin keamanan informasi yang ada. **Tujuan:** mengetahui seberapa jauh penerapan keamanan sistem informasi (*security system)* di Rumah Sakit "X", menganalisis dan mendesain DSS (*Decision Support System)* untuk audit keamanan sistem informasi Rumah Sakit "X", dan melaksanakan uji coba DSS (*Decision Support System*) di Rumah Sakit "X". **Metode Penelitian:** analisis data pada penelitian ini menggunakan analisis data kuantitatif deskriptif dengan pengujian DSS audit keamanan sistem informasi Rumah Sakit "X". Pengumpulan data menggunakan instrumen berupa pengisian kuisioner dan form data pada DSS yang telah dibuat yang sebelumnya dilakukan pelatihan penggunaan perangkat lunak tersebut. **Hasil:** hasil audit keamanan sistem informasi Rumah Sakit "X" menggunakan DSS menunjukkan bahwa sistem informasi di rumah sakit ini kurang aman dengan jumlah nilai perolehan 75 (59%). **Kesimpulan:** kondisi keamanan sistem informasi Rumah Sakit "X" masuk dalam kategori kurang aman, DSS pada audit sistem informasi Rumah Sakit "X" ini terdiri dari 5 tahap yaitu masukan, proses, informasi, analisis, dan keluaran, *Decision Support System* (DSS) yang telah dibuat ini sangat membantu dan mempermudah audit terhadap keamanan sistem informasi Rumah Sakit "X". **Saran:** mensosialisasikan pentingnya audit terhadap keamanan sistem informasi, penggunaan perangkat lunak DSS audit keamanan sistem informasi, meningkatkan kualitas sumber daya manusia.

Kata kunci:
Decision Support System, Audit, Keamanan, Sistem Informasi, Rumah Sakit "X".

ABSTRACT

Name : SUMARYANTO
NPM : 0706193265
Study Program: Biomedical Engineering
Title : ***DECISION SUPPORT SYSTEM*** **TO INFORMATION SYSTEM SECURE AUDIT IN "X" HOSPITAL 2009**

Problem Statement: the real information system helps to increase the quality of hospital. The oriented of service must be developed continually. According society needed more service, so that they can be easy to compare the service. The role of the tool DSS (***Decision Support System***) will be useful to state and help for getting excellent decision. "X" Hospital is one of the biggest hospital in Jakarta has information system that coverage's all data. The system has worked with its function in processing all information but it doesn't guarantee the security system. **Purpose:** to know how for the application of security system at "X" Hospital, to analyze and design DSS for security system audit, and try out DSS in "X" Hospital. **Research Method:** to analyze data on research using descriptive quantitative for testing DSS security system audit in "X" Hospital, to get data using questioner and form at DSS it has training for using this software. **Result:** the result of security system audit in "X" Hospital uses DSS that show the security system at that hospital is unsafe with score 75 (59%). **Conclusion:** the condition of security system at "X" Hospital shows unsafe category, Audit DSS at "X" Hospital consist of 5 steps input, processing, information, analyzing and report DSS has been made it helps and make easier to have audit for security system at "X" Hospital. **Recommendations**: to give information about the essential audit for security system, using DSS software for security system information, to increase human resource quality.

Keyword :
Decision Support System, Audit, Secure, Information System, "X" Hospital.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

1.1. Latar Belakang Masalah

Pada saat suasana persaingan rumah sakit yang ketat, maka adanya upaya yang tepat dalam pengambilan keputusan sangatlah penting. Kebutuhan adanya sistem informasi vital dalam pengambilan keputusan yang realistik. Sistem informasi secara nyata membantu upaya peningkatan mutu suatu rumah sakit. Orientasi pada mutu pelayanan harus terus dikembangkan, sejalan tuntutan masyarakat yang terus bertambah karena masyarakat akan dengan mudah membandingkan pelayanan yang didapat sehingga peran alat bantu berupa DSS (*Decision Support System*) akan sangat berguna dalam menetapkan dan membantu adanya keputusan yang unggul.

Menyikapi perubahan yang terjadi pada keadaan dan dasar pola pengambilan keputusan, maka pengambilan keputusan harus diarahkan pada pengambilan keputusan berdasar informasi, sehingga diperlukan sistem informasi yang mendukung. Selain itu, diperlukan pula metoda pengambilan keputusan yang sistematis dan akan lebih baik bila dibantu oleh program komputer sebab dengan metoda yang sistematis, akan dihasilkan informasi yang tepat sasaran.

Adanya perubahan pola pengambilan keputusan dan keterkaitan dengan kebutuhan sistem informasi, terutama keuangan rumah sakit dalam kondisi harga alat yang mahal dan kompetisi yang ketat, maka pengambilan keputusan yang menyangkut uang harus hati-hati, dan perlu dicari keputusan yang benar-benar unggul dan tepat sasaran. Bila tidak, kerugian akan membebani secara berkepanjangan.[1]

Perkembangan teknologi informasi telah menempatkan informasi menjadi industri tersendiri. Informasi telah menjadi material yang strategis bagi setiap institusi atau perusahaan. Sehingga setiap institusi/perusahaan

[1] Sabarguna, B.S. (2001). *Sistem Inforamsi Pemasaran Rumah Sakit Berbasis Rekam Medis.* Yogyakarta: Gama Press.

memerlukan unit pengolahan informasi tersendiri dengan menerapkan berbagai teknologi pengolahan informasinya.

Munculnya teknologi-teknologi baru baik dari segi *hardware* maupun *software* tersebut memicu perusahaan mengadaptasi teknologi-teknologi baru, menggantikan sistem yang telah dimiliki. Pada tahun 2000, tercatat investasi sebesar dua triliun Dolar Amerika telah dikeluarkan oleh berbagai perusahaan untuk membangun teknologi informasinya.[2]

Penyebaran yang cepat ini tidak menjamin *awareness* masyarakat pengguna teknologi informasi (TI) tentang keamanan sistem semakin bertambah pula. Munculnya banyak kasus kejahatan komputer adalah akibat dari tidak adanya pengetahuan yang memadai oleh masyarakat pengguna teknologi informasi. Nilai informasi yang begitu penting dan strategis mengakibatkan serangan dan ancaman terhadap sistem dan arus informasi semakin meningkat.

Kasus penggantian *content website* atau penyalahgunaan kartu kredit oleh oknum yang sering disebut *hacker* atau *cracker* tersebut hanyalah sebuah contoh kecil bentuk kejahatan komputer. Sebuah survey yang dilakukan oleh FBI (*Federal Bureau of Investigation*) tahun 1999 justru menyatakan bahwa 86% kejahatan komputer dilakukan oleh karyawan perusahaan itu sendiri yang tidak puas (*disgruntled employees*). Para penyerang luar (*independent hacker*) hanya menempati urutan kedua dengan prosentase 74%.[3]

Informasi adalah sebuah aset, dan seperti aset bisnis yang lain informasi sangat bernilai bagi rumah sakit sehingga harus dilindungi. Karena itu, implementasi sebuah sistem informasi saja belum menjamin keamanan sistem informasi yang ada di dalamnya. Sebuah sistem harus memiliki mekanisme kontrol keamanan.

---

[2] Indrajit, Richardus E. (2004). *Kajian Strategis Cost Benefit Teknologi Informasi.* Yogyakarta: Andi Offset.

[3] Rahardjo, B. (1999). *Keamanan dalam Electronic Commerce, Paper yang dipresentasikan pada Seminar.* Jakarta: Infokomputer.

Kontrol keamanan dari sebuah sistem dapat dibagi menjadi dua, yaitu kontrol terhadap keamanan *fisik* dan *logic*. Keamanan fisik meliputi perlindungan terhadap semua ancaman fisik terhadap informasi seperti akses langsung data oleh pihak yang tidak berwenang seperti pencurian hingga bencana alam. Kontrol terhadap keamanan *logic* mengatur tentang semua usaha perlindungan informasi yang bersifat non-fisik seperti manajemen *password, autorisasi* dan *autentikasi identitas pengguna, kriptografi* hingga pemasangan perlundangan terhadap serangan dari luar seperti *firewall* dan *IDS (Instrucsion Detection System).*[4]

Dua kontrol inilah yang harus diperhatikan untuk memastikan keamanan sebuah sistem. Untuk mengukur (*assess*) sejauh mana tingkat keamanan yang telah dimiliki oleh sebuah sistem informasi diperlukan audit terhadap keamanan informasi yang dikelola sistem.

Rumah Sakit "X" sebagai salah satu rumah sakit terbesar di Jakarta mempunyai sistem informasi yang mengintegrasikan seluruh data yang ada, mulai dari data pasien, pegawai, stok, hingga data keuangan. Selama ini sistem telah berjalan, dengan memenuhi fungsinya dalam memproses informasi-informasi yang ada, tetapi belum tentu menjamin keamanan informasi yang dimiliki Rumah Sakit "X".

1.2. Tujuan Penelitian

1.2.1. Tujuan Umum

Mengetahui seberapa jauh penerapan keamanan sistem informasi (*security system)* di Rumah Sakit "X".

1.2.2 Tujuan Khusus

Penelitian ini bertujuan sebagai berikut.

---

[4] Champlain, Jakck J. (2003). *Auditing Information System.* New Jersey: John Wiley & Sons, Inc.

a. Menganalisis dan mendesain DSS (*Decision Support System)* untuk audit keamanan sistem informasi Rumah Sakit "X".

b. Melaksanakan uji coba DSS (*Decision Support System*) di Rumah Sakit "X".

1.3 Manfaat Penelitian

Penelitian ini diharapkan akan memberikan manafaat sebagai berikut.

a. Menghasilkan DSS (*Decision Support System*) yang dapat digunakan oleh rumah sakit lain untuk mengaudit keamanan sistem informasi.

b. Menghasilkan sebuah dokumen metode pengumpulan data yang dapat langsung digunakan oleh para auditor yang akan menggunakan control pada ISO 17799 untuk melakukan audit keamanan sistem informasi.

c. Memberikan evaluasi kepada Rumah "X" tentang keamanan informasi pada sistem informasi yang dimiliki.

d. Memberikan rekomendasi pada Rumah Sakit "X" tentang perbaikan dari keamanan informasi yang telah dimiliki berdasar ISO 17799.

e. Bagi pemerintah khususnya Departemen Kesehatan, penelitian ini diharapkan dapat menjadi suatu perangkat lunak standar dalam melakukan audit internal keamanan sistem informasi rumah sakit yang ada di seluruh Indonesia.

f. Menghasilkan perangkat lunak yang dapat memperoleh hak cipta sebagai sumbangan bagi hasil karya bangsa Indonesia.

BAB 2
TINJAUAN PUSTAKA

Keamanan sistem informasi menjadi hal yang sangat penting bagi perusahaan yang menggunakan fasilitas teknologi informasi dan menempatkannya sebagai infrastruktur penting. Sebab sistem informasi adalah aset bagi perusahaan tersebut. Keamanan sistem informasi secara langsung maupun tidak langsung dapat mempertahankan kelangsungan bisnis, mengurangi resiko, mengoptimalkan *return of investment* dan bahkan memberikan peluang bisnis semakin besar. Semakin banyak informasi perusahaan yang disimpan, dikelola dan digunakan secara bersama, akan semakin besar pula resiko terjadinya kerusakan, kehilangan atau terekspos nya data/informasi ke pihak lain yang tidak berhak. Ancaman dan resiko yang ditimbulkan akibat kegiatan pengelolaan dan pemeliharaan data/informasi menjadi alasan disusunnya standar sistem manajemen keamanan informasi yang salah satunya adalah ISO (*International Organization for Standardization*) 17799.

Pada penelitian ini dibuat sistem bantu keputusan atau DSS (*Decision Support System*) untuk mendukung pemecahan masalah meliputi data, proses, informasi, analisis dan laporan. Pembuatan DSS berdasarkan ISO 17799 yang meliputi 10 klausa pengendalian (10 *control clauses*), 36 sasaran pengendalian (36 *control objectives*) dan 127 pengendalian keamanan (127 *controls security*). Hasil dari penelitian ini adalah analisis data menggunakan laporan berupa tingkat keamanan sistem informasi Rumah Sakit "X" dan solusi masalah berupa rekomendasi terhadap beberapa hal yang perlu diperhatikan untuk lebih meningkatkan keamanan sistem informasi.

2.1. *Decision Support System (DSS)*

Decision Support System (DSS) merupakan sistem bantu berbasis komputer untuk pengambilan keputusan di bidang

manajemen yang bergelut dalam keputusan terstruktur. DSS mencakup sumber daya individu dan kemampuan komputer unntuk meningkatkan kualitas keputusan. Ciri-ciri DSS yang baik sebagai berikut.

a. Sederhana
b. Dapat diandalkan
c. Mudah dikendalikan
d. Menyesuaikan
e. Lengkap pada masalah penting
f. Mudah berkomunikasi dengannya.[5]

Adapun hal-hal yang membedakan DSS dengan proses data elektronik adalah sebagai berikut.

Tabel 2.1 DSS versus PDE

Dimensi	*Decision Support System (DSS)*	*Pengolah Data Elektronik (PDE)*
Penggunaan	Aktif	Pasif
Pemakaian	Manajemen lini dan staf	Pencatat
Tujuan	Keefektifan	Efisiensi
Rentang waktu	Sekarang dan masa datang	Masa lalu
Sasaran	Lentur	Taat azas

Manfaat yang dapat diambil dengan menggunakan DSS adalah sebagai berikut.

a. Punya kemampuan mendukung pemecahan masalah yang komplek.
b. Bereaksi cepat terhadap situasi yang tak diharapkan pada kondisi yang berubah DSS melakukan analisis kuantitatif dengan sangat cepat, dan menghemat waktu.

[5] Turban, E, at all. (2008). *E-Commerce 2008*. New Jersey: Pearson International.

c. Punya kemampuan dengan mencoba berbagai strategi berbeda kondisi dengan tepat dan cepat.

d. Belajar dan mengembangkan program baru, dengan menggunakan pola analisis "*what if*" (apabila), merupakan sarana dalam pelatihan manajer.

e. Membangun jembatan komunikasi, sehingga pengumpulan data dan pemecahan masalah yang merupakan alat untuk meningkatkan kerjasama tim.

f. Meningkatkan pengendalian pengukuran dan meningkatkan kinerja organisasi.

g. Menghemat biaya, pembuatan atau menghambat biaya akibat keputusan yang salah.

h. Keputusan lebih objektif, dan konsisten dibandingkan dengan intuisi saja.

i. Meningkatkan efektivitas manajerial, dengan menghemat waktu kerja pada bidang analisis, perencanaan dan pelaksanaan.

j. Meningkatkan produktivitas dari analisis.

2.2. *Audit*

Jurnal *Accounting Review dari American Accounting Association* mendefinisikan proses auditing sebagai "suatu proses sistematis untuk memperoleh serta mengevaluasi bukti secara objektif mengenai kegiatan dan peristiwa ekonomi, dengan tujuan menetapkan derajat kesuaian antara asersi-asersi tersebut dengan kriteria yang telah ditetapkan sebelumnya serta penyampaian hasil-hasilnya kepada pihak-pihak yang berkepentingan". [6]

[6] Boynton, William, C, Johnson, Raymond N., Kell, Walter G. (2003). *Modern Auditing 7th Edition.* Jakarta: Erlangga.

Boynton et. all. lebih lanjut mengelompokkan audit menjadi 3 jenis berdasarkan karakteristik kunci yang dimiliki masing-masing.

Ketiga jenis audit tersebut adalah sebagai berikut.

1. Audit laporan keuangan
2. Audit kepatuhan
3. Audit operasional

Audit sistem informasi dapat digolongkan sebagai gabungan dari jenis kepatuhan (mengevaluasi tingkat kepatuhan terhadap mekanisme kontrol atau pengendalian terhadap sistem) dan audit operasional (akan menilai kegiatan operasional yang berkaitan dengan keamanan informasi pada sistem).

Berdasarkan penyebabnya kegiatan audit dapat dibedakan menjadi 2 macam.

1. Audit operasi

   Audit jenis ini bersifat umum. Dilakukan karena rutin atau sebab lain. Penyebab dilakukannya audit operasi tidak spesifik atau tertentu.

2. Audit investigasi

   Jenis audit ini dilakukan karena ada masalah. Sehingga audit investigasi dilakukan untuk menemukan bukti-bukti dari kesalahan yang terjadi dalam sebuah system.

Berikut tahapan dalam suatu pemeriksaan atau audit terhadap sistem informasi.[7]

1. Peninjauan pendahuluan

   Pengumpulan informasi, seua informasi yang berkaitan dengan audit yang akan dilakukan, termasuk latar belakang perusahaan serta informasi umum lain yang terkait.

2. Analisis aplikasi

[7] Tugiman, H. (1996), *Pengantar Audit Sistem Informasi*. Yogyakarta: Kanisius.

Melakukan analisis terhadap aplikasi-aplikasi yang ada di dalam sistem.

3. Penilaian pengendalian intern

   Menentukan sejauh mana prosedur dan struktur organisasi yang relevan diberlakukan terhadap suatu sistem tertentu.

4. Pengujian ketaatan

   Dilakukan pengujian ketaatan atau compliance test dengan melakukan pembandingan atas criteria yang tercantum dalam suatu uraian narasi atau setiap aplikasi.

5. Review atas pengendalian kompensasi

   Dilakukan apabila ditemukan kemungkinan bahwa hasil pemeriksaan audit intern tidak tepat. Pengujian kompensasi ini diharapkan akan meyakinkan bahwa pengendalian kompensasi memang kuat dan dimiliki oleh perusahaan.

6. Pengujian substantive

   Berkaitan dengan catatan atau keluaran dan arus transaksi yang telah diuji melalui pengujian ketaatan.

Dalam hubungannya dengan komputer, kegiatan audit dibedakan menjadi 2 macam.

1. *Audit around computer* yaitu pengumpulan bukti-bukti audit hanya dilakukan seputar komputer saja, tidak melakukan penetrasi ke dalam komputer itu sendiri seperti menyelidiki alur *software logic* hingga sampai menelusuri data yang tersimpan.
2. *Audit through computer* yaitu melakukan assessment kondisi yang diaudit dengan menggunakan komputer. Isi dari komputer akan dilihat, terutama pada *software* yang digunakan dan semua informasi yang disimpan di dalamnya.

Pada penelitian ini akan dilakukan audit tipe *around computer* saja, tidak dilakukan penetrasi *through computer* untuk memperoleh bukti-bukti yang diperlukan dalam proses *assessment* kegiatan audit.

Standart-Standart Acuan untuk Melakukan Audit

1. ***ISO (International Standart Organization) 17799***

   Pada tahun 1995 Badan Standarisasi Inggris (*British Standards Institute*) mengeluarkan sebuah standart mengenai manajemen informasi yang disebut sebagai BS7799 Part 1 : *Information Technology–Code of practice for information security management.* Kemudian pada tahun 2000 standart tersebut diadaptasi seluruhnya oleh badan standarisasi dunia, ISO (*International Standart Organization)* menjadi ISO 17799 : 2000 *Information Technology – Code of practice for information security management.* [8]

   ISO 17799 terdiri dari kumpulan *best practice* yang bisa menjadi *guidelines* dalam melakukan assessment terhadap keamanan informasi dalam suatu organisasi. *Best practice* dinilai sebagai standart yang teruji karena disusun berdasar pengalaman hasil implementasi oleh para pakar keamanan informasi.

   ISO 17799 berisi 10 bagian utama yang disebut dengan control klousa. *Control clousa* ini terbagi menjadi 36 *control objek*. Pada *control objek* ini dijabarkan menjadi lebih detil dalam 127 *control security*.

   Sepuluh kontrol klousa dari ISO 17799 ini adalah sebagai berikut.

   1. Kebijakan keamanan (*Security policy*)

      Menjelaskan tentang kebijakan keamanan informasi (information security policy), jangakuan serta alsan mengapa kebijakan ini harus diterapkan pada tiap organisasi.

   2. Pengelolaan keamanan (*Organization security*)

[8] Dahblerg, T., Kivijarvi, H. (2006). *An Integrated Framework for IT Governance and the Development and Validation of an Assessment. IEEE : Proceeding of the 39th Hawaii International Conference on Systems Sciences.* Finland: Helsinki School of Economics.

Menjelaskan bagaimana keamanan informasi dikelola dalam sebuah organisasi.

3. Klasifikasi dan pengendalian asset (*Asset classification and control*)

   Aset organisasi dapat berupa informasi, software, hardware dan bahkan layanan (*services*). Semua hal tersebut berharga sehingga perlu dikelola dan dilindungi.

4. Keamanan personil (*Personel security*)

   Berisi hal-hal yang terkait dengan unsur manusia (*personnel*) dalam sebuah organisasi, seperti pelatihan, tanggung jawab, dan pemeliharaan prosedur.

5. Keamanan fisik dan lingkungan (*Physical and environment security*)

   Menjelaskan keamanan informasi ditinjau dari aspek fisik dan lingkungannya seperti bagaimana melindungi peralatan dan informasi dari ancaman secara fisik.

6. Pengaturan komunikasi dan operasional (*Communication and operation management*)

   Berisi hal-hal yang mengatur bagaimana sebaiknya pengelolaan dan keamanan dari kegiatan operasional pengolahan informasi sehari-hari agar aman.

7. Pengawasan terhadap akses (*System access control*)

   Kontrol pada akses terhadap sistem dan informasi yang ada sangat penting bagi keamanan dan kelangsungan bisnis sebuah organisasi. Sehingga kontrol akses harus dikelola dengan baik.

8. Pengembangan sistem dan perawatan (*System development and maintenance*)

   Mengatur tentang pengembangan sistsem dan perawatannya (*maintenance*). Apakah melibatkan vendor dari luar, serta bagaimana pengembangan system yang baru akan

mempengaruhi desain dan jalannya system yang sudah ada yang dapat mempengaruhi tingkat keamanan dan integritas informasi.

9. Pengelolaan kelangsungan bisnis (*Business continuity planning*)

   Terkait dengan bagaimana memperlakukan aktivitas bisnis yang esensial sehubungan dengan ancaman keamanna yang mungkin terjadi (misal bencana alam).

10. Pemenuhan/Kelengkapan (*Compliance*)

    Membicarakan bagaimana aturan bisnis dari suatu organisasi relevan dengan peraturan perundang-undangan yang berlaku.

2. *COBIT (Control Objectives for Information and Related Technology)*

Dalam bidang audit teknologi informasi terdapat satu nama standarisasi yang telah dikenal luas yaitu COBIT. Asosiasi auditor sistem informasi internasional atau *International System Audit and Control Association (ISACA)*, pada tahun1996 untuk pertama kalinya mengeluarkan standarisasi audit teknologi ifnormasi ini yang kemudian disebut *Control Objectives for Information and Related Technology (COBIT).*[9]

COBIT mendefinisikan 34 proses didalamnya yang dibagi menjadi 4 domain yaitu 11 proses pada Planning and organization, 6 proses pada domain *Acquisition and Implementation,* 13 proses pada domain *Delivery and Support,* serta 4 proses pada domain *monitoring*. COBIT mempunyai sebuah control objectives tentang keamanan yaitu pada proses DS5, *Ensure System Security Control Objectives*. DS5 ini dijabarkan dalam 21 detil. Tetapi *control objective* dari COBIT ini terlalu luas, karena hanya berbicara tentang keamanan umum.

[9] Weber, R. (1999). *Information Systems Control and Audit.* New Jersey: Prentice Hall.

2.3. Keamanan Informasi

Informasi yang terdapat pada sistem informasi harus dilindungi dari berbagai ancaman yang dapat terjadi. Keamanan terhadap informasi pada sistem informsi harus sesuai dengan standart mekanisme keamanan yang ada.

Burch dan Grudnitski menyebutkan 5 (lima) akibat yang dapat terjadi yang disebabkan oleh kurangnya tingkat pengendalian keamanan (*secuirity control)*, hal itu adalah sebagai berikut.

a. Menurut kinerja sistem
b. Kinerja sistem yang tidak akurat dapat berubah
c. Sistem tidak dapat memberikan layanan
d. Hilangnya asset
e. Penyingkapan informasi oleh pihak yang tidak berwenang. [10]

Akibat-akibat tersebut dapat terjadi karena adanya tujuh resiko terhadap keamanan sistem informasi yaitu sebagai berikut.

a. Tidak berfungsi sebagaimana mestinya (*malfunction)* baik pada *software*, *hardware* maupun manusia
b. Kecurangan (*fraud*) dan pencurian akses
c. Gangguan pada listrik dan alat komunikasi
d. Api
e. Sabotase dan kerusuhan
f. Bencana alam dan
g. Resiko lain

2.4. Sistem Informasi

Burch dan Grudnitski mendefinisikan informasi sebagai *data that have been put into a meaningful and useful context and*

[10] Burch, J; Grdnitski, G. (1989). *Information Systems Theory and Practice 5th Edition.* New York: John Wiley & Sons, Inc.

communicated to a recipient who uses it to make decisions, atau dengan kata lain informasi adalah data yang mengandung makna.

Pengolahan dari data menjadi informasi yang mengandung makna, dilakukan dalam sebuah sistem, yang disebut sebagai sebuah sistem informasi. Sistem informasi adalah kombinasi antara prosedur kerja, informasi, orang dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam sebuah organisasi.[11]

Prosedur kerja dalam sistem informasi ini akan mengatur agar sistem dapat berjalan dengan baik, untuk memastikan hal tersebut didalam sebuah sistem informasi perlu dipasang pengendalian-pengendalian. Pengendalian-pengendalian pada sistem informasi dapat dibedakan menjadi dua, yaitu pengendalian aplikasi dan pengendalian secara umum.[12]

Pengendalian aplikasi adalah pengendalian yang dipasang pada pengolahan aplikasi, yaitu pada pengendalian masukan (*input control),* pengendalian pengolahan proses (*processing control),* serta pengendalian keluaran (*output control).* Adapun pengendalian umum (*general control)* adalah sebagai berikut.

a. Pengendalian organisasi
b. Pengendalian dokumentasi
c. Pengendalian kerusakan perangkat keras
d. Pengendalian keamanan fisik
e. Pengendalian keamanan data

Kesemua bagian dari pengendalian aplikasi dan pengendalian umum ini ada pada sebuah sistem informasi.

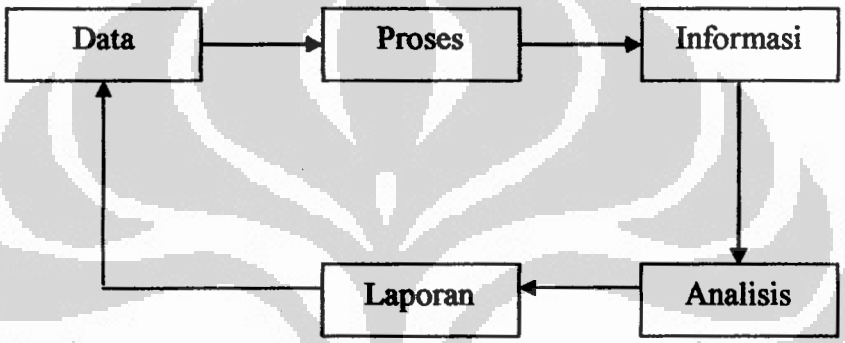
---

[11] Champlain, Jakck J. (2003). *Auditing Information System.* New Jersey: John Wiley & Sons, Inc.

[12] Jogiyanto. (1989). *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis.* Yogyakarta: Andi Offset.

2.5. Kerangka Teori

Decision Support System (DSS) pada Audit Keamanan Sistem Informasi Rumah Sakit "X" ini dilakukan menggunakan suatu perangkat lunak dengan bahasa pemrogaman Basic. 6.0, dan MySQL sebagai database server.



Gambar 2.1 Kerangka Teori

Penjelasan

1. **Data**

   Pada proses ini responden memasukan data :

   a. Nama Rumah Sakit

   b. Alamat Rumah Sakit

   c. Waktu : Tanggal, Bulan, Tahun (pelaksanaan audit)

   d. Jawaban : Nilai 1 "Ya", jika ada (diklik)

   e. Jawaban : Nilai 0 "Tidak", jika tidak ada (biarkan kosong)

2. **Proses**

   Pada tahap ini dihitung dihitung jawaban "Ya" dan "Tidak", untuk mendapatkan hasil akhir dimana dihitung jawaban yang terbanyak.

3. **Informasi**

   Pada proses ini ditampilkan hasil perolehan jawban "Ya" dan "Tidak" untuk kemudian dicari prosentase. Prosentase diperoleh dari nilai

perolehan "Ya" dibagi dengan Nilai Maximal Perolehan dikalikan dengan 100%. Berikut ini adalah tabel perolehan nilai maximal jawaban "Ya".

Tabel 2.2 Perolehan Nilai Maximal Jawaban Ya

No	*Clousa Control*	Nilai Maximal
1	**Kebijakan Keamanan**	2
2	**Pengelolaan Keamanan**	10
3	**Klasifikasi dan Pengendalian Aset**	3
4	**Keamanan Personil**	10
5	**Keamanan Fisik dan Lingkungan**	13
6	**Pengaturan Komunikasi dan Operasional**	24
7	**Pengawasan Terhadap Akses**	31
8	**Pengembangan dan Perawatan Sistem**	18
9	**Pengelolaan Kelangsungan Bisnis**	5
10	**Pemenuhan/Kelengkapan**	11
Jumlah		**127**

4. Analisis

Pada proses analisis ini berdasarkan data yang diperoleh dari proses kemudian dikelompokkan dalam bentuk tabel dan divisualkan dalam bentuk grafik serta trend.

5. Laporan

Tahap terakhir adalah laporan yang berisi kesimpulan, yaitu nilai perolehan, prosentase dan kondisi keamanan serta masalah yang timbul serta solusi.

BAB 3
METODE PENELITIAN

3.1. Ruang Lingkup Penelitian

Penelitian ini dilakukan antara bulan April sampai dengan bulan Mei 2009 berlokasi di Rumah Sakit "X" yang beralamat di Jalan Salemba Raya Jakarta Pusat. Penelitian dilakukan untuk mengetahui seberapa jauh penerapan keamanan sistem informasi (*security system)* di Rumah Sakit "X". Selain itu penelitian ini juga dilakukan untuk menganalisis dan mendesain DSS (*Decision Support System)* untuk audit keamanan sistem informasi Rumah Sakit, serta melakukan uji coba di Rumah Sakit "X".

Analisis data pada penelitian ini menggunakan analisis data kuantitatif deskriptif dengan pengujian DSS audit keamanan sistem informasi Rumah Sakit "X". Pengumpulan data menggunakan instrumen berupa pengisian kuisioner dan form data pada DSS yang telah dibuat yang sebelumnya dilakukan pelatihan penggunaan perangkat lunak tersebut. Data primer diperoleh dari observasi, wawancara serta hasil isian kuisioner.

3.2. Desain Penelitian

Metodologi peneltian yang digunakan pada penelitian ini adalah deskriptif. Penelitian ini dilakukan dalam tiga tahap.

1. Melakukan pengumpulan data tentang keamanan informasi pada sistem informasi Rumah "X".

   Sistem informasi Rumah Sakit "X" terkait langsung dengan 3 (tiga) bagian yaitu *Electronic Data Processing* (EDP), pengguna sistem informasi, serta pihak manajemen. Dari 3 (tiga) unsur inilah *assessment* terhadap keamanan informasi di sistem informasi milik Rumah Sakit "X" dilakukan. Pengumpulan data dilakukan menggunakan DSS yang telah dibuat terhadap 3 pihak terkait.

2. Menganilisis hasil temuan

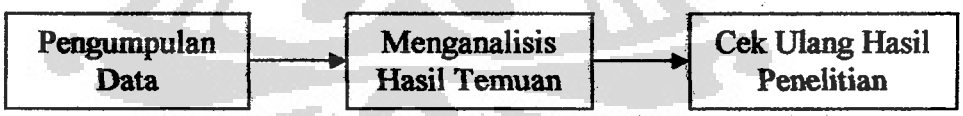
   Pada DSS ini, hasil temuan dianalisa mengikut cara penilaian Peltier (2002), yaitu menilai berapa banyak jawaban "Ya" yang diberikan. Jumlah jawaban "Ya" akan menentukan seberapa tingkat keamanan informasi pada sistem informasi yang diteliti.

Tabel 3.1 Penggolongan Kriteria Keamanan

No	*Nilai Perolehan Ya*	*Tingkat Keamanan*
1	> 91	Aman
2	79 – 90	Cukup Aman
3	65 – 78	Kurang Aman
4	52 – 64	Tidak Aman
5	< 51	Beresiko Tinggi

3. Melakukan cek ulang hasil penelitian

   Dengan cara melakukan wawancara dan observasi akan kondisi sebenarnya serta memeriksa konsistensi jawaban pada laporan DSS.



Gambar 3.1 Desain Penelitian

3.3. Subjek Penelitian

Adapun subjek penelitian ini adalah:

1. Manajemen Rumah Sakit (wakil direktur)
2. Pengguna Sistem Informasi/Operator Sistem Informasi (bagian instalasi rekam medik, HRD, farmasi)
3. Staf Bagian EDP (kepala divisi, staf bagian pengembangan, pengolah data SIM, programer dan teknisi).

3.4. Lokasi dan Waktu Penelitian

Penelitian ini dilakukan antara bulan April sampai dengan bulan Mei 2009 berlokasi di Rumah Sakit "X".

3.5. Pengumpulan Data

Pada penelitian ini akan dilakukan perhitungan nilai perolehan klousa dan nilai % menggunakan perangkat lunak DSS (*Decision Support System)* dan secara manual menggunakan *lembaran kuesioner*. Alat yang akan digunakan dalam penelitian ini adalah DSS yang mengacu pada 10 klausa pengendalian (*10 control clauses*), 36 sasaran pengendalian (36 *control objectives*) dan 127 pengendalian keamanan (127 *control security*) dari standarisasi keamanan informasi ISO 17799 yang terkandung didalamnya. Responden akan diminta menjawab dalam pilihan jawaban, yaitu "Ya" jika ada atau "Tidak" bila tidak ada yang sesuai.[13] Jawaban "Tidak" dari sebuah control yang diberikan oleh responden akan dilihat seberepa penting peranan control tersebut di dalam sistem dan dilihat potensi bahaya yang dapat ditimbulkan untuk kemudian diberikan rekomendasi bagaimana seharusnya control tersebut diberlakukan agar keamanan sistem informasi menjadi lebih terjamin.

Berikut ini adalah hal-hal yang yang akan dijadikan *clause control* pada DSS.

1. *Security policy* : mengetahui sejauh mana arah dan dukungan dari pihak manajemen terhadap keamanan informasi perusahaan.
2. *Asset classification and control* : mengetahui sejauhmana cara penanganan aset di Rumah Sakit "X".

---

[13] Peltier, Thomas R. (2002). *ISO 17799 Self Assessment Checklist*. http://www.occure.org/. Diakses tanggal 20 Mei 2009.

3. *Personel security* : mengetahui tingkat pengelolaan personil/staf yang berkaitan dengan keamanan informasi (meliputi tanggung jawab, deskripsi tugas dan sebagainya).
4. *Physical and environment security* : mengetahui tingkat keamanan ditinjau dari aspek fisik dan lingkungannya seperti bagaimana melindungi peralatan dan informasi dari ancaman keamanan secara fisik.
5. *Communication and operations management* : mengetahui sejauhmana pengelolaan dan keamanan dari kegiatan operasional pengolahan informasi.
6. *Access control* : mengetahui keamanan dan pengawasan terhadap hak akses terhadap system.
7. *Access Control :* pengawasan terhadap akses.
8. *System development and maintenance* : mengetahui tingkat keamanan dari kegiatan pengembangan sistem serta perawatannya (*maintenance)*.
9. *Business continuity planning* : mengetahui bagaimana keamanan informasi dilindungi agar tetap terjamin kondisi yang berhubungan dengan kelangsungan/kesinambungan jalannya bisnis/kegiatan operasional perusahaan.
10. *Compliance* : untuk mengetahui sejauhmana kesesuaian implementasi keamanan informasi di perusahaan dengan peraturan dan perundang-undangan yang berlaku.

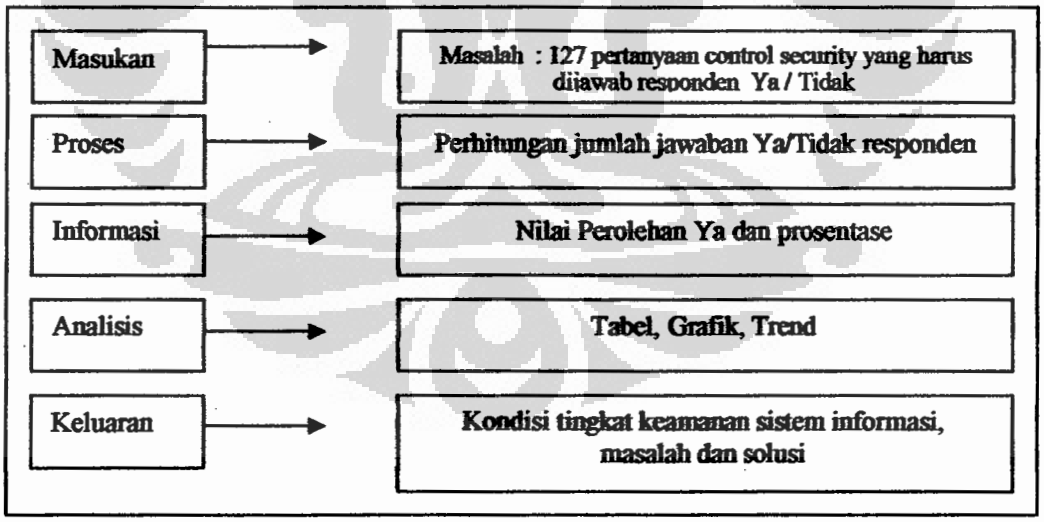
3.6. Pertanyaan Penelitian

Pertanyaan penelitian yang akan dijawab dalam penelitian ini adalah apakah sistem informasi pada Rumah Sakit "X" telah memenuhi standar keamanan berdasarkan ISO 17799 ?

BAB 4
ANALISIS DAN DESAIN SISTEM

4.1. Analisis Sistem

Analisis sistem adalah suatu penelitian yang dilakukan untuk memecahkan masalah yang mendasar atau untuk mengetahui keadaan yang sebenarnya tentang komponen-komponen objek penelitian menurut metode yang relevan dan konsisten sehingga tercapai pengertian tentang prinsip-prinsip dasar yang sebenarnya.[14] Pelaksanaan kegiatan analisis sistem pada hakekatnya mempunyai sejumlah langkah atau tahapan yang harus dilalui. Langkah-langkah atau tahapan-tahapan tersebut adalah melaksanakan identifikasi masalah dasar sebagai penyebab timbulnya masalah, mengidentifikasi keputusan apa yang harus diambil, menganalisa aktivitas apa saja yang akan dilakukan untuk perancangan sistem selanjutnya.



Gambar 4.1 Analisis Sistem DSS

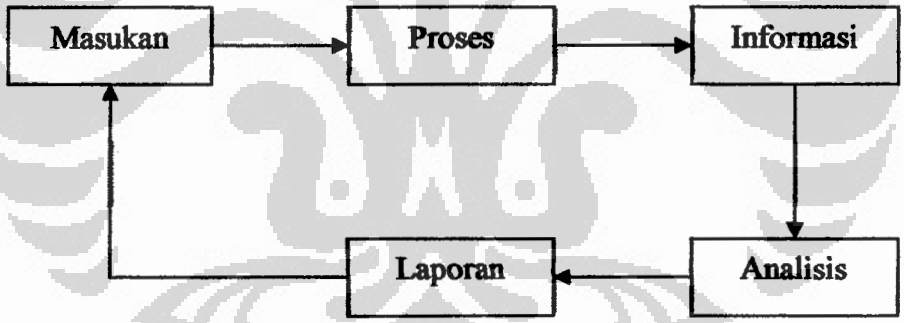
[14] Jogiyanto. (1989). *Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis.* Yogyakarta: Andi Offset.

4.2. Desain Sistem

Desain sistem adalah suatu penggambaran, perencanaan dan pembuatan sketsa atau pengaturan dari beberapa elemen yang terpisah ke dalam suatu kesatuan yang utuh dan berfungsi.

4.2.1. *Data Flow Diagram*

Data Flow Diagarm (DFD) adalah merupakan desain suatu sistem secara logika dan sangat tepat untuk digunakan dalam menggambarkan sistem yang dirancang. Penekanan *data flow diagram* adalah pada diagram arus data logika sehingga pemakai sistem dapat lebih mudah memahami arus data yang terjadi pada sistem yang diusulkan. Bentuk DFD dari DSS tersebut adalah seperti gambar berikut.



Gambar 4.2 Data Flow Diagram DSS

Tabel 4.1 DSS Pada Audit Sistem Informasi Rumah Sakit "X"

Masukan	*Proses*	*Informasi*	*Analisis*	*Laporan*
1.Form Data	1.Perhitungan	1.Hasil Perhitungan	1. Tabel 2. Grafik 3. Trend	1. Masalah 2.Tingkat Keamanan 4. Solusi

4.2.2. Manajemen Basis Data[15]

Manajemen basis data menggunakan perangkat lunak MySQL (Bahasa Inggris: *database management system*) atau DBMS yang *multithread*, *multi-user*, dengan sekitar 6 juta instalasi di seluruh dunia. MySQL adalah *Relational Database Management System* (RDBMS) yang didistribusikan secara gratis dibawah lisensi GPL (*General Public License*). Setiap orang bebas untuk menggunakan MySQL, namun tidak boleh dijadikan produk turunan yang bersifat *closed source* atau komersial. MySQL sebenarnya merupakan turunan salah satu konsep utama dalam database sejak lama, yaitu SQL (*Structured Query Language*). SQL adalah sebuah konsep pengoperasian basis data, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis. Keandalan suatu sistem database (DBMS) dapat diketahui dari cara kerja optimizernya dalam melakukan proses perintah-perintah SQL, yang dibuat oleh user maupun program-program aplikasinya. Sebagai database server, MySQL dapat dikatakan lebih unggul dibandingkan database server lainnya dalam query data. Hal ini terbukti untuk *query* yang dilakukan oleh *single user*, kecepatan *query* MySQL dapat sepuluh kali lebih cepat dari PostgreSQL dan lima kali lebih cepat dibandingkan *interbase*. Selain itu MySQL juga memiliki beberapa keistimewaan, antara lain sebagai berikut.

1. *Portability*

   MySQL dapat berjalan stabil pada berbagai sistem operasi seperti Windows, Linux, FreeBSD, Mac Os X Server, Solaris, Amiga, dan masih banyak lagi.

[15] Diakses dari : http://www.mysql.com (1 Mei 2009)

2. *Open Source*

   MySQL didistribusikan secara *open source* (gratis), dibawah lisensi GPL sehingga dapat digunakan secara cuma-cuma.

3. *Multiuser*

   MySQL dapat digunakan oleh beberapa pengguna dalam waktu yang bersamaan tanpa mengalami masalah atau konflik.

4. *Performance tuning*

   MySQL memiliki kecepatan yang menakjubkan dalam menangani *query* sederhana, dengan kata lain dapat memproses lebih banyak SQL per satuan waktu.

5. *Column types*

   MySQL memiliki tipe kolom yang sangat kompleks, seperti *signed/unsigned integer*, *float*, *double*, *char*, *text*, *date*, *timestamp*, dan lain-lain.

6. *Command* dan *functions*

   MySQL memiliki operator dan fungsi secara penuh yang mendukung perintah "*Select*" dan "*Where*" dalam *query*.

7. *Security*

   MySQL memiliki beberapa lapisan sekuritas seperti *level subnetmask*, nama *host*, dan izin akses pengguna dengan sistem perizinan yang mendetail serta kata sandi terenkripsi.

8. *Scalability* dan *limits*

   MySQL mampu menangani database dalam skala besar, dengan jumlah records lebih dari 50 juta dan 60 ribu tabel serta 5 milyar baris. Selain itu batas indeks yang dapat ditampung mencapai 32 indeks pada tiap tabelnya.

9. *Connectivity*

   MySQL dapat melakukan koneksi dengan *client* menggunakan protokol TCP/IP, Unix soket (UNIX), atau Named Pipes (NT).

10. *Localisation*

    MySQL dapat mendeteksi pesan kesalahan pada *client* dengan menggunakan lebih dari dua puluh bahasa. Meskipun demikian, bahasa Indonesia belum termasuk didalamnya.

11. *Interface*

    MySQL memiliki *interface* (antar muka) terhadap berbagai aplikasi dan bahasa pemrograman dengan menggunakan fungsi API (*Application Programming Interface*).

12. *Clients* dan *tools*

    MySQL dilengkapi dengan berbagai *tool* yang dapat digunakan untuk administrasi basis data, dan pada setiap *tool* yang ada disertakan petunjuk *online*.

13. Struktur tabel

    MySQL memiliki struktur tabel yang lebih fleksibel dalam menangani ALTER TABLE, dibandingkan *database* lainnya semacam PostgreSQL ataupun Oracle.

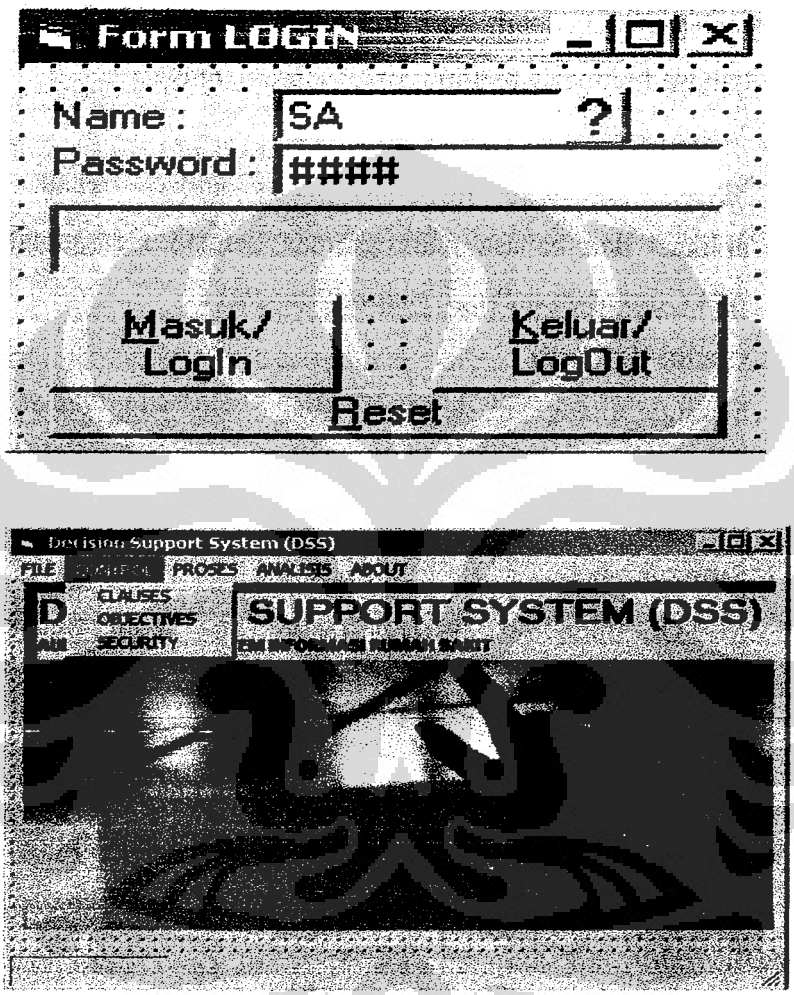
    Desain *database* meliputi desain menu utama, menu data dan menu proses, menu analisis, menu informasi dan menu laporan.

4.2.3. Desain *Input*

Desain atau perancangan *input* digunakan untuk menampilkan pemasukan data pada layar komputer yang dapat digunakan sebagai masukan. Tujuan dari desain input adalah untuk mengefektifkan dan menjamin masukan data. Desain *input* merupakan dialog antara pemakai sistem dengan program aplikasi, supaya diperoleh data yang akurat sesuai dengan yang diinginkan. Dengan adanya perancangan masukan ini maka kesalahan dalam pemasukan data dapat dihindari. Proses pemasukan data yang efieisen dan efektif dibuat menggunakan kode-kode untuk mewakili suatu data.

Desain *input* meliputi desain menu utama dan menu data.

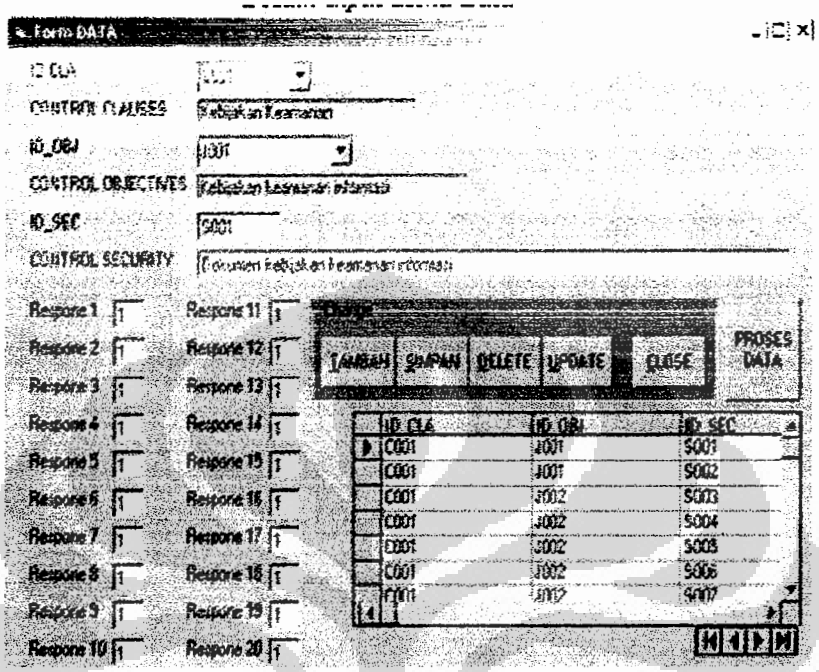
a. Desain Menu Utama



Gambar 4.3 Desain *Input* Menu Utama

b. Desain Menu Data

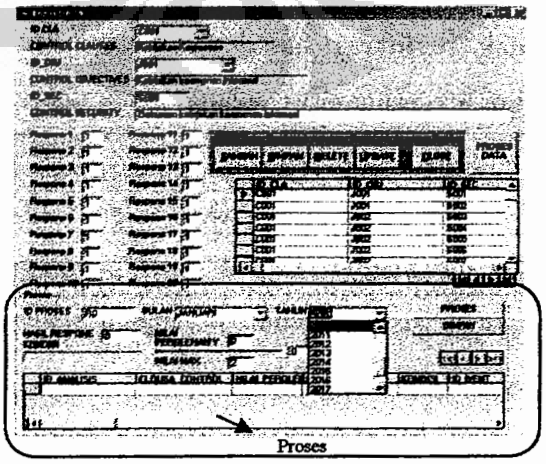
Desain *input* atau perancanan input digunakan untuk menampilkan masukan program. Desain *input* meliputi desain *form* data.



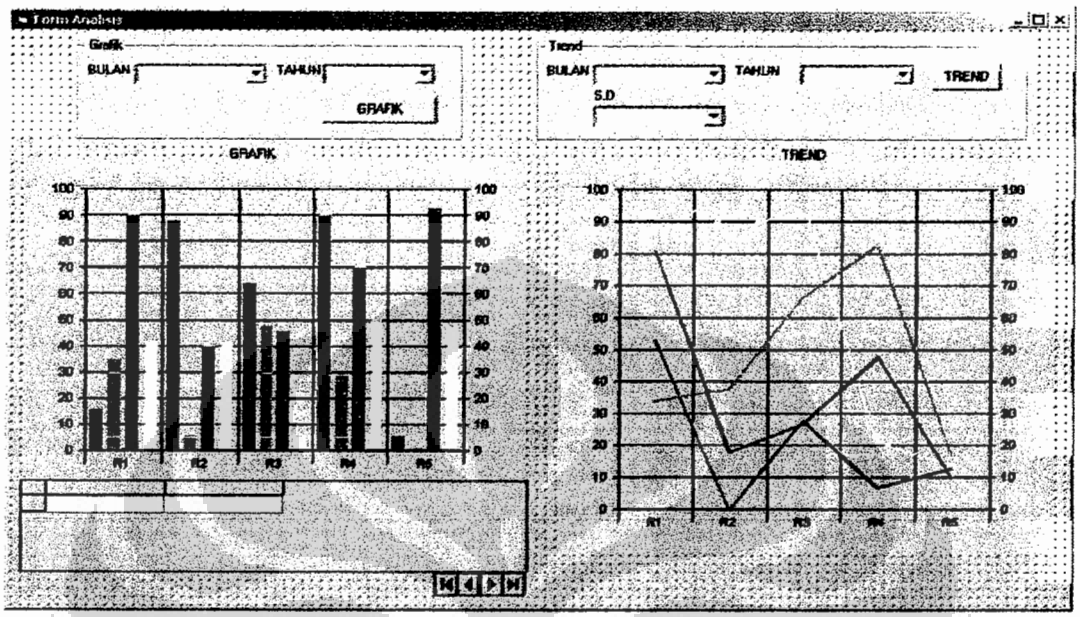
Gambar 4.4 Desain *Input* Menu Data

4.2.4. Desain *Output*

Desain *output* atau perancanan *output* digunakan untuk menampilkan keluaran program. Desain *output* meliputi desain menu informasi, analisis dan laporan.



Gambar 4.5 Desain *Output* Menu Proses



Gambar 4.6 Desain *Output* Menu Analisis

4.3. Implementasi Sistem

Jika sistem telah dirancang, maka tahap berikutnya adalah tahap penerapan dari sistem tersebut (*system implementation*). Pada tahap ini akan teruji apakah sistem yang diarancang akan berfungsi dan dapat dioperasikan dengan baik pada kondisi yang sesungguhnya ataukah tidak.

Sistem berfungsi baik, jika sistem yang digunakan dapat mencapai tujuan organisasi dengan prinsip efisien dan efektif. Sedangkan sistem dikatakan tidak berfungsi baik, jika sistem tersebut ternyata banyak kelemahan dan kekurangannya sehingga memboroskan tenaga, waktu dan biaya.

4.3.1. Konfigurasi Sistem

Konfigurasi sistem adalah perangkat keras pendukung sistem dan perangkat lunak yang dibutuhkan.

1. Perangkat keras (*Hardware*)
   a. Prosesor : minimal Pentium III 500 atau setara

b. *Memory/RAM* : minimal 128 MB

c. *Harddisk* : sisa minimal 50 MB

d. *Device input* : *keyboard, mouse*

e. *Device output* : *monitor* (resolusi 800 x 600) atau yang lebih tinggi

: *printer*

2. Perangkat lunak (*software*)
   a. Sistem operasi Windows XP atau yang lebih tinggi
   b. Program Visual Basic 6.0
   c. Program MySQLODBC
   d. Program aplikasi DSS
3. Sistem Operasi

   Sistem ini dijalankan menggunakan sistem Windows XP atau yang lebih tinggi.

4.3.2 Proses Sistem

Proses sistem yang akan penulis kemukakan berisi penjelasan tentang proses : masukan (data), proses, informasi, analisis, laporan (keluaran).

Data

Pada proses ini responden memasukan data :

- Nama Rumah Sakit
- Alamat Rumah Sakit
- Waktu : Bulan, Tahun (pelaksanaan audit)
- Jawaban : 1 "Ya", jika ada
- Jawaban : 0 "Tidak", jika tidak ada

Proses

Pada tahap ini dihitung dihitung jawaban "Ya" dan "Tidak", untuk mendapatkan hasil akhir dimana dihitung jawaban yang terbanyak.

Informasi

Pada proses ini ditampilkan hasil perolehan jawaban "Ya" dan "Tidak" untuk kemudian dicari prosentase. Prosentase diperoleh dari nilai perolehan "Ya" dibagi dengan Nilai Maximal Perolehan dikalikan dengan 100%. Berikut ini adalah tabel perolehan nilai maximal jawaban "Ya".

Tabel 4.2 Perolehan Nilai Maximal Jawaban Ya

No	*Clousa Control*	*Nilai Maximal*
1	Kebijakan Keamanan	2
2	Pengelolaan Keamanan	10
3	Klasifikasi dan Pengendalian Aset	3
4	Keamanan Personil	10
5	Keamanan Fisik dan Lingkungan	13
6	Pengaturan Komunikasi dan Operasional	24
7	Pengawasan Terhadap Akses	31
8	Pengembangan dan Perawatan Sistem	18
9	Pengelolaan Kelangsungan Bisnis	5
10	Pemenuhan/Kelengkapan	11
	Jumlah	127

Analisis

Pada proses analisis ini berdasarkan data yang diperoleh dari proses kemudian dikelompokkan dalam bentuk tabel dan divisualkan dalam bentuk grafik.

Laporan

Tahap terakhir adalah laporan yang berisi kesimpulan, yaitu nilai perolehan, prosentase dan kondisi keamanan serta masalah yang timbul serta solusi.

4.3.3 Pengetesan

Proses pengetesan dilakukan untuk mengetahui apakah sistem ini berfungsi baik atau tidak. Pengetesan sistem dilakukan dengan cara

memasukkan data yang sebenarnya dan kemudian memasukkan data rekaan.

Dengan cara pengetesan tersebut maka akan ada beberapa hal yang telah terpenuhi sebagai berikut.

1. Kesahihan data, *field-field* pada setiap database telah memilki nama, tipe, dan ukuran yang benar.
2. Kelengkapan, setiap record semua file database telah sesuai dengan batasan tertentu yang telah ditentukan sebelumnya.
3. Batasan, *field* data tertentu pada *field-field* database telah sesuai dengan batasan tertentu yang telah ditentukan sebelumnya.
4. Logika program, telah sesuai dengan logika yang diinginkan, seperti pencarian data, tampilan pesan-pesan. Misalnya pada saat memasukkan password, tetapi lupa, maka akan ada pesan *error* dan diulangi lagi.

Langkah-langkah instalasinya adalah sebagai berikut.

1. Masukkan flash / CD instalasi ke CD ROM drive.
2. Install file MySQLODBC.exe
3. Install file xampp-win32-1.6.3-installer
4. Jalankan file *DSS.exe* dan ikuti proses instalasi sampai selesai.
5. Jalankan program dengan cara klik tombol Start, pilih Program, pilih DSS atau atau klik icon untuk memanggil DSS.

4.4. Evaluasi Sistem

Di dalam pembuatan atau perancangan suatu sistem, tentu akan terdapat beberapa kelebihan ataupun kekurangan sistem.

BAB 5
HASIL PENELITIAN

Penelitian ini dilakukan untuk mengetahui kondisi keamanan informasi pada sistem informasi Rumah Sakit "X" yang dilakukan pada bulan April sampai Mei 2009. Penelitian terbagi menjadi dua tahap yaitu berupa pengambilan data sekunder dan pengambilan data primer. Data sekunder diperoleh dari Rumah Sakit "X" (Manajemen Rumah Sakit, Pengguna Sistem Informasi dan Staf Bagian Pengolahan Data Elektronik). Data primer yang mencakup *usability* dan *performance* perangkat lunak DSS (*Decision Support System*) untuk audit keamanan informasi diperoleh dari observasi, wawancara, dan pengisian formulir tanggapan pada responden Rumah Sakit "X". Sebelum menggunakan DSS, responden diberi penjelasan cara mengisi kuisioner dan cara menggunakan perangkat lunak DSS. Setiap responden mengisi kuesioner secara manual dan menggunakan perangkat lunak DSS untuk audit keamanan informasi pada Rumah Sakit "X".

5.1. Jumlah Responden

Jumlah responden untuk audit keamanan informasi Rumah Sakit "X" sebanyak 9 orang responden, jumlah ini sudah mewakili dari bagian-bagian yang berkaitan langsung dengan penggunaan sistem informasi Rumah Sakit "X" baik ditinjau dari *job description* dan latar belakang pendidikan. Responden terdiri dari 1 orang dari manajemen rumah sakit (wakil direktur), 3 orang dari pengguna sistem informasi (staf bagian rekam medik, HRD dan farmasi) serta 5 orang dari bagian pengolahan data elektronik (kepala divisi, staf bagian pengembangan, pengolahan data, programer dan teknisi).

5.2. Pendidikan Responden

Pendidikan terakhir responden adalah diploma 3 sebanyak 4 orang, strata 1 (S1) 4 orang dan strata 2 (S2) sebanyak 1 orang.

5.3. Sistem Operasi yang Digunakan

Sistem operasi yang digunakan oleh responden adalah sebagai berikut.

a. Windows.Vista : 4 orang
b. Windows XP : 4 orang
c. Linux : 1 orang

5.4. Instalasi

Perangkat lunak yang digunakan yaitu bahasa pemrogaman Visual Basic 6.0, untuk menjalankannya maka harus dilakukan instalasi terlebih dahulu.

5.5. Langkah Audit Keamanan Sistem Informasi

5.5.1. Menggunakan Kuesioner

Audit keamanan sistem informasi menggunakan kuesioner dilakukan dengan cara responden mengisi kuesioner yang telah tersedia dengan menuliskan tanda ✓ (*checklist*) pada jawaban "Ya" atau "Tidak". Jumlah jawaban "Ya" akan menentukan seberapa tingkat keamanan informasi pada sistem informasi yang diteliti. Mengetahui kondisi keamanan sistem informasi rumah sakit ini, semua jawaban ya dan tidak responden dihitung menggunakan kalkulator kemudian di cari persentase dengan cara menjumlah nilai perolehan "Ya" dibagi dengan nilai maximal perolehan dikalikan 100%.

5.5.2. Menggunakan Perangkat Lunak *Decision Support System*

Audit keamanan sistem informasi menggunakan alat bantu DSS (*Decision Support System*) dilakukan dengan cara sebagai berikut.

1. Aktifkan komputer.
2. Jalankan perangkat lunak DSS, dengan cara klik icon DSS atau double klik pada file DSS.exe.
3. Lakukan proses *log-in* (mengisi *username* dan *password*)
4. Pada tampilan awal akan muncul menu utama Data, Proses, Informasi, Analisis, dan Laporan.

5. Jawaban Responden diisi dengan cara klik menu Data, kemudian klik pada kotak yang tersedia jika jawaban "Ya" dan biarkan kosong (tidak diisi) untuk jawaban "Tidak" sampai dengan pertanyaan terakhir.

   Pertanyaan klousa kontrol yang harus dijawab responden adalah sebagai berikut.

   a. Manajemen Rumah Sakit sebanyak 7 klousa kontrol, yaitu *Security Policy, Organizational Security, Asset Classification and Control, Personal Security, Physical and Environmental Security, Business Continuity Management, Compliance*.
   b. Pengguna Sistem Informasi sebanyak 4 klousa control, yaitu *Security Policy, Personal Security, Physical and Environmental Security, Acess Control*.
   c. Pengolah Data Elektronik sebanyak 10 klousa control, yaitu *Security Policy, Organizational Security, Asset Classification and Control, Personal Security, Physical and Environmental Security, Communication and Operation Management, Acess Control, System Development and Maintenance, Business Continuity Management, Compliance*.
6. Hasil akhir dihitung dari jawaban yang terbanyak dengan cara klik menu Proses.
7. Hasil perhitungan dalam bentuk prosentase dapat dilihat dengan cara klik menu informasi. Perhitungan prosentase diperoleh dari jumlah nilai perolehan "Ya" dibagi dengan nilai maksimal perolehan dikalikan 100%.
8. Visualisasi dalam bentuk grafik bisa dilihat dengan cara klik menu Analisis, ini diperoleh dari hasil perhitungan pada menu proses.
9. Sedangkan laporan akhir yang berisi nilai perolehan, prosentase dan kondisi keamanan serta solusi dapat dilihat dengan cara klik menu Laporan.

Jawaban Responden adalah sebagai berikut.

a. Hasil Jawaban Responden Bagian Manajemen Rumah Sakit

Pertanyaan pada DSS diberikan kepada Wakil Direktur Penunjang Medik.

1. *Security Policy*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini sudah **aman,** dilihat dari jawaban yang mencapai nilai 100% (2 dari 2).

2. *Organizational Security*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini sudah **aman,** dilihat dari jawaban yang mencapai nilai 100% (10 dari 10).

3. *Asset Clasification and Control*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **beresiko tinggi,** dilihat dari jawaban yang mencapai nilai 33% (1 dari 3).

4. *Personal Security*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **aman,** dilihat dari jawaban yang mencapai nilai 100% (10 dari 10).

5. *Physical and Environmental Security*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **aman,** dilihat dari jawaban yang mencapai nilai 100% (13 dari 13).

6. *Business Continuity Management*

   Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 60% (3 dari 5).

   Dua hal yang belum dilaksanakan pihak manajemen adalah memastikan rencana business continuity planning konsisten dalam semua levelnya serta menguji secara berkala rencana tersebut.

7. *Compliance*

Menurut pihak manajemen, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 63% (7 dari 11).

b. Hasil Jawaban Responden Bagian Pengguna Sistem Informasi

Pertanyaan pada DSS diberikan kepada personil dari:

1) Instalasi Rekam Medik;
2) *Human Resource Department;*
3) Farmasi.

Jawaban responden adalah sebagai berikut.

1. *Kebijakan Keamanan (Security Policy)*

Menurut pihak pengguna, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **beresiko tinggi,** dilihat dari jawaban yang mencapai nilai 0% (0 dari 2).

2. *Personal Security*

Menurut pihak pengguna, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 60% (6 dari 10).

3. *Physical and Environmental Security*

Menurut pihak pengguna, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **cukup aman,** dilihat dari jawaban yang mencapai nilai 61% (8 dari 13).

4. *Acess Control*

Menurut pihak pengguna, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **cukup aman,** dilihat dari jawaban yang mencapai nilai 61% (19 dari 31).

c. Hasil Jawaban Responden Bagian PDE

Pertanyaan pada DSS diberikan kepada personil dari :

1. Kepala Divisi

2. Staf bagian Pengembangan Program
3. Pengolahan Data SIM
4. Programmer
5. Teknisi

Jawaban responden adalah sebagai berikut.

1. Kebijakan keamanan *(Security Policy)*

Pada clousa ini terdapat perbedaan pendapat, ada yang menyatakan telah didokumentasikan dan ada yang menyatakan tidak. Setelah dilakukan cek, ternyata memang belum ada dokumentasi akan kebijakan keamanan informasi. Kebijakan keamanan memang telah ada tetapi belum didokumentasikan.

Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masih **beresiko tinggi,** dilihat dari jawaban yang mencapai nilai 0% (0 dari 2).

2. Pengelolaan keamanan *(Organizational Security)*

Dari jawaban kuesioner terdapat beberapa perbedaan tentang resiko yang mungkin timbul dari akses oleh pihak luar (kontrol 2.2.1.), dimana kepala divisi (P1) menyatakan belum ada standart keamanan yang khusus diterapkan untuk kemungkinan akses oleh pihak luar, sementara staf lain menyatakan sudah ada.

Setelah dilakukan pemeriksaan ternyata belum ada langkah pengamanan pada klousa tersebut.

Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masih **beresiko tinggi,** dilihat dari jawaban yang mencapai nilai 30% (3 dari 10).

3. Asset classification and control (Klasifikasi dan pengendalian aset)

Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **beresiko tinggi,** dilihat dari jawaban yang mencapai nilai 33% (1 dari 3).

4. *Personal security* (Keamanan personil)

   Pada klousa ini terdapat perbedaan yang menarik yaitu pada 4.1.3 dan 4.1.4, dimana kepala divisi menyatakan bahwa ada perjanjian kerahasiaan dan ada persyaratan tentang tanggung jawab keamanan pada kontrak kerja, tetapi semua karyawan mengatakan sebaliknya. Setelah dilakukan pemeriksaan ulang ternyata memang tidak ada perjanjian kerahasiaan, tetapi dalam kontrak kerja memang disebutkan tanggung jawab terhadap keamanan informasi milik perusahaan (4.1.4).

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **cukup aman,** dilihat dari jawaban yang mencapai nilai 80% (8 dari 10).

5. *Physical and environment security* (Keamanan fisik dan lingkungan)

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **aman,** dilihat dari jawaban yang mencapai nilai 77% (10 dari 13).

6. *Communication and operation management* (Pengaturan komunikasi dan operasional)

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 54% (13 dari 24).

7. *System access control* (Pengawasan terhadap akses)

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **aman,** dilihat dari jawaban yang mencapai nilai 85% (24 dari 29).

8. *System development and maintenance* (Pengembangan dan perawatan system)

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 50% (9 dari 18).

9. *Business Continuity Management* (Pengelolaan kelangsungan bisnis)

   Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 60% (3 dari 5).

10. *Compliance* (Pemenuhan/kelengkapan)

    Menurut bagian PDE, kondisi Rumah Sakit "X" dari segi ini masuk dalam kategori **kurang aman,** dilihat dari jawaban yang mencapai nilai 45% (5 dari 11).

BAB 6
PEMBAHASAN

6.1. Proses Penelitian

Pada penelitian ini pengumpulan data dimulai dengan melakukan pengumpulan data sekunder yang akan digunakan sebagai bahan pembuatan *Decision Support System* (DSS). Data diambil dengan wawancara dan mengisi kuesioner kepada Rumah Sakit "X" (manajemen rumah sakit, pengolah data elektronik, dan pengguna sistem informasi). Selanjutnya pengambilan data primer dilakukan dalam bentuk wawancara, observasi, dan pengisian kuesioner.

6.2. Keterbatasan Penelitian

Dalam penelitian ini ditemukan beberapa kendala antara lain sebagai berikut.

a. Keterbatasan waktu dan sumber daya yang ada, penelitian hanya dibatasi dari segi *usability* yaitu menilai apakah perangkat ini dapat melakukan audit dengan tepat, cepat, dan kesulitan atau kemudahan apa yang dijumpai pada penggunaan perangkat lunak tersebut.
b. Dari segi verifikasi dinilai apakah perangkat lunak ini dapat dijalankan di berbagai sistem operasi, dan dari segi validasi dicari *fault* apakah yang ditemui selama perangkat lunak ini dijalankan. Pengujian observasi lain seperti *performance*, *security*, *availability*, *reliability*, dan *capacity* tidak mungkin dilakukan karena membutuhkan waktu yang lebih lama dan observasi yang lebih cermat.
c. Kompatibilitas pada penelitian ini hanya terbatas pada sistem operasi yang digunakan. Kompatibilitas dengan program atau perangkat lunak lain tidak diteliti sehubungan dengan keterbatasan waktu dan subjek penelitian.

6.3. Pembahasan Hasil Penelitian

6.3.1. Kompatibilitas

Dalam penelitian ini ditemukan 1 responden tidak dapat menjalankan perangkat lunak DSS, karena menggunakan sistem operasi Linux. Hal ini menunjukkan ada suatu *inkompatibilitas* perangkat lunak dengan sistem operasi (atau program lain yang berhubungan) yang digunakan. Ini terjadi pada saat pembuatan suatu perangkat lunak, apabila perancangannya mengkoding atau melakukan pengujian perangkat lunak dengan menggunakan sistem operasi versi terbaru atau satu sistem operasi saja. Akibat yang ditimbulkan adalah perangkat lunak menjadi tidak sepenuhnya kompatibel dengan sistem operasi yang digunakan atau sistem operasi lain. Salah satu penyebab kegagalan perangkat lunak adalah tidak adanya kompatibilitas dengan program lain seperti sistem operasi atau program lain yang terkait dengan perangkat lunak. Sebenarnya hal ini tidak dapat dikatakan menjadi suatu kegagalan dari perangkat lunak apabila perancangan, koding, dan pengujian memang ditujukan untuk sebagian besar pengguna yang menggunkan sistem operasi yang sesuai. Suatu kegagalan terjadi apabila perangkat lunak ditujukan untuk kompatibel dengan berbagai sistem operasi dan dalam versi apapun atau secara signifikan tidak dapat digunakan oleh kebanyakan pengguna.[16]

6.3.2. *Fault*

Responden menemukan beberapa *fault* yang menyebabkan harus menghentikan proses pengerjaan, atau mengulang pengerjaan dari awal. *Fault* yang dijumpai berupa tidak munculnya data yang dimasukkan dan tidak dapat melakukan proses *log-in*. Hal ini disebabkan oleh adanya ketidakmampuan program membaca atau menautkan sistem manajemen basis data MySQL yang ada. Idealnya

[16] Diakses dari [redacted] (1 Mei 2009).

sebelum penggunaan dipastikan terlebih dahulu apakah sudah terpasang MySQL pada komputer.

Selain itu munculnya *fault* tersebut akibat adanya kesalahan koding (*coding errors)*. Tidak semua *fault* pada suatu perangkat lunak disebabkan oleh kesalahan koding. Salah satu yang umumnya menyebabkan kecacatan atau *defek* adalah adanya kesenjangan kebutuhan (*requirements gaps*), misalkan adanya kebutuhan yang tidak terpenuhi sehingga menimbulkan kesalahan oleh perancang program tersebut. *Requriements gaps* yang umumnya digunakan adalah *non-functional requirements* yang terdiri dari *testability, scalability, maintanability, usability, performance,* dan *security*. *Fault* dapat muncul dalam berbagai proses tersebut. Seorang programer dapat membuat kesalahan yang menghasilkan suatu *fault* pada kode sumber (*source code*). Jika *fault* ini tetap dijalankan (*execute*) pada situasi tertentu akan menimbulkan hasil yang salah yang menyebabkan suatu kegagalan (*failure*).[17]

6.3.3. Hasil Audit

Pada sub bab ini akan dibahas hasil penelitian keseluruhan dari hasil tiap klausa kontrol dari semua responden.

1. *Security policy*

   Nilai total clouse 0 = 0% (dari nilai maksimal 2), *kondisi beresiko tinggi*.

   Walaupun pihak manajemen menyatakan telah terdapat dokumen keamanan informasi tetapi pihak yang terkait langsung dalam hal ini bagian PDE serta pengguna sistem informasi di Rumah Sakit "X" menyatakan belum terdapat dokumentasi tersebut serta tidak terdapat pula bukti atas hasil audit ini (tidak ada dokumentasi yang dimaksud).

[17] Kolawa, Adam; Huizinga, Dorota (2007) Wiley-IEEE Computer Society Press. p. 86.

Sehingga disimpulkan bahwa Rumah Sakit "X" belum melaksanakan langkah yang diperlukan yakni membuat dan mensosialisasikan dokumentasi keamanan informasi.

2. *Organization security*

   Nilai total clouse 3 = 30% (dari nilai maksimal 10), ***kondisi beresiko tinggi.***

   Hal-hal yang perlu diperhatikan adalah sebagai berikut.

   a. **Belum terdapat koordinasi lintas gugus untuk penerapan keamanan informasi (2.1.2).**
   b. **Belum adanya tenaga ahli yang dapat memberikan nasihat khusus dalam bidang keamanan informasi (2.1.5).**
   c. **Belum adanya kerjasama antar lembaga.**
   d. **Belum terdapat kajian independen terhadap praktek keamanan informasi (2.1.7).**
   e. **Belum adanya langkah menganalisa konektivitas dengan pihak luar (2.2.1).**
   f. **Belum adanya penyertaan spesifikasi tentang keamanan informasi pada kontrak dengan pihak luar (2.2.2 dan 2.3.1).**

3. *Asset classification and control*

   Nilai total clouse 1 = 33% (dari nilai maksimal 3), ***kondisi beresiko tinggi.***

   Hal-hal yang harus diperhatikan oleh Rumah Sakit "X" adalah sebagai berikut.

   a. **Membuat klasifikasi informasi berdasar prioritas untuk keperluan proteksi (3.2.1).**
   b. **Membuat prosedur penamaan dan penanganan informasi untuk mengindikasikan tingkat keamanan informasi (3.2.2).**

4. *Personel security*

   Nilai total clouse 8 = 80% (dari nilai maksimal 10), ***kondisi aman.***

Untuk meningkatkan jaminan keamanan informasi yang dimiliki sebaiknya Rumah Sakit "X" membuat prosedur formal untuk menangani karyawan yang melanggar kebijakan keamanan (4.3.5) sehingga karyawan akan bersikap hati-hati dan ikut menjaga keamanan informasi rumah sakit.

5. *Physical and environment security*

   Nilai total clouse 10 = 77% (dari nilai maksimal 13), ***kondisi aman.***

   Hal-hal yang perlu diperhatikan untuk meningkatkan keamanan informasi dari segi ini adalah sebagai berikut.

   a. Memastikan pengamanan ruangan/bangunan yang menyediakan layanan pemrosesan informasi karena pengguna berpendapat masih belum cukup aman (5.1.3).
   b. Perlu adanya perlindungan keamanan lebih untuk staf yang bekerja di daerah khusus (5.1.4) maupun untuk melindungi peralatan yang berada di luar kantor (5.2.5).
   c. Meminimalisir kemungkinan penyadapan pada sarana telekomunikasi (5.2.3).

6. *Communication and operation management*

   Nilai total clouse 13 = 54% (dari nilai maksimal 24), ***kondisi kurang aman.***

   Hal-hal yang membuat Rumah Sakit "X" kurang aman adalah sebagai berikut.

   a. Belum terdokumentasikannya prosedur operasional (6.1.1).
   b. Belum adanya proses pengendalian perubahan (6.1.2).
   c. Tidak adanya catatan kegiatan operasional (6.4.2).
   d. Perlunya perhatian lebih pada pengelolaan pemindahan media penyimpanan (6.6.1 dan 6.7.2).
   e. Perlunya pengamanan dokumentasi sistem, perjanjian pertukaran informasi dengan pihak lain (6.7.1).
   f. Perlunya pengamanan e-commerce (6.7.3).

g. Pengamanan pemakaian e-mail (6.7.4).

h. Kebijakan kemanan kantor elektronis (6.7.5).

i. Pengawasan keamanan pada pertukaran informasi dengan cara lain (6.7.7).

7. *System access control*

Nilai total clouse 23 = 74% (dari nilai maksimal 31), *kondisi aman.*

Hal-hal yang perlu ditingkatkan lagi adalah sebagai berikut.

a. Adanya review periodik atas akses pengguna (7.2.4).

b. Perlunya sosialisasi bagi pengguna dan kontraktor tentang pentingya keamanan dan prosedur perlindungan peralatan yang digunakan maupun tidak (7.3.2).

c. Perlunya autentikasi pengguna untuk konektivitas keluar (7.4.3).

d. Perlunya autentikasi titik/node pada koneksi jarak jauh (7.4.4).

e. Perlunya proses yang dilakukan oleh teknisi untuk mengontrol akses terhadap port yang didiagnosis digunakan untuk jarak jauh (remote) (7.4.5).

f. Pembatasan waktu koneksi bagi terminal yang terkoneksi pada data sensitif (7.5.8).

g. Keamanan penggunaan komputasi mobile dan teleworking harus mulai diatur (7.8.1 dan 7.8.2).

8. *System development and maintenance*

Nilai total clouse 9 = 50% (dari nilai maksimal 18), *kondisi tidak aman.*

Hal-hal yang perlu ditingkatkan lagi adalah sebagai berikut.

a. Kontrol pemrosesan internal (8.2.2).

b. Autentikasi pesan untuk data sensitif (8.2.3).

c. Validasi data keluaran (8.2.4).

d. Kebijakan kontrol tentang penggunaan kriptografi (8.3.1).

e. Penggunaan enkripsi dengan metode terbaru (8.3.2).
f. Peninjauan tentang perlunya digital signatures (8.3.3).
g. Non repudiation service (8.3.4).
h. Key management (8.3.5).
i. Langkah pencegahan akan kemungkinan adanya channel tersembunyi dan kode trojan (8.5.4).

9. *Business continuity planning*

Nilai total clouse 3 = 60% (dari nilai maksimal 5), ***kondisi kurang aman.***

Agar maksimal dalam pengelolaan kelangsungan bisnis, Rumah Sakit "X" perlu memperhatikan hal-hal sebagai berikut.

a. Mengkonsistensikan rencana kesinambungan bisnis dalam tiap level organisasi (9.1.4);
b. Menguji rencana tersebut secara berkala (9.1.5);

10. *Compliance*

Nilai total clouse 5 = 45% (dari nilai maksimal 11), ***kondisi tidak aman.***

Hal-hal yang belum dipenuhi Rumah Sakit "X" agar menjadi aman adalah sebagai berikut.

a. Pada identifikasi peraturan yang diberlakukan (10.1.1).
b. Hak atas kekayaan intelektual (10.1.2).
c. Pengawasan akan kriptografi (10.1.6).
d. Pengumpulan bukti (10.1.7).
e. Kesesuaian keseluruhan organisasi dengan kebijakan keamanan (10.2.1).
f. Perlindungan terhadap perangkat sistem audit (10.3.2).

Hasil akhir yang diperoleh adalah penjumlahan hasil dari kesepuluh clouse yaitu sebagai berikut.

Tabel 6.1 Hasil Akhir Perolehan

No	*Clouse*	*Nilai Total Clouse*
1	*Security policy* (Kebijakan keamanan)	0
2	*Organization security* (Pengelolaan kemaanan)	3
3	*Asset classification and control* (Klasifikasi dan pengendalian asset)	1
4	*Personal security* (Keamanan personil)	8
5	*Physical and environment security* (Keamanan fisik dan lingkungan)	10
6	*Communication and operation management* (Pengaturan komunikasi dan operasional)	13
7	*System access control* (Pengawasan terhadap akses)	23
8	*System development and maintenance* (Pengembangan dan perawatan system)	9
9	*Business continuity planning* (Pengelolaan kelangsungan bisnis)	3
10	*Compliance* (Pemenuhan/kelengkapan)	5
	Jumlah	***75***
	%	***59%***
	Kategori	***Kurang Aman***

6.4. Waktu Audit

Penelitian ini tidak dapat meneliti lebih jauh lagi kondisi keamanan informasi yang sebenarnya di Rumah Sakit "X" secara rinci per kontrol karena keterbatasan waktu dan izin yang diberikan. Hal ini dapat ditindaklanjuti oleh penelitian berikutnya untuk dapat meneliti secara lebih mendalam lagi.

6.5. Kesulitan Penggunaan Perangkat Lunak DSS

Kesulitan yang dijumpai oleh responden sebagai pengguna DSS ini dianggap sebagai kekurangan dari perangkat lunak ini. Kesulitan yang ditemui dari penggunaan perangkat lunak ini adalah sebagai berikut.

1. Harus dilakukan instalasi file *xampp-win32-1.6.3-installer* dan MyODBC-3.51.03. Instalasi file *xampp-win32-1.6.3-installer* ini

diperlukan sebagai *database*. Sedangkan MyODBC-3.51.03.exe untuk koneksi dari DSS ke *database*.

2. Perbaikan kesalahan tidak praktis

   Apabila terjadi kesalahan, untuk melakukan perbaikan tidak praktis karena tidak adanya fitur kembali ke awal atau "*back*" sehingga menyebabkan pengguna harus mengulang langkah dari awal lagi jika melakukan kesalahan. Proses pengerjaan yang mengulang ini menyebabkan waktu pengerjaan jadi lebih lama, adanya fitur yang memungkinkan untuk kembali ke langkah pengerjaan sebelumnya memudahkan pengguna untuk melakukan perbaikan pada setiap kesalahan yang dilakukan.

6.6. Kemudahan Penggunaan Perangkat Lunak DSS

Kemudahan yang dijumpai oleh para responden sebagai pengguna, dianggap sebagai kelebihan dari perangkat lunak ini. Kemudahan yang ditemui dari penggunaan perangkat lunak penghitung ini adalah sebagai berikut.

1. Hasil audit dapat diketahui secara otomatis

   Dalam perangkat lunak DSS audit ini responden atau pengguna tidak perlu menghitung atau memasukkan rumus perhitungan. Perangkat lunak akan melakukan perhitungan secara otomatis. Dengan adanya perhitungan otomatis ini diharapkan dapat mengurangi kesalahan perhitungan yang disebabkan oleh kesalahan rumus yang dimasukkan.

   Jika pengguna telah menguasai penggunaan perangkat lunak ini, diharapkan akan cepat diketahui kondisi keamanan rumah sistem informasi rumah sakit ini.

2. Tampilan lebih sederhana

   Audit menggunakan *kuesioner* prosesnya rumit karena menggunakan lembaran kertas yang banyak. Pada perangkat lunak DSS ini, pengisian data yang ditampilkan lebih sedikit dan tampilan menjadi lebih sederhana.

6.7. Validasi dan Verifikasi

Pada pembuatan perangkat lunak baru tidak terlepas dari validasi, yaitu apakah program yang dibuat sudah sesuai dengan yang diinginkan oleh pengguna. Dengan adanya validasi dapat ditentukan apakah perangkat lunak layak untuk digunakan atau tidak. Selain validasi, perangkat lunak juga harus diverifikasi, yaitu sudah dipastikan terbuat dengan spesifikasi yang jelas. Jika tidak mememenuhi validasi dan verifikasi, maka suatu perangkat lunak akan disempurnakan kembali sehingga sesuai dengan yang diinginkan oleh pengguna.[18]

Verifikasi perangkat lunak ini adalah apabila dijalankan pada sistem operasi setingkat Windows XP dengan dan telah terinstalasi file xampp-win32-1.6.3-installer dan MyODBC-3.51.03. Pada perangkat lunak DSS Audit ini pada prinsipnya mampu melakukan audit seperti yang diharapkan pada tujuan perancangannya, akan tetapi masih dijumpai *fault* dan terdapat fitur yang belum lengkap sehingga menimbulkan kesulitan bagi penggunanya, untuk itu perlu diperbaiki kembali *fault* yang ditemui dan fitur dilengkapi.

6.8. Usulan Perbaikan dan Penambahan Fitur

Selain perbaikan *fault* yang ada, agar perangkat lunak ini lebih mudah dijalankan oleh responden perlu dilakukannya perbaikan fitur. Perbaikan fitur ini tentunya merupakan hasil kesepakatan antara analis sistem (berdasarkan hasil uji coba pada responden), perancang program dan programmer yang membuat perangkat lunak tersebut.

Beberapa fitur yang perlu ditambahkan atau di perbaiki antara lain sebagai berikut.

1. Fitur *back* memudahkan pengguna untuk kembali ke langkah sebelumnya jika melakukan kesalahan, tanpa harus menyelesaikan seluruh perintah.

---

[18] Diakses dari http://www.ece.cmu.edu/~koopman/des_s99/verification/index.html (1 Mei 2009)

2. Perbaikan kesalahan yang lebih praktis, jika pengguna melakukan kesalahan input data, dapat dilakukan pada titik itu juga tanpa harus menyelesaikan terlebih dahulu, sehingga tidak perlu mengulang langkah pengerjaan.

6.9. Usulan Peningkatan Kualitas Sumber Daya Manusia

Perlunya memiliki konsultan/pakar ahli yang bertugas menangani perencanaan serta implementasi keamanan informasi sistem informasi rumah sakit. Hal yang dapat dilakukan adalah dengan menambah sumber daya manusia yang mempunyai keahlian tinggi dan spesifik di bidang ini atau menyewa jasa konsultan/pakar ahli dari luas khusus untuk menangani masalah ini.

6.10. Usulan Pengujian Kompatibilitas Dengan Sistem Operasi Lain

Windows merupakan sistem operasi berlisensi, untuk menghemat biaya dapat digunakan sistem operasi *open-source*. Beberapa komputer telah dilengkapi dengan sistem operasi sendiri yang juga tidak berbayar misal Linux. Agar dapat dipastikan apakah perangkat lunak ini dapat dijalankan pada berbagai sistem operasi, maka perlu dilakukan pengujian kembali di berbagai sistem operasi yang berbeda.

6.11. Usulan Test Ulang Setelah Perbaikan

Walaupun telah diperbaiki semua *fault* dan kekurangan fitur yang ada, tetap saja perangkat lunak ini harus diuji kembali penggunaannya. Hal ini untuk meyakinkan apakah perangkat lunak tersebut sudah sesuai dengan yang diinginkan. Jika waktu pengujian tidak terbatas, maka uji *non-functional* lainnya seperti *performance, security, availability, reliability,* dan *capacity* hendaknya dilakukan.

6.12.Pengembangan Aplikasi

a. Perangkat lunak DSS Audit Keamanan Sistem Informasi ini dapat dikembangkan dengan mengikuti perkembangan ISO tentang Audit Keamanan Sistem Informasi terbaru.

BAB 7
KESIMPULAN DAN SARAN

7.1. Kesimpulan

1. Kondisi keamanan sistem informasi Rumah Sakit "X" masuk dalam kategori **kurang aman**, berdasarkan hasil audit menggunakan DSS yang mengadaptasi 127 *controls security* dari ISO 17799.
2. DSS pada audit sistem informasi Rumah Sakit "X" ini terdiri dari 5 tahap yaitu masukan (127 pertanyaan yang harus dijawab ya atau tidak), proses (perhitungan jumlah jawaban ya dan tidak), informasi (nilai perolehan ya dan prosentase), analisis (tabel, grafik, trend), dan keluaran (kondisi tingkat keamanan sistem informasi, masalah dan solusi).
3. *Decision Support System* (DSS) yang telah dibuat ini sangat membantu dan mempermudah audit terhadap keamanan sistem informasi Rumah Sakit "X".

7.2. Saran

Saran dan rekomendasi yang diperoleh dari hasil penelitian ini untuk meningkatkan keamanan sistem informasi pada Sistem Informasi Rumah Sakit "X" agar menjadi lebih aman.

1. Mensosialisasikan pentingnya audit terhadap keamanan sistem informasi.
2. Mensosialisasikan penggunaan perangkat lunak DSS audit keamanan sistem informasi.
3. Meningkatkan kualitas sumber daya manusia dengan memberikan pelatihan, menambah tenaga ahli, atau mendatangkan konsultan.
4. Perlu dibentuk forum gabungan lintas unit independen yang khusus menangani dan mengawasi keamanan sistem informasi dari rumah sakit ini. Hal ini berdasarkan fakta yang diperoleh dalam penelitian bahwa baru divisi PDE yang peduli akan masalah keamanan informasi, sedangkan bagian yang lain cenderung tidak peduli karena menganggap

keamanan informasi menjadi tanggung jawab PDE semata. Padahal sistem informasi di rumah sakit ini akaan aman jika seluruh komponen yang terlibat dalam sistem informasi ikut berpartisipasi, termasuk operator dan regulator.

5. Perlu ditingkatkan lagi komunikasi antara pihak manajemen dan staf, baik staf IT maupun pengguna sistem informasi, terutama untuk membahas maupun mensosialisasikan isu-isu penting serta kebijakan-kebijakan di bidang keamanan informasi.
6. Dari hasil penelitian tampak bahwa masih kurang adanya komunikasi antara pihak manajemen dan staf rumah sakit, dilihat dari jawaban-jawaban kuesioner yang sangat jauh berbeda tentang pandangan atas kondisi keamanan sistem informasi rumah sakit ini.
7. Perlunya memiliki konsultan/pakar ahli untuk membantu menangani perencanaan serta implementasi keamanan informasi sistem informasi rumah sakit. Hal yang dapat dilakukan adalah dengan menambah sumber daya manusia yang mempunyai keahlian tinggi dan spesifik di bidang ini atau menyewa jasa konsultan/pakar ahli dari luas khusus untuk menangani masalah ini.
8. Perlu diimplementasikan teknologi terbaru seperti metode/algoritma enkripsi terbaru, serta penggunaan alat autentikasi lain seperti *smart card*, maupun alat identifikasi lain. Rekomendasi ini diberikan kerena hasil penelitian yang menunjukkan bahwa selama ini metode keamanan (misal enkripsi) yang digunakan masih belum merupakan metode yang terbaru. Penggunaan metode terbaru akan menekan resiko bocornya informasi pada pihak yang tidak berwenang.
9. Keamanan secara fisik perlu ditingkatkan karena sejauh ini cukup beresiko, dimana penghalang yang ada hanya berupa kunci biasa dan tidak diperlukan identifikasi tertentu untuk dapat masuk ke ruangan-ruangan khusus.

Daftar Pustaka

Boynton, William, C, Johnson, Raymond N, Kell, Walter G. (2003). *Modern Auditing 7th Edition*, Jakarta: Erlangga.

Burch, J; Grdnitski, G. (1989). *Information Systems Theory and Practice 5th Edition*. New York: John Wiley & Sons, Inc.

Champlain, Jakck J. (2003). *Auditing Information System.* New Jersey: John Wiley & Sons, Inc.

Dahblerg, T; Kivijarvi, H. (2006). *An Integrated Framework for IT Governance and the Development and Validation of an Assessment. IEEE : Proceeding f the 39th Hawaii International Conference on Systems Sciences.* Finland: Helsinki School of Economics.

Davis, Gordon B. (1984). "*Kerangka Dasar Sistem Informasi Manajemen*", *Bagian II, Struktur dan Pengembangan*, Jakarta: PT. Pustaka Binaman Pressindo.

Indrajit, Richardus E. (2004). *Kajian Strategis Cost Benefit Teknologi Informasi.* Yogyakarta: Andi Offset.

Jogiyanto. (1989). "*Analisis dan Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*", Penerbit Andi Offset, Yogyakarta.

Kristanto, Harianto. (1993). *"Konsep dan Perancangan Database*". Yogyakarta: Andi Offset.

Mahyuzir, Tavri D. (1999). *Analisis dan Perancangan Sistem Pengolah Data.* Jakarta: PT. Elexmedia Komputindo.

Ma'ruf, N. (2005). *Evaluasi Penerapan Sistem Informasi Akademik Jurusan Teknik Elektro Fakultas Teknik Universitas Gadjah Mada.* Yogyakarta: Universitas Gadjah Mada.

Moekijat. (1991). *Pengantar Sistem Informasi.* Bandung: PT. Remadja Rosda.

Peltier, Thomas R. (2002). *ISO 17799 Self Assessment Checklist.* http://www.occure.org/. Diakses tanggal 20 Mei 2009.

Rahardjo, B. (1999). *Keamanan dalam Electronic Commerce, Paper yang dipresentasikan pada Seminar*. Jakarta: Infokomputer.

Sabarguna, B.S., (2001). *Sistem Inforamsi Pemasaran Rumah Sakit Berbasis Rekam Medis.* Yogyakarta: Gama Press.

Siagian, Sondang, P. (1979) *Sistem Informasi untuk Pengambilan Keputusan.* Jakarta: PT. Gunung Agung.

Tugiman, H. (1996). *Pengantar Audit Sistem Informasi*. Yogyakarta: Kanisius.

Turban, E, at all. (2008). *E-Commerce 2008.* New Jersey: Pearson International.

Weber, R. (1999). *Information Systems Control and Audit.* New Jersey : Prentice Hall.

Lampiran 1. Kuesioner Penelitian

KUISIONER PENELITIAN DECISION SUPPORT SYSTEM PADA AUDIT KEAMANAN SISTEM INFORMASI RUMAH SAKIT MH THAMRIN INTERNASIONAL SALEMBA TAHUN 2009

Kuesioner ini dibuat dalam rangka penelitian untuk mengidentifikasi kondisi keamanan informasi pada sistem informasi Rumah Sakit MH Thamrin Internasional Salemba, sesuai dengan persyaratan standart keamanan dari ISO 17799:2000 *Information Technology – Code of Practice for Information Security Management.*

Penulis memohon kesediaan Bapak/Ibu/Saudara untuk mengisi kuesioner ini sesuai dengan kondisi yang sebenarnya di Rumah Sakit MH Thamrin Internasional Salemba menurut anda pribadi. Hasil dari pengisian kuesioner ini hanya akan digunakan sebatas kebutuhan penelitian dan penulisan thesis untuk memenuhi syarat Magister Sains.

Setiap jawaban yang diberikan merupakan bantuan yang tak ternilai harganya bagi penelitian ini. Atas kesediaan Bapak/Ibu/Saudara, penulis mengucapkan banyak terima kasih.

A. DATA RESPONDEN

1. Nama : _____
2. Jenis Kelamin : Laki-Laki / Perempuan *)
3. Pendidikan Terakhir : SMP / SMA / D3 / S1 / S2 / S3 *)
4. Jurusan : _____
5. Pekerjaan/Jabatan : _____
6. Divisi/Bagian : _____

B. PETUNJUK PENGISIAN KUISIONER

Berikut ini adalah pertanyaan-pertanyaan mengenai kondisi keamanan informasi pada system informasi Rumah Sakit. MH Thamrin Internasional Salemba. Berilah tanda (✓) pada kolom jawaban yang tersedia, bagian "Y" (untuk jawaban **Ya**) dan "T" (untuk jawaban **Tidak**). Jika diperlukan, tambahkan komentar/catatan pada kolom yang tersedia.

Peneliti,

Sumaryanto

1. Kebijakan Keamanan (*Security Policy*)				
1.1. Kebijakan keamanan informasi		Manajemen harus mengarahkan dan mendukung kebijakan keamanan informasi.		
1.1.	Dokumen kebijakan keamanan informasi	Apakah ada aturan/kebijakan tentang keamanan informasi ?	Y T	
1.2.	Publikasi dokumen kebijakan keamanan informasi.	Apakah aturan kebijakan tentang keamanan informasi telah disebarluaskan ?	Y T	

Keterangan :
Dokumen kebijakan informasi adalah dokumen yang berisi kebijakan-kebijakan perusahaan (Rumah Sakit) tentang keamanan informasi, seperti Standart Operasional Prosedur (SOP), kondisi-kondisi yang boleh dilakukan maupun tidak boleh oleh personil/staf Rumah Sakit, yang terkait dengan keamanan data/ informasi.

2. Pengelolaan Keamanan (*Organizational Security)*				
2.1. Infrastruktur kemanan informasi		Kerangka kerja manajerial harus dibangun untuk memulai dan mengendalikan penerapan keamanan informasi dalam organisasi.		
2.1.1.	Forum manajemen keamanan informasi	Adakah forum untuk mengawasi dan mewakili keamanan informasi ?	Y T	
2.1.2.	Koordinasi tentang keamanan informasi	Adakah forum lintas instansi/unit untuk koordinasi penerapan pengukuran keamanan informasi ?	Y T	
2.1.3.	Alokasi tanggung jawab keamanan informasi	Apakah tanggung jawab untuk pencapaian keamanan informasi didefinisikan dengan jelas?	Y T	
2.1.4.	Proses autorisasi untuk fasilitas pengolahan informasi	Apakah ada proses pengesahan dari manajemen untuk tiap fasilitas pemrosesan informasi baru (hardware dan software) dilihat baik dari segi bisnis maupun teknis ?	Y T	
2.1.5.	Arahan tentang topik khusus pada keamanan informasi	Apakah nasehat tentang suatu topik khusus dalam keamanan informasi dapat diperoleh organisasi sewaktu-waktu ? (misal : melalui tenaga konsultan IT, pakar dll)?	Y T	
2.1.6.	Kerjasama antar lembaga	Apakah komunikasi antar lembaga (ter-masuk spesialisasi keamanan baik industri maupun pemerintah, aparat penegak hukum, penyedia layanan IT, serta penyedia telekomuni-kasi) dijaga	Y T	

		dengan baik agar dapat dilakukan tindakan tepat dan cepat dalam *kaitan dengan* keamanan informasi ?		
2.1.7.	Penilaian independent tentang keamanan informasi	Apakah kajian independen tentang praktek keamanan informasi sudah dijalankan untuk menjamin keberlaku-an, keefektifan serta kesesuaian dengan kebijakan tertulis ?	Y __ T __	
2.2. Keamanan terhadap akses dari pihak luar		Fasilitas IT milik organisasi dan aset informasi lain yang mengendalikan akses dari pihak luar harus dijaga supaya aman dari pihak luar.		
2.2.1.	Mengidentifikasi resiko yang mungkin ditimbul-kan oleh akses *dari pihak* luar	Apakah koneksi ke pihak luar sudah dianalisis ?	Y __ T __	
	Mengatasi resiko yang muncul dari konektivitas dengan pihak luar	Apakah spesifikasi/standart keamanan khusus sudah diidentifikasi untuk menangkal resiko keamanan dari pihak luar ?	Y __ T __	
2.2.2.	Kondisi-kondisi keamanan yang tertera pada kontrak dengan pihak luar	Apakah persyaratan keamanan dima-sukkan dalam kontrak formal dengan pihak ketiga ? (Vendor, konsultan developer dll)	Y __ T __	
2.3. Outsourcing		Keamanan informasi harus dijaga bahkan saat tanggung jawab untuk keamanan sudah dialihkan (outsourced) ke pihak lain.		
2.3.1.	Spesifikasi tentang keamanan pada kontrak outsorcing	Apakah syarat kemanan dari pemilik informasi sudah dijelaskan dalam kontrak antara pemilik dan organisasi luar yang menangani ?	Y __ T __	

3. Klasifikasi dan Pengendalian Aset (Asset Clasification and Control				
3.1. Pencatatan Aset		Pencatatan terhadap aset organisasi harus dijalankan.		
3.1.1.	Inventarisasi Aset	Adakah *inventarisasi*/pencatatan asset-aset utama yang terhubung dengan masing-masing sistem informasi ?	Y T	
3.2. Pengklasifikasian Informasi		Klasifikasi keamanan harus digunakan untuk mengindikasikan kebutuhan dan prioritas kebutuhan terhadap perlindungan untuk informasi.		
3.2.1.	Petunjuk klasifikasi	Apakah panduan klasifikasi keamanan sudah dibuat untuk mengindikasikan kebutuhan dan prioritas kebutuhan untuk proteksi keamanan ?	Y T	
3.2.2.	Penamaan (labeling) dan penanganan (handling) informasi	Apakah proses untuk memberi label terhadap informasi yang membutuhkan proteksi kemanan sudah diimplemen-tasikan ?	Y T	

4. Keamanan Personil (Personel Security)				
4.1. Tanggung jawab keamanan staf		Keamanan harus dijalankan pada tahap perekrutan, dimasukkan dalam deskripsi pekerjaan dan kontrak serta di monitor selama proses kerja seseorang.		
4.1.1.	Pendefinisian keamanan pada deskripsi pekerjaan *(job description)*	Apakah tanggung jawab kemanan dimasukkan dalam deskripsi pekerjaan karyawan ?	Y T	
4.1.2.	Kebijakan penyeleksi staf	Apakah seleksi khusus terhadap aplikasi karyawan dilakukan untuk pekerjaan yang membutuhkan akses informasi sensitif ?	Y T	
4.1.3.	Perjanjian kerahasiaan	Apakah karyawan diminta untuk menandatangani perjanjian untuk tidak mengungkapkan kerahasiaan *(non disclosure agreements)* sebagai bagian dari syarat dan kondisi pekerjaan ?	Y T	
4.1.4.	Syarat dan kondisi yang berlaku (*terms and conditions of employment*)	Apakah dalam kontrak kerja/*term and conditions* karyawan dicakup tanggung jawab karyawan terhadap keamanan informasi, termasuk jangka waktu setelah kontrak dan konsekuensi bila terjadi pelanggaran ?	Y T	
4.2. *Pelatihan Pengguna*		Pengguna harus diberi pelatihan terhadap prosedur keamanan dan penggunaan fasilitas IT yang baik.		
4.2.1.	Pelatihan dan pendidikan tentang keamanan informasi	Sebelum mendapatka akses ke fasilitas IT, apakah pengguna diberi pelatihan terhadap kebijakan dan prosedur keamanan informasi, persyaratan keamanan, kendali bisnis dan penggunaan fasilitas IT yang benar?	Y T	
4.3. *Respon/penanganan terhadap insiden rusak atau tidak ber-fungsinya keamanan*		Insiden yang berhubungan dengan keamanan harus dilaporkan melalui saluran komunikasi manajemen secepat mungkin.		

4.3.1.	Pelaporan atas insiden keamanan	Apakah prosedur formal untuk melaporkan kejadian/kecelakaan terkait *keamanan informasi* melalui jalur manajemen secepat mungkin?	Y T	
4.3.2.	Pelaporan akan ketidak-amanan/kelemahan keamanan	Apakah pengguna diharuskan untuk mencatat dan melaporkan tentang sesuatu yang dicurigai sebagai kelemahan dalam sistem keamanan atau ancaman terhadap sistem informasi ?	Y T	
4.3.3.	Pelaporan akan ketidak-berfungsian software	Adakah prosedur untuk melaporkan adanya software yang tidak berfungsi dengan benar ?	Y T	
4.3.4.	Belajar dari kegagalan	Adakah mekanisme untuk mengawasi dan mengetahuii tipe, jumlah *dan biaya dari* insiden/kegagalan keamanan informasi ?	Y T	
4.3.5.	Proses pendisplinan	Adakah proses formal untuk menangani karyawan yang melanggar prosedur dan kebijakan keamanan informasi ?	Y T	

5. Keamanan Fisik dan Lingkungan (Physical and Environmental Security)				
5.1. Area aman		Fasilitas IT untuk mendukung aktivitas bisnis penting dan sensitif harus terletak di daerah aman.		
5.1.1.	Parameter keamanan fisik	Adakah proteksi keamanan fisik untuk melindungi layanan pemrosesan informasi, berbasiskan parameter khusus dan hambatan yang diletakkan secara strategis tersedia di seluruh organisasi (misal : gerbang/pintu masuk yang memerlukan kartu identitas untuk masuk, aset yang dikelilingi tembok, penjagaan oleh satpam, dll).	Y T	
5.1.2.	Pengawasan akses masuk	Apakah tersedia sistem di daerah khusus (*secure area*) untuk menjamin hanya personel yang berwenang yang bisa mendapat akses ?	Y T	
5.1.3.	Pengamanan bangunan, kantor, ruangan dan fasilitas	Apakah ruangan/bangunan yang menyediakan layanan pemrosesan informasi telah dilindungi secara fisik (adanya kunci dll), serta dari kemungkinan adanya ancaman dari luar maupun bencana alam ?	Y T	
5.1.4.	Bekerja pada area aman	Adakah kendali tambahan (misal kartu identitas dll) untuk personel dan pihak luar yang bekerja di daerah khusus ?	Y T	
5.1.5.	Isolasi area pengiriman dan pengisian data	Apakah ruang pengisian dan pengiriman ke komputer pusat/pusat data terisolasi dan dapat mencegah akses dari pihak yang tidak berwenang?	Y T	

5.2. Kelengkapan keamanan		Peralatan harus dilindungi secara fisik dari ancaman keamanan dan bahaya lingkungan.		
5.2.1.	Perlindungan dan peletakan peralatan/ perlengkapan	Apakah peralatan *diletakkan untuk* mengurangi resiko bahaya lingkungan dan akses dari pihak yang tidak berwenang?	Y T	
5.2.2.	Sumber daya/power supplies	Apakah peralatan elektronik dilindungi dari kemungkinan kegagalan sumber listrik atau *anomaly* listrik lain ?	Y T	
5.2.3.	Keamanan kabel	Apakah kabel daya dan telekomunikasi dilindungi dari penyadapan/kerusakan ?	Y T	
5.2.4.	Perawatan perlengkapan	Apakah prosedur sudah dibentuk untuk menjaga kelangsungan ketersediaan dan *kelangsungan integrasi* peralatan TI (misal merawat sessuai spesifikasi dari supplier dan dalam interval waktu yang rutin)	Y T	
5.2.5.	Keamanan peralatan di luar kantor	Apakah peralatan yang digunakan di luar kantor (*off site*), tanpa memandang kepemilikan mempunyai derajat perlindungan serperti peralatan IT di dalam kantor (*on-site*) ?	Y T	
5.3. Pengawasan umum		Fasiltias informasi dan pemrosesan informasi harus dilindungi dari kemungkinan pembeberan, modifikasi dan pencurian dari pihak yang tidak berwenang dan kendali harus diberikan untuk meminimalkan kerusakan.		
5.3.1.	Kebijakan akan layar/ meja yang bersih	Apakah kebijakan layar bersih/meja bersih untuk bahan-bahan sensitif sudah diterapkan untuk mengurangi resiko akses dari pihak yang tidak	Y T	

		berwenang, kehilangan atau kerusakan di luar jam kerja biasa ?		
5.3.2.	Pemindahan properti	Apakah personel diharuskan untuk menjalankann dokumentasi tentang wewenang saat membawa peralatan dan data ke luar kantor utama (off site)?	Y T	

6. Pengaturan Komunikasi dan Operasional (Communication and Operations Management)				
6.1. Tanggung jawab dan prosedur operasional		Tanggung jawab dan prosedur harus dibangun untuk manajemen dan pengoperasian seluruh komputer dan jaringan.		
6.1.1.	Dokumentasi prosedur operasional	Apakah prosedur operasional sudah terdokumentasi sepenuhnya pada semua sistem komputer untuk meyakinkan bahwa mereka menjalan-kan operasi yang tepat dan aman ?	Y T	
6.1.2.	Pengawasan atas perubahan pada kegiatan operasional	Adakah proses untuk mengendalikan perubahan yang terjadi di fasilitas dan sistem TI untuk semua perubahan pada peralatan, software atau prosedur ? (Misal *tiap perubahan harus* melalui proses autorisasi dll)	Y T	
6.1.3	Pengaturan prosedur atas insiden keamanan	Apakah tanggung jawab manajemen insiden dan prosedur sudah diterapkan untuk menjamin adanya penanggulang-an yang cepat dan efektif terhadap insiden keamanan ?	Y T	
6.1.4.	Pemisahan tugas	Apakah tugas sensitif atau area pertanggungjawaban dipisahkan untuk mengurangi kemungkinan modifikasi *dari pihak yang tidak* berwenang atau penyalahgunaan data dan servis ?	Y T	
6.1.5.	Pemisahan fasilitas pengembangan dan operasional	Apakah fasilitas operasional dan pe-ngembangan dipisah	Y T	

		untuk mengurangi resiko perubahan yang tidak sengaja/ akses pihak *tidak berwenang* ke software operasional dan data bisnis ?	__	
6.2. Perencanaan dan penerimaan sistem		Tanggung jawab dan prosedur harus dibangun untuk manajemen dan pengoperasian seluruh komputer dan jaringan.		
6.2.1.	Perencanaan kapasitas	Apakah kapasitas kebutuhan diawasi dan kebutuhan masa depan diproyeksi untuk mengurangi resiko *system overload* ?	Y __ T __	
6.2.2.	Penerimaan akan sistem baru	Apakah persyaratan penerimaan (*acceptance criteria*) untuk sistem baru sudah dibangun, dan tes dilaksanakan ke sistem setelah tahap *penerimaan* ? (*Sistem* baru meliputi sistem informasi yang benar-benar baru, versi baru dari sistem yang sekarang atau di-upgrade)	Y __ T __	
6.3. Perlindungan terhadap software yang berbahaya		Mengaplikasikan sistem peringatan untuk mencegah dan mendeteksi penggunaan software berbahaya dapat menjaga integritas software dan data.		
6.3.1	Pengawasan terhadap software berbahaya	Apakah alat pendeteksi dan pencegah virus serta prosedur pengawasan pengguna sudah diimplementasikan ?	Y __ T __	
6.4. Housekeeping		Prosedur rutin untuk membuat salinan back-up data, catatan kejadian (*event logging*) dan kesalahan, dan bila dibutuhkan pengawasan terhadap lingkungan peralatan.		
6.4.1	*Back-up*/menyalin cadangan informasi	Apakah proses untuk membuat salinan back-up data bisnis penting dan software untuk menjamin bahwa data itu bisa	Y __ T __	

		diambil setelah bencana komputer atau kegagalan media sudah dibuat ?		
6.4.2.	Catatan kegiatan operasional	Apakah penggunaan computer harus membuat catatan tentang semua pekerjaan yang dijalankan ? (Misal tediri dari nama user, error yang terjadi, langkah pengoreksian dst).	Y T	
6.4.3.	Pencatatan kesalahan	Adakah prosedur untuk mencatat kesalahan yang dilakukan oleh user berkaitan dengan masalah pada komputer atau sistem komunikasi ?	Y T	
6.5. Manajemen jaringan		Keamanan jaringan komputer yang mencakup batas organisasi harus diatur untuk menjaga informasi dan melindungi infrastruktur pendukung.		
6.5.1	Pengawasan jaringan/ *network*.	Apakah kendali yang cukup untuk menjamin keamanan data di jaringan dan proteksi terhadap servis yang berhubung ke luar dari akses pihak yang tidak berwenang ?	Y T	
6.6. Keamanan dan penanganan media		Media menyimpan komputer harus diawasi dan secara fisik dilindungi untuk mencegah kerusakan aset serta gangguan akan aktivitas bisnis.		
6.6.1	Pengelolaan pemindahan media computer	Apakah ada prosedur untuk mengelola pemindahan media (penyimpanan) komputer seperti tape, disket, kaset, maupun laporan yang telah dicetak (*printed report*) ?	Y T	
6.6.2.	Pembuangan media	Adakah proses untuk memastikan bahwa media komputer (seperti contoh di atas) dibuang dengan aman ketika sudah tidak dibutuhkan ?	Y T	

6.6.3.	Prosedur penangan informasi	Apakah ada prosedur untuk menangani penyimpanan data-data *penting/sensitif* untuk melindungi data tersebut dari kemungkinan salah penggunaan maupun pemilikan data oleh pihak yang tidak berwenang ?	Y T	
6.6.4.	Keamanan dokumentasi sistem	Apakah dokumentasi dari sistem telah dilindungi dari kemungkinan akses oleh pihak yang tidak berwenang ?	Y T	
6.7. Pertukaran software dan informasi		Pertukaran data dan software antar lembaga harus diawasi untuk mencegah kehilangan, modifikasi atau salah penggunaan atas data.		
6.7.1	Perjanjian pertukaran software dan informasi	Apakah ada perjanjian formal, untuk mengatur pertukaran data dan *software antar lembaga* baik secara manual maupun elektronis ? (Misal hubungan RS Intl. Thamrin dengan Bank, Supplier, dll).	Y T	
6.7.2.	Keamanan media dalam proses transit	Apakah ada pengawasan untuk melindungi media (penyimpanan) seperti disket, laporan tercetak (*printed report*) dll, ketika dipindahkan antar area untuk meminimalkan akses dari pihak yang tidak berwenang, salah penggunaan atau pengurangan ?	Y T	
6.7.3.	Keamanan E-commerce	Apakah telah ada pengawasan untuk mengurangi resiko keamanan dan bisnis sehubungan dengan pemakaian e-commerce ?	Y T	
6.7.4.	Keamanan e-mail	Apakah telah ada	Y	

		pengawasan untuk mengurangi resiko keamanan dan bisnis sehubungan dengan pemakaian surat elektronik (*e-mail*) dari intersepsi, modifikasi serta error ?	T	
6.7.5.	Keamanan sistem kantor elektronis (*e-office*)	Apakah telah ada kebijakan dan petunjuk yang jelas untuk mengawasi resiko keamanan dan binis pada sistem kantor elektronis ? (kantor yang sudah menggunakan komputer/otomatis, tidak lagi manual menggunakan tangan, mesin ketik/dll dalam aktivitasnya).	Y T	
6.7.6.	Sistem pengadaan publisitas	Apakah ada proses autorisasi formal sebelum informasi dipublikasikan untuk umum ? (Misal memastikan server/computer yang digunakan untuk mengakses informasi oleh umum telah aman, adanya firewall dll).	Y T	
6.7.7.	Pertukaran informasi lain	Apakah ada pengawasan dan prosedur untuk melindungi pertukaran informasi lewat suara (seperti telepon), faximile maupun fasilitas komunikasi lewat video.	Y T	

7. Pengawasan Terhadap Akses (Access Control)				
7.1. Kebutuhan bisnis pada sistem pengaksesan		Kebijakan akan pengadaan dan penyertaan informasi harus ada untuk pengawasan atas akses pada layanan komputer dan data sesuai dengan kebutuhan bisnis.		
7.1.1.	Kebijakan pengawasan terhadap akses	Apakah kebutuhan bisnis telah didefinisikan dan didokumentasikan untuk mengatur hak akses ?	Y / T	
7.2. Pengaturan akses oleh pengguna		Prosedur formal diperlukan untuk mengontrol hak akses atas layanan TI.		
7.2.1.	Pendaftaran pengguna	Apakah ada pendaftaran penggunaan/ user secara formal (dan sebaliknya, penghapusan penggunaan/user) untuk dapat mengakses berbagai layanan TI ?	Y / T	
7.2.2.	Pengaturan kewenangan	Apakah ada pembatasan dan pengawasan atas pengguna/user yang dapat menggunakan berbagai fasilitas TI agar tidak merusak sistem maupun aplikasi ?	Y / T	
7.2.3.	Pengaturan password pengguna	Apakah telah ada proses pengelolaan password untuk mengontrol/menangani password ?	Y / T	
7.2.4.	Peninjauan kembali (*review*) atas hak akses pengguna	Apakah secara periodik dilakukan peninjauan kembali/review atas hak akses pengguna/user ?	Y / T	
7.3. Tanggung jawab pengguna		Pengguna harus tahu tanggung jawab mereka untuk tujuan efektivitas kontrol atas akses, terutama akan penggunaan password dan keamanan peralatan/perlengkapan yang digunakan pengguna/user.		
7.3.1.	Penggunaan password	Apakah pengguna/user telah diberi tahu tentang cara pemilihan password yang aman ?	Y / T	
7.3.2.	Peralatan yang tidak digunakan	Apakah semua pengguna dan kontraktor telah diberi tahu tentang pentingnya kebutuhan keamanan dan	Y / T	

		juga prosedur untuk melindungi peralatan yang tidak digunakan ? (misal *logoff* ketika komputer tidak digunakan lagi, dll).		
		Apakah semua pengguna dan kontraktor telah diberi tahu tentang tanggung jawab masing-masing untuk melindungi peralatan walau tidak digunakan ?	Y T	
7.4. Pengawasan akses pada jaringan (*network acess control*)		Koneksi ke layanan jaringan harus diwasi untuk memastikan bahwa sebuah layanan yang terkoneksi tidak berkompromi dengan keamanan sistem yang lain..		
7.4.1.	Kebijakan tentang penggunaan layanan jaringan (*network services*)	Apakah ada proses untuk memastikan bahwa jaringan dan layanan computer (*service*/aplikasi) yang dapat diakses penggunna atau dari tempat/klien komputer tertentu konsisten dengan kebijakan kontrol akses ?	Y T	
7.4.2.	Arah/path yang diamankan	Apakah ada kontrol yang membatasi rute mana saja yang boleh diakses oleh pengguna yang terautorisasi ketika terminal/komputer pengguna terhubung dengan komputer server ?	Y T	
7.4.3.	Autentikasi pengguna untuk konektivitas keluar	Apakah koneksi oleh pengguna jarak jauh melalui jaringan publik atau diluar LAN perusahaan diautentikasi, demi menghalangi akses pihak yang tidak berwenang dari mengakses aplikasi bisnis ?	Y T	
7.4.4.	Autentikasi titik/*node*	Apakah koneksi jarak jauh oleh sebuah sistem komputer diautentikasi terlebih dahulu untuk mencegah akses dari pihak yang tidak berwenang.	Y T	
7.4.5.	Perlindungan terhadap	Apakah ada proses yang		

	port yang didiagnosis digunakan untuk jarak jauh (remote)	dilakukan oleh teknisi (*maintenance engineer*) untuk mengontrol akses terhadap port yang didesain untuk diakses dari jarak jauh ?	Y T	
7.4.6.	Pembagian jaringan/ network	Apakah jaringan yang besar telah dibagi/pisahkan menjadi beberapa bagian yang lebih kecil untuk mengurangi resiko penggunaan sistem komputasi di jaringan oleh pihak yang tidak berwenang ?	Y T	
7.4.7.	Pengawasan konektivitas jaringan / network	Apakah telah ada kontrol untuk membatasi kemampuan koneksi pengguna demi mendukung kebijakan akses yang disesuaikan *dengan batasan/peraturan* perusahaan ?	Y T	
7.4.8.	Kontrol terhadap routing jaringan/network	Apakah *control routing* pada jaringan yang digunakan bersama telah sesuai dengan peraturan perusahaan untuk memastikan bahwa konektivitas komputer dan aliran informasi sesuai dengan kebijakan akses dari masing-masing unit bisnis ?	Y T	
7.4.9.	Keamanan layanan jaringan	Apakah penyedia jaringan telah secara jelas mendeskripsikan semua layanan yang digunakan, dan memberlakukan *keamanan demi* kerahasiaan, integritas dan ketersediaan aplikasi bisnis ?	Y T	
7.5. Kontrol terhadap akses pada sistem operasi		Akses ke computer seharusnya secara tegas dibatasi dengan cara memberlakukan : - identifikasi terminal secara otomatis;		

		- prosedur masuk/*logon* terminal; - identitas pengguna *user-id/user name*; - pengelolaan *password*; - alarm - batasan waktu terminal; dan - waktu koneksi yang dibatasi.		
7.5.1.	Identifikasi terminal secara otomatis	Apakah identifikasi terminal secara otomatis dapat sekaligus mengauten-tikasi koneksi dari lokasi tertentu ?	Y T	
7.5.2.	Prosedur logon terminal	Apakah telah didesain prosedur untuk masuk (logging) ke suatu sistem komputer untuk meminimalisir kemungkinan pengaksesan oleh pihak yang tidak berwenang ?	Y T	
7.5.3.	Identifikasi dan autentikasi user	Apakah semua user punya identitas yang unik (*user-id/username*) untuk masing-masing individu sehingga aktivitas yang terjadi dapat dilacak pada mereka ?	Y T	
7.5.4.	Sistem manajemen password	Apakah telah ada system manajemen password yang efektif untuk mengautentikasi user ?	Y T	
7.5.5.	Penggunaan utilitas sistem	Apakah program utilitas sistem yang dapat digunakan untuk merusak/ mengganti/mengganggu sistem serta kontrol terhadap aplikasi yang telah ada secara ketat diawasi penggunaannya ?	Y T	
7.5.6.	Alarm untuk melindungi user	Berdasar atas perkiraan resiko, apakah ada alarm, tanda bahaya disediakan untuk melindungi/memberi tahu user yang mungkin menjadi target usaha	Y T	

		paksa pengaksesan oleh pihak yang tidak berwenang ?		
		Adakah tanggung jawab yang didefinisikan untuk merespon adanya alarm/tanda bahaya ?	Y T	
7.5.7.	Waktu batas akses terminal	Apakah terminal yang berada di lokasi yang beresiko tinggi diset untuk *time-out*/waktu habis ketika terminal tidak aktif untuk menghindari akses oleh orang yang tidak berwenang ?	Y T	
7.5.8.	Pembatasan waktu koneksi	Apakah yang telah diset batasan periode waktu untuk terminal yang kemungkinan terkoneksi ke aplikasi yang *penting/sensitif* ?	Y T	
7.6. Kontrol terhadap akses ke aplikasi		Kontrol terhadap logik akses seharusnya dibuat untuk melindungi sistem aplikasi dan data dari akses oleh yang tidak berwenang.		
7.6.1.	Pembatasan akses terhadap suatu informasi	Apakah akses ke data dan fungsi dari aplikasi sistem dibatasi sesuai dengan kebijakan akses yang ada serta berdasar kebutuhan individu ?	Y T	
7.6.2.	Pengisolasian sistem yang sensitif	Menurut resiko yang telah diiden-tifikasi, apakah aplikasi sistem sensitif berjalan dilingkungan terisolasi?	Y T	
7.7. Pengawasan akses dan penggunaan system		Sistem harus dimonitor untuk menjamin kesesuaian dengan standar dan kebijakan akses, untuk mendeteksi aktivitas yang tidak berhak, dan untuk mengetahui tingkat efektivitas keamanan yang diberlakukan.		
7.7.1.	Kebijakan pengawasan terhadap akses	Apakah laporan audit yang menyimpan catatan kesalahan dan kejadian lain yang terkait dengan keamanan telah dibuat	Y T	

		dan dijaga untuk membantu investigasi masa yang akan datang serta *memonitor control* akses ?		
7.7.2.	Memonitor penggunaan sistem	Apakah telah ada prosedur untuk memonitor sistem demi menjamin user hanya melakukan pemrosesan/aktivitas yang dibolehkan saja ?	Y T	
7.7.3.	Penyesuaian waktu	Untuk menjamin keakuratan catatan audit, apa computer/device komunikasi lain diset waktunya menurut sebuah standart ? (Misal GMT, WIB, dll).	Y T	
7.8. Komputasi bergerak/mobile dan pengerjaan *jarak jauh*		Ketika menggunakan komputasi mobil dan pengerajaan jarak jauh, perusahaan harus *menilai resiko membuat perlindungan yang* memadai akan peralatan / tempat yang ada.		
7.8.1.	Komputasi mobile	Apakah telah ada kebijakan formal yang menyangkut resiko pengerjaan dengan fasilitas komputasi mobile (misal laptop), termasuk kebutuhan untuk perlindungan secara fisik, juga kontrol akan akses, teknik kriptografi, penyalinan/back up, dan perlindungan terhadap virus ?	Y T	

8. Pengembangan dan Perawatan Sistem (Systems Development and Maintenance)				
8.1. *Kebutuhan keamanan sistem*		Untuk menjamin keamanan diterapkan pada sistem TI, kebutuhan keamanan harus diidentifikasi, dijustifikasi, disetujui dan didokumentasi sebagai bagian tahap definisi kebutuhan (*requirements definitions stage)* seperti pada layaknya semua proyek pengembangan sistem TI.		
8.1.1.	Spesifikasi dan analisa kebutuhan keamanan	Apakah analisis kebutuhan keamanan adalah bagian dari tahap analisa kebutuhan dari setiap proyek pengembangan ?	Y T	
8.2. Keamanan aplikasi sistem		Kontrol keamanan yang sesuai dengan standar industri penerapan keamanan seharusnya didesain di sistem aplikasi untuk mencegah hilang, modifikasi atau salah penggunaan data pengguna		
8.2.1.	Validasi masukan data/ input	Apakah data yang *dimasukkan ke apli*-kasi sistem divalidasi untuk menjamin data tersebut benar dan cocok ?	Y T	
8.2.2.	Kontrol atas pemrosesan internal	Apakah sistem mempunyai kemam-puan cek validasi untuk mendeteksi kesalahan yang disebabkan oleh kesalahan yang disengaja maupun tidak disengaja ?	Y T	
8.2.3.	Autentikasi pesan	Apakah autentikasi pesan telah disertakan pada aplikasi yang terkait dengan *pengiriman data* penting/ sensitif ?	Y T	
8.2.4.	Validasi data keluaran/ output	Apakah data yang berupa keluaran dari aplikasi sistem divalidasi untuk menjamin data	Y T	

		tersebut benar dan cocok ?		
8.3. Kriptografi		Untuk melindungi kerahasiaan, keautentikan, atau integritas dari informasi, sistem dan teknik kriptografi harus digunakan sebagai perlindungan menyeluruh dari informasi yang dipandang beresiko.		
8.3.1.	Kebijakan tentang penggunaan kriptografi	Apakah manajemen telah membuat kebijakan, kontrol atas kriptografi, termasuk pengelolaan kunci yang terenkripsi dan pengimplementasian yang efektif ?	Y T	
8.3.2.	Enkripsi	Apakah enkripsi data dengan metode/ algoritma terbaru digunakan untuk melindungi data yang sensitif dalam proses *transmisi atau dalam* penyimpanannya ?	Y T	
8.3.3.	Digital signatures	Apakah digital signatures dengan metode/algoritma terbaru digunakan untuk melindungi autentikasi dan integrasi dari suatu dokumen elektronis ?	Y T	
8.3.4.	Non-repudiations services	Apakah anti penolakan/*non repudiation services* digunakan ketika ketidakcocokan dapat terjadi dalam penggunaan enkripsi atau digital signatures ?	Y T	
8.3.5.	Key management	Apakah ada sebuah sistem yang membantu perusahaan mengelola penggunaan teknik kriptografi, termasuk	Y T	

		teknik *secret key* dan public key ?		
8.4. Keamanan file sistem		Untuk memastikan proyek TI dan aktivitas pendukung dijalankan dengan benar, tanggung jawab untuk pengawasan akses ke file sistem dari suatu aplikasi harus diadakan denga kepemilikan *user function* atau *development group*.		
8.4.1.	Kontrol atas software operasional	Apakah ada pengawasan ketat atas implementasi software pada sistem oprasional ?	Y T	
8.4.2.	Perlindungan terhadap data tes sistem	Apakah data tes sistem aplikasi dilindungi dan diawasi ?	Y T	
8.4.3.	Kontrol akses atas library dari source program	Untuk mengurangi potensi kesalahan program komputer, apakah akses ke *library source program* diawasi ?	Y T	
8.5. Keamanan pada lingkungan pengembangan dukungan		Lingkungan proyek dan pengembangan harus dikontrol secara ketat untuk menjaga keamanan dari software dan data dari aplikasi sistem.		
8.5.1.		Prosedur kontrol terhadap perubahan pada sistem operasi		
8.5.2.	Review teknis terhadap perubahan sistem operasi	Apakah prosedur pengawasan perubahan telah diimplementasikan ?	Y T	
8.5.3.	Pembatasan terhadap perubahan pada paket software	Apakah dilakukan review terhadap aplikasi ketika perubahan pada sistem operasi terjadi ?	Y T	
8.5.4.	Chanel tersembunyi dan kode Trojan	Apakah modifikasi terhadap software buatan vendor tidak direkomendasikan, dan semisal memang diperlukan perubahan, apakah diawasi dengan ketat ?	Y T	
8.5.5.	Pengembangan	Untuk menghindari	Y	

	software yang di-*outsourcing*	adanya chanel tersembunyi maupun kode trojan, apakah perusahaan : - Membeli program software hanya dari pihak yang terpercaya; - Membeli program/software dalam *source code* yang terverifikasi; - Hanya menggunakan produk yang telah dievaluasi/uji; - Menginspeksi semua source code sebelum digunakan dalam kegiatan operasional; - Mengontrol akses dan modifikasi ke kode yang telah terinstall; - Mempekerjakan staf yang dipercaya untuk menangani *key system*.	T	

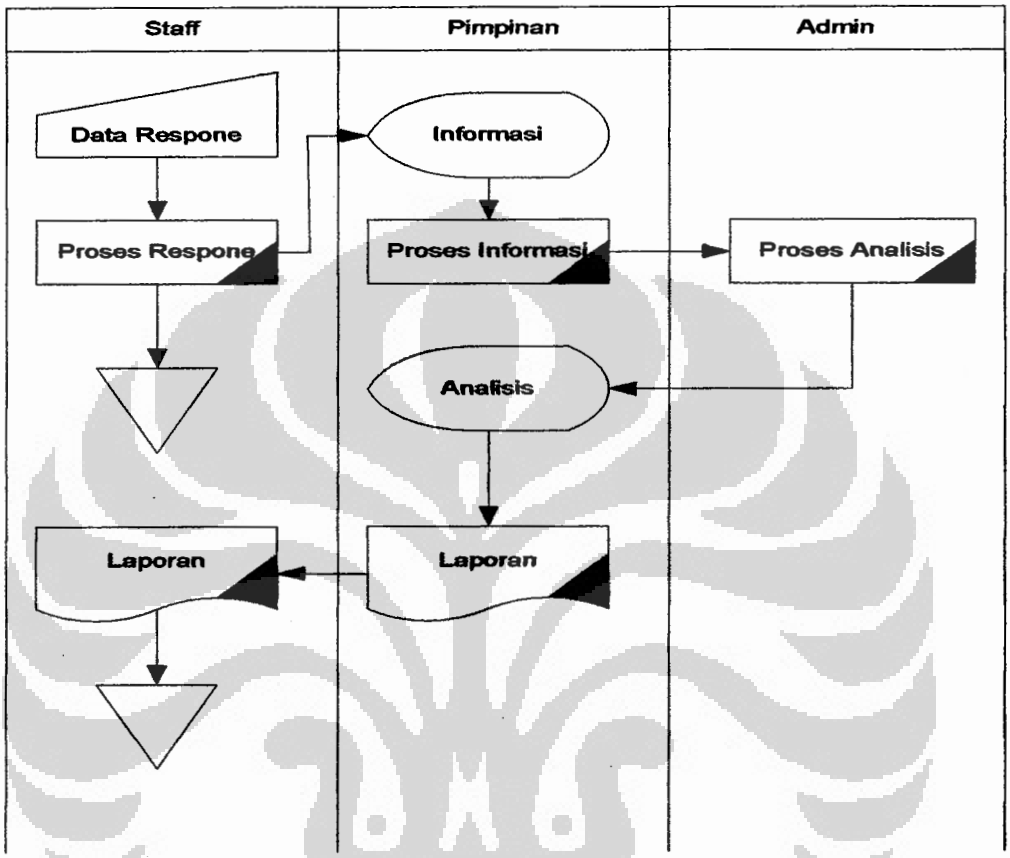
9. Pengelolaan Kelangsungan Bisnis (Business Continuity Management)				
9.1. Aspek perencanaan kelangsungan bisnis		Rencana kelangsung/kesinambungan/kelanjutan bisnis seharusnya untuk mencegah usaha interupsi pada aktivitas bisnis.		
9.1.1.	Proses manajemen kelangsungan bisnis	Apakah ada proses untuk mengembangkan/menjaga rencana kelangsungan/kelanjutan bisnis perusahaan ?	Y T	
9.1.2.	Analisis kelangsungan bisnis dan akibat	Apakah strategi untuk menjaga kelangsungan bisnis perusahaan dari berbagai pendekatan yang didukung oleh pihak manajemen ?	Y T	
9.1.3.	Membuat dan mengimplementasikan rencana berkelanjutan	Sudahkan rencana berkelanjutan menekankan identifikasi dan kesesuaian dari semua tanggung jawab serta prosedur darurat ?	Y T	
9.1.4.	Kerangka kerja rencana bisnis berkelanjutan	Apakah kerangka rencana kesinambungan bisnis telah konsisten dalam semua levelnya ?	Y T	
9.1.5.	Pengujian, perawatan dan pengukuran ulang rencana kesinambungan bisnis	Apakah rencana kesinambungan bisnis telah diuji secara berkala untuk memastikan bahwa rencana tersebut terlaksana dan efektif ?	Y T	

10. Pemenuhan/Kelengkapan (Compliance)				
10.1. Kelengkapan akan kebutuhan legal.		Semua kebutuhan yang relevan dengan sistem TI harus diidentifikasi dan didokumentasikan.		
10.1.1.	Identifikasi peraturan yang diberlakukan	Apakah semua undang-undang, peraturan dan kebutuhan kontrak secara spesifik didefinisikan dan didokumentasikan untuk tiap sistem informasi ?	Y __ T __	
10.1.2.	Hak atas kekayaan intelektual	Apakah telah ada pelarangan secara legal untuk penggunaan materi-materi yang mempunyai hak patent/copyright untuk menjamin bahwa hanya *aplikasi/ software* yang dibuat dan disediakan oleh perusahaan (RS. MH. Thamrin) ?	Y __ T __	
10.1.3.	Penggunaan catatan/ arsip organisasional	Apakah catatan/arsip organisasional telah diberlakukan secara aman agar sesuai dengan kebutuhan perundangan serta untuk mendukung aktivitas bisnis yang penting ?	Y __ T __	
10.1.4.	Perlindungan akan data dan informasi pribadi	Apakah aplikasi yang memproses data pribadi telah dilengkapi dengan peraturan perlindungan data ?	Y __ T __	
10.1.5.	Pencegahan atas salah penggunaan dari fasilitas pemrosesan informasi	Apakah fasilitas TI hanya digunakan untuk tujuan bisnis ?	Y __ T __	
10.1.6.	Peraturan pengawasan kriptografi	Apakah pengawasan kriptografi di perusahaan telah sesuai dengan hukum yang berlaku nasional dan inter- nasional ? (Kriptografi : cara penyandian untuk melindungi data dengan cara merubah data menjadi bentuk lain sehingga tidak terbaca oleh pihak lain).	Y __ T __	
10.1.7.	Pengumpulan bukti	Apakah telah ada proses untuk pengumpulan bukti	Y __	

		membutktikan kualitas, kebenaran dan kelengkapan jika kelak diperlukan dilakukan tindakan terhadap seseorang yang menyangkut masalah hukum ?	T __	
10.2. Pengkajian ulang/review atas kebijakan keamanan dan kelengkapan teknis		Untuk memastikan sistem TI telah dilengkapi dengan kebijakan dan standar keamanan perusahaan, kajian kelengkapan harus dilaksanakan secara rutin.		
10.2.1.	Kesesuaian dengan kebijakan keamanan	Apakah semua bidang dalam organisasi telah dikaji untuk memastikan kelengkapannya atas kebijakan dan standart keamanan ?	Y __ T __	
10.2.2.	Pengecekan kesesuaian teknis	Apakah fasilitas TI secara *rutin dicek* kelengkapannya atas pemberlakuan standar keamanan ?	Y __ T __	
10.3. Pertimbangan tentang sistem audit		Seharusnya ada pengawasan akan sistem operasional dan perangkat audit dalam audit sistem untuk meminimalisir interfensi ke dan dari proses audit, serta untuk melindungi integritas dan mencegah salah penggunaan perangkat audit.		
10.3.1.	Pengaturan sistem audit	Apakah audit dan aktivitas lain yang bertujuan mengecek/review sistem operasional telah direncanakan dan diatur dengan baik ?	Y __ T __	
10.3.2.	Perlindungan terhadap perangakat sistem audit	Apakah akses terhadap perangkat sistem audit diatur ?	Y __ T __	

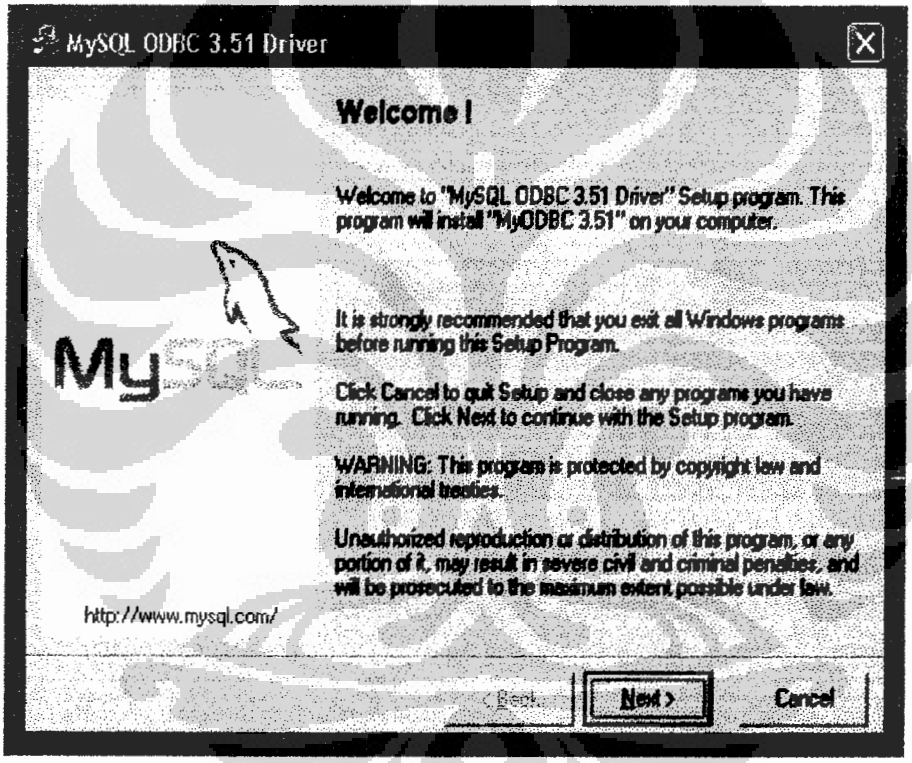
= *Terima Kasih* =

Lampiran 2. ***Flow Chart Paperwork*** **Sistem Audit Keamanan Sistem Informasi**

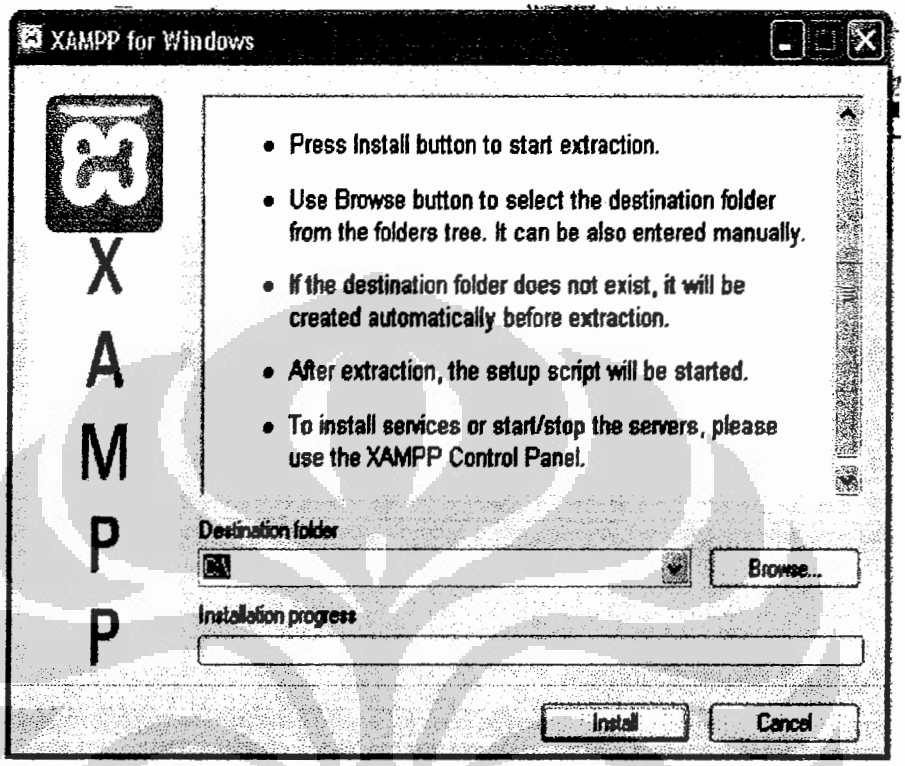


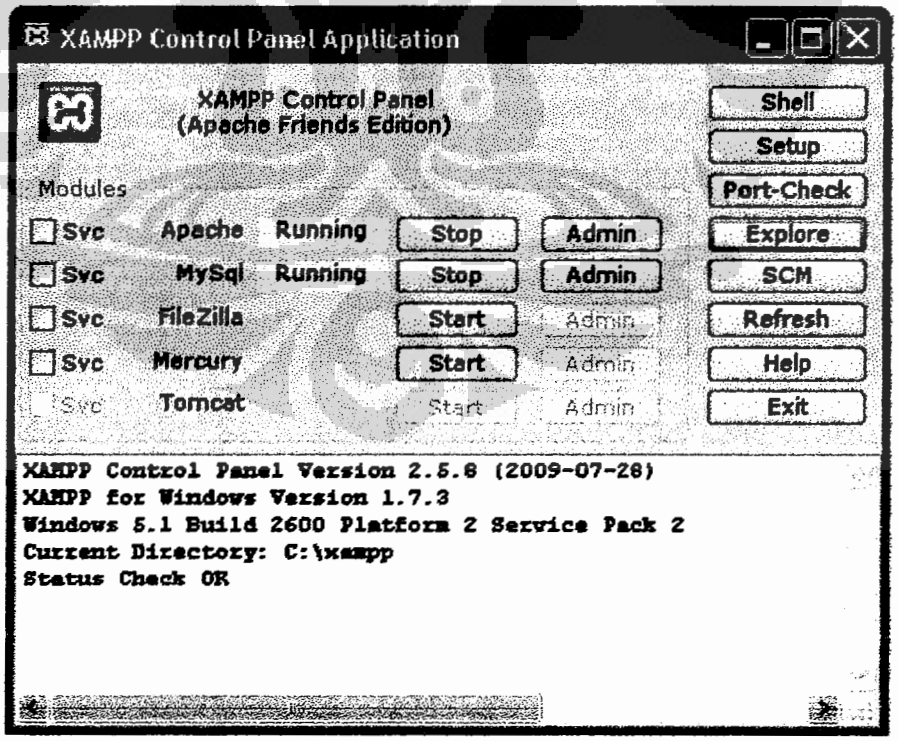
Lampiran 3. Petunjuk Instalasi Program

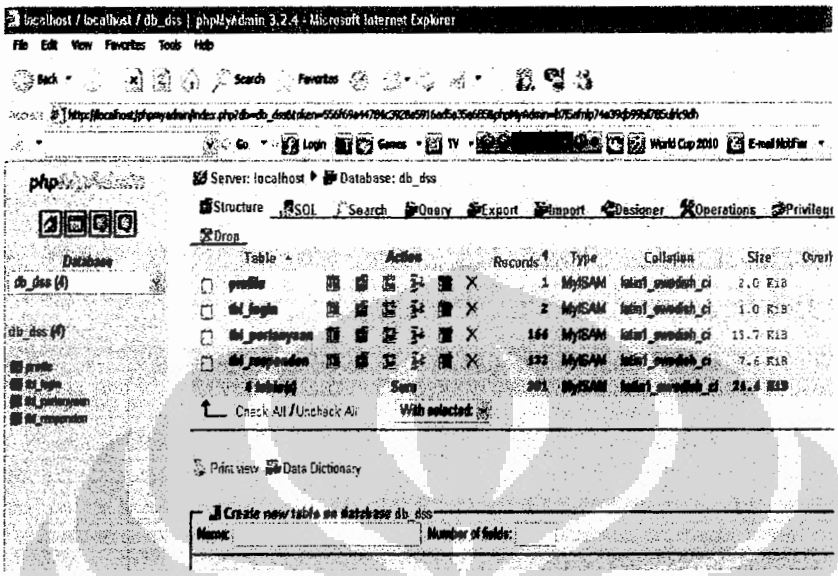
1. Instalasi : *MyODBC-3.51.03.exe* **(*Untuk Koneksi dari DSS ke Database*)**
   Cari file MyODBC-3.51.03.exe **pada CD program DSS, kemudian *double click* dan ikuti petunjuk selanjutnya.**



2. **Instalasi : *Xampp-win32-1.7.3* (Sebagai *database*)**
   ***Cari file* Xampp-win32-1.7.3 pada CD program DSS, kemudian *double click* dan ikuti petunjuk selanjutnya.**







4. ***Relation Database* DSS**

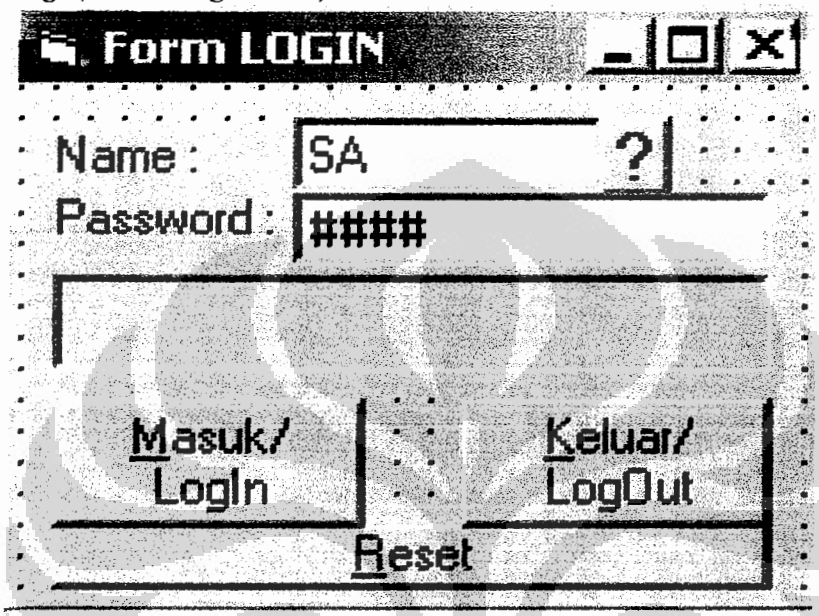
Name : db_dss

Apache/2.2.14 (Win32) DAV/2 mod_ssl/2.2.14 OpenSSL/0.9.8l mod_autoindex_color PHP/5.3.1 mod_apreq2-20090110/2.7.1 mod_perl/2.0.4 Perl/v5.10.1

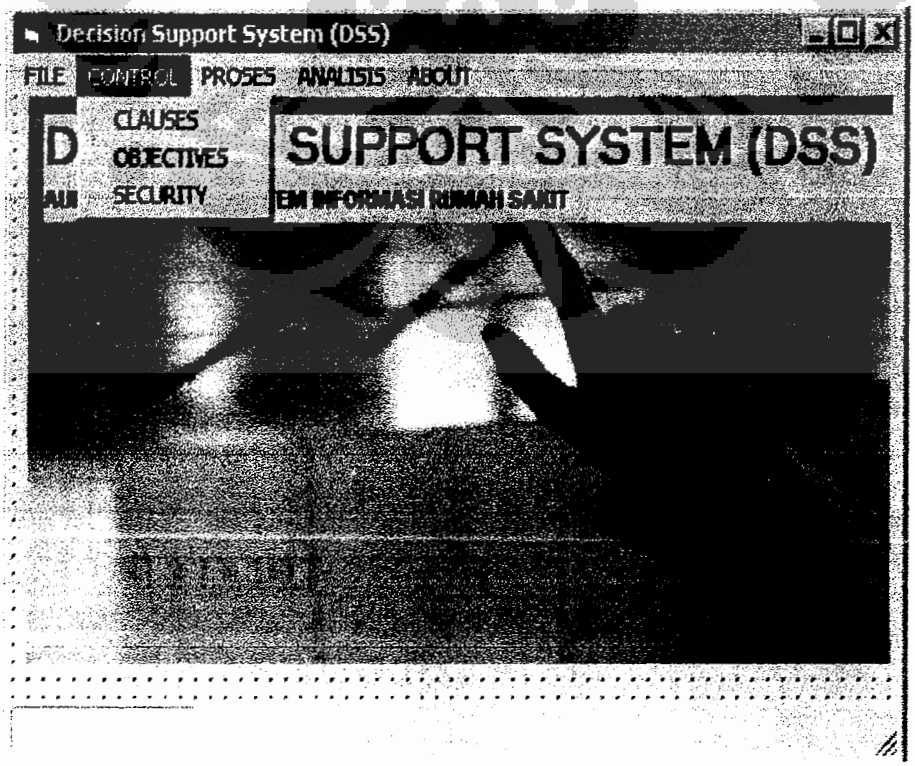
MySQL client version: 5.1.41

Lampiran 5. *Desain Input* dan *Output*

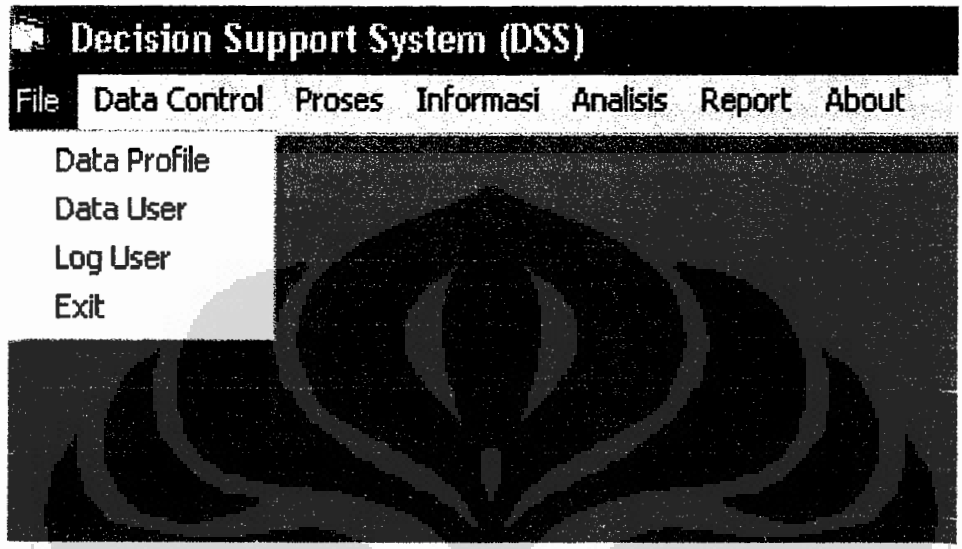
1. ***Log*** *(Untuk Login User)*

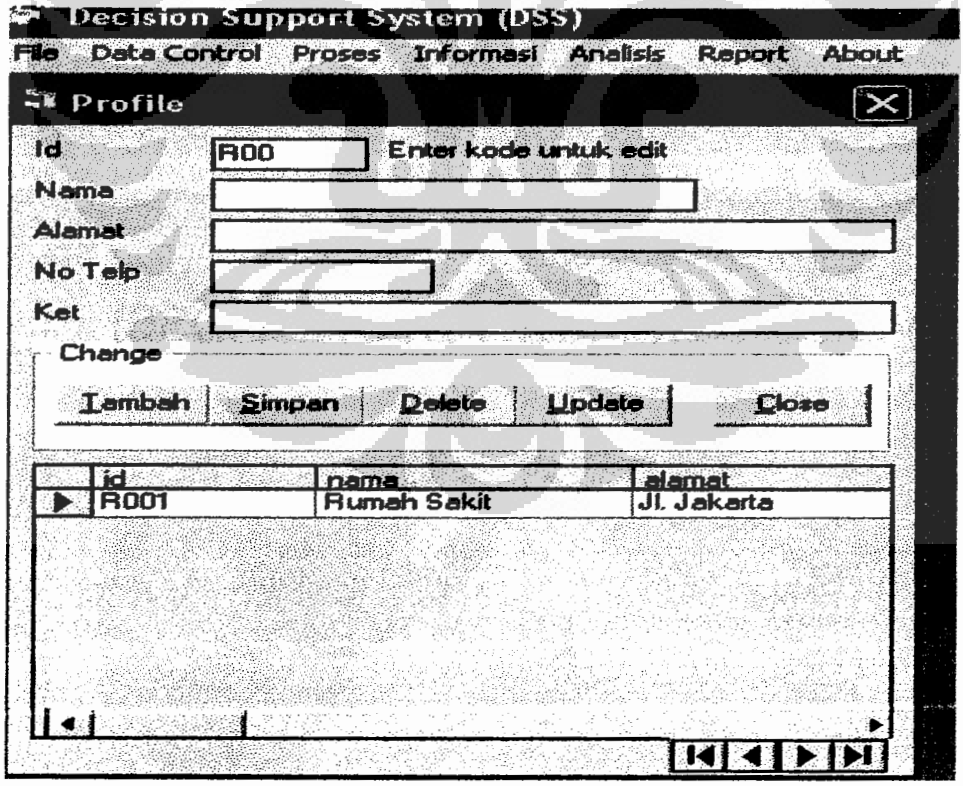


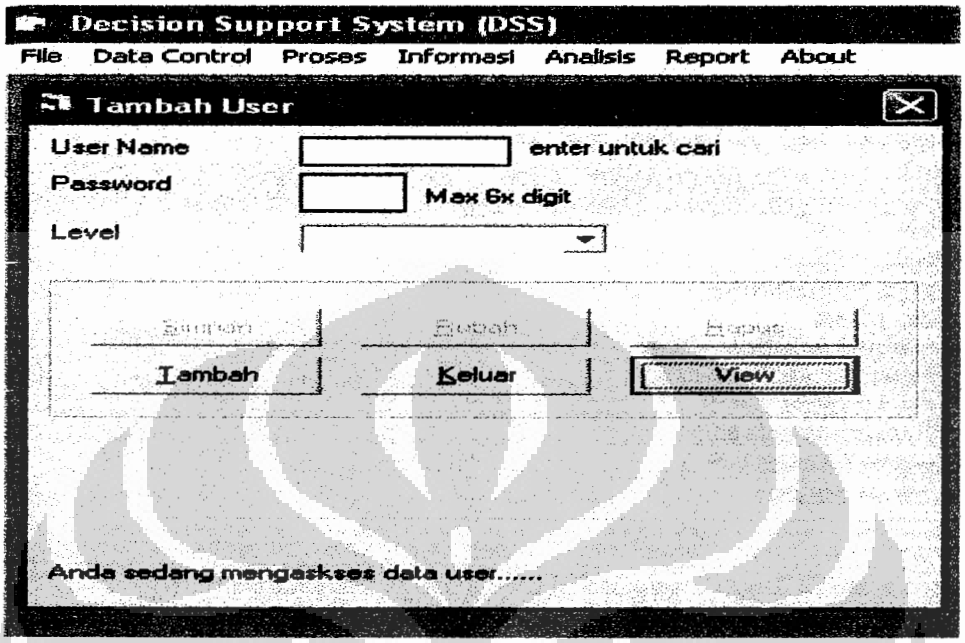
2. **Utama** ***(Menu File, Data, Proses, Informasi, Analilsis, Report, dan About)***

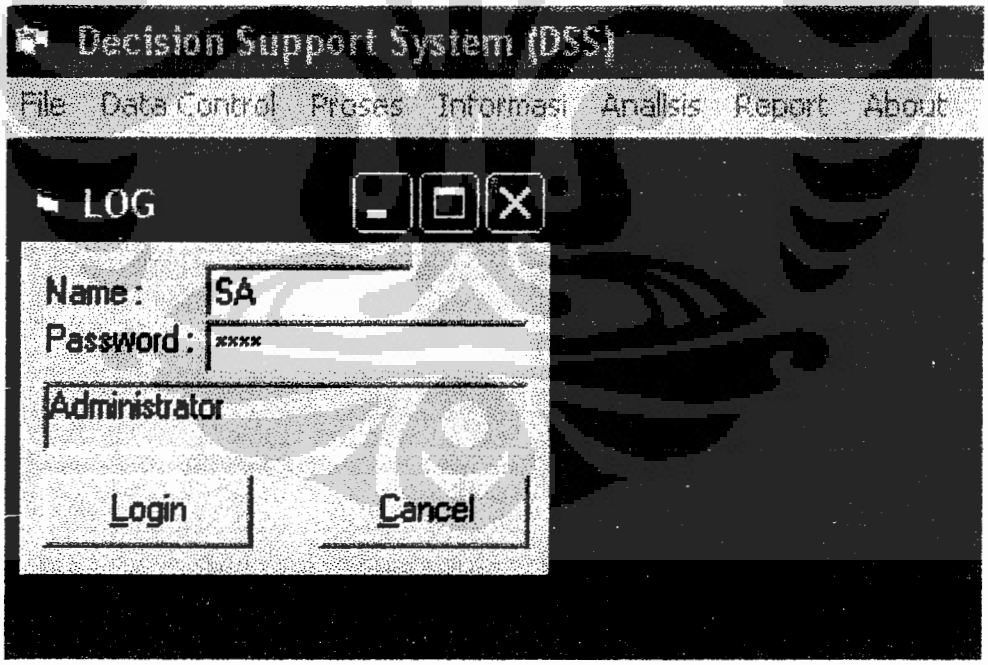


3. ***File***

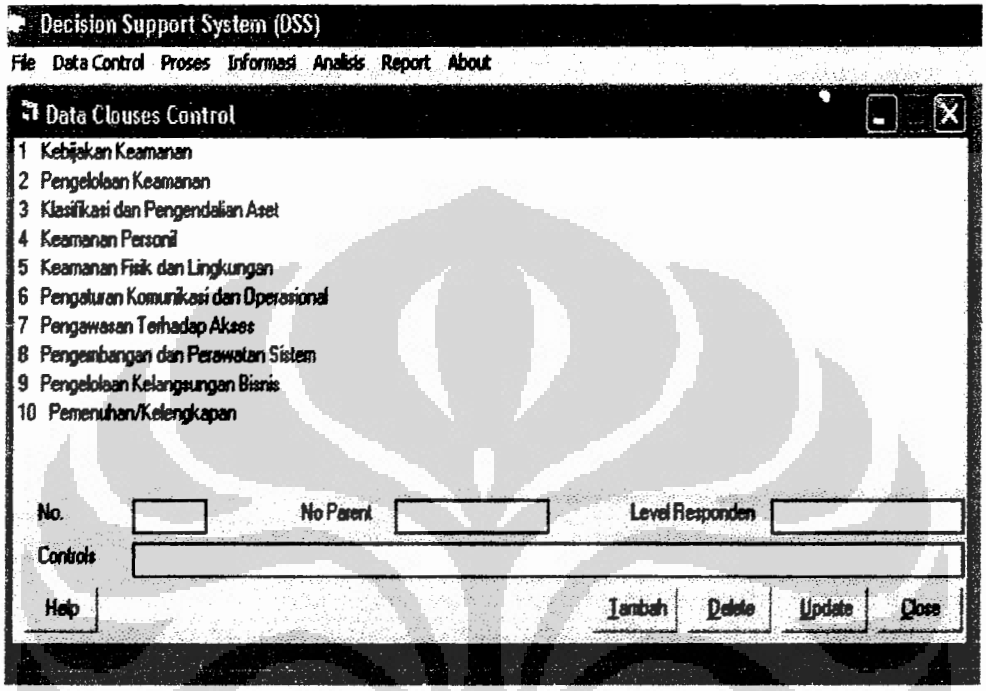


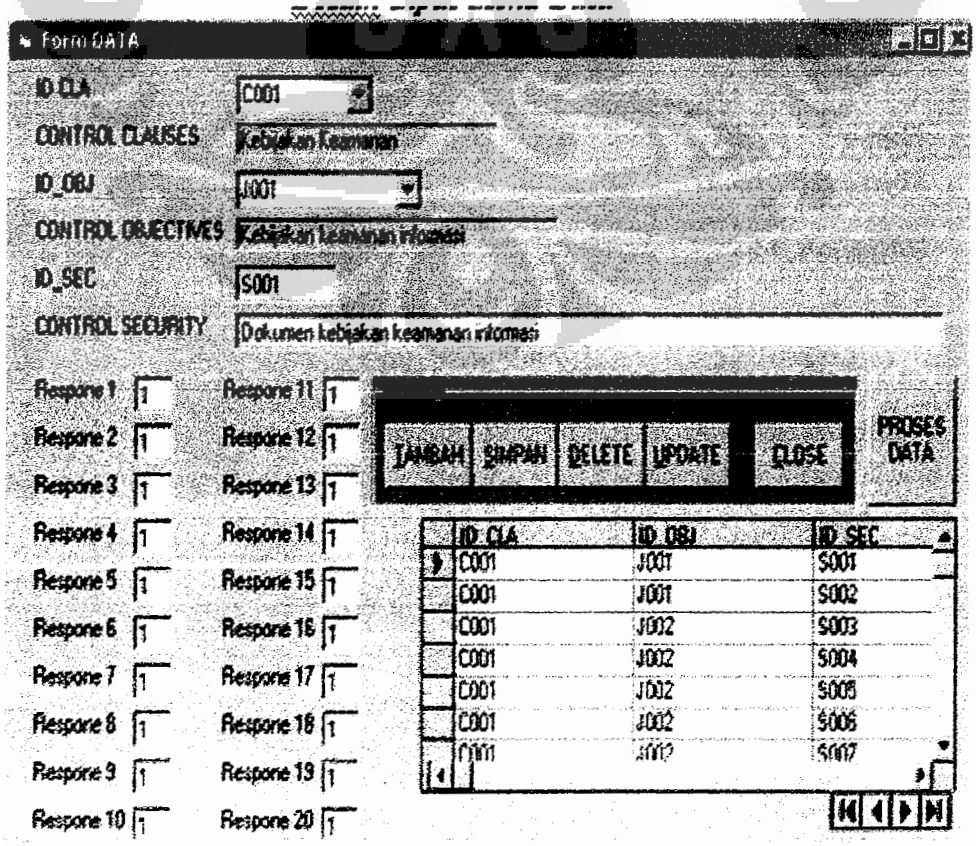




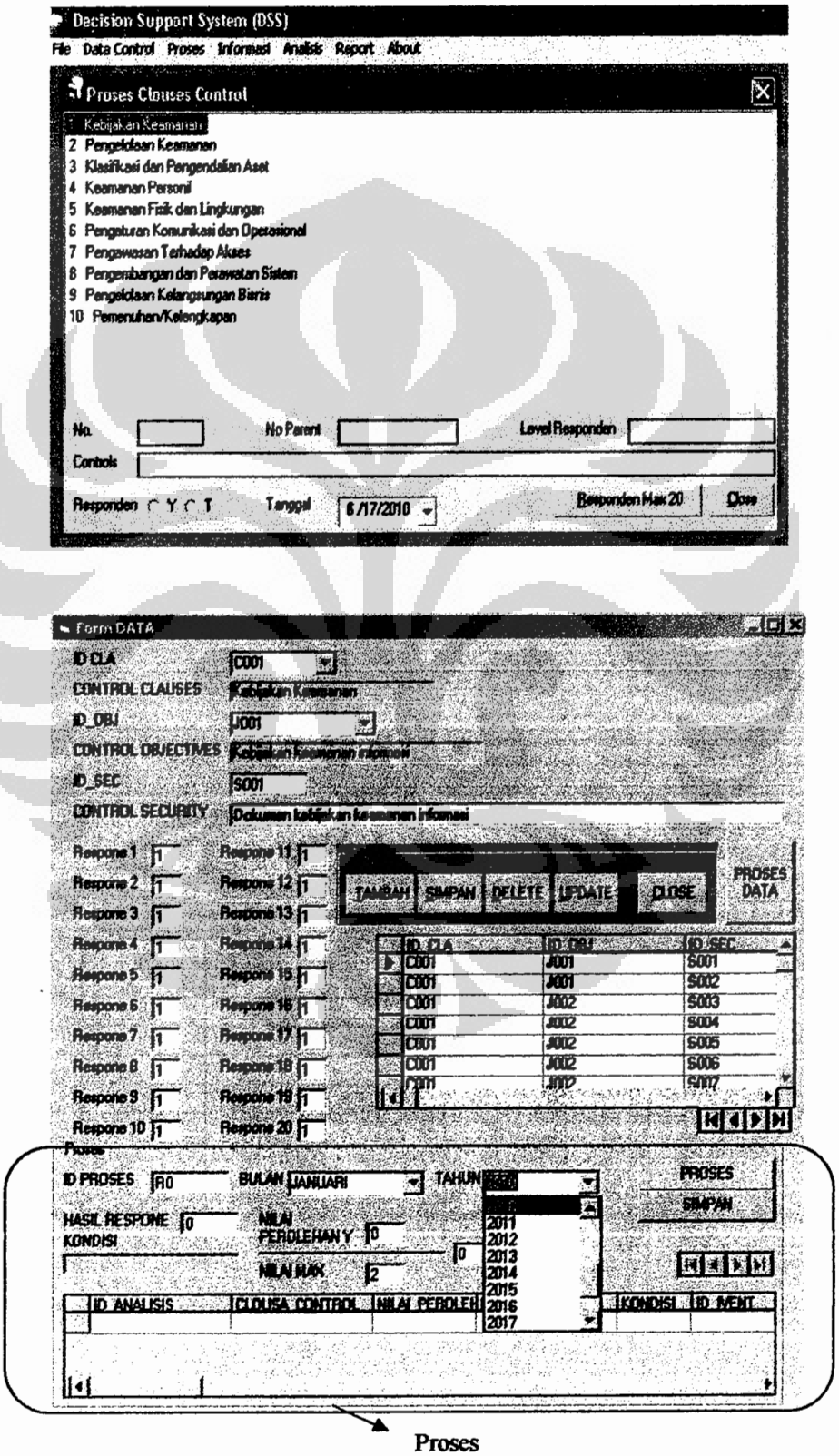


4. Data



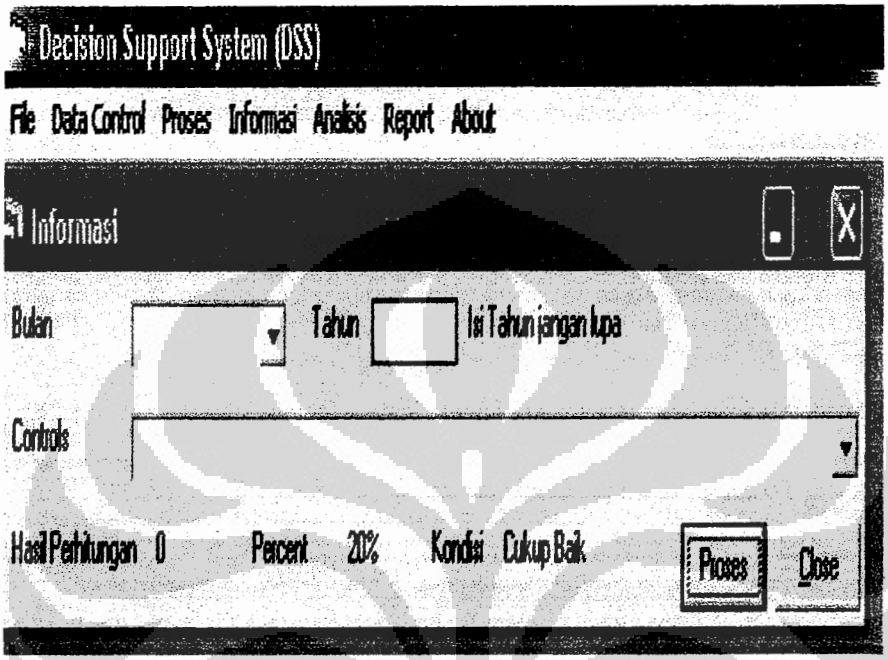


5. Proses

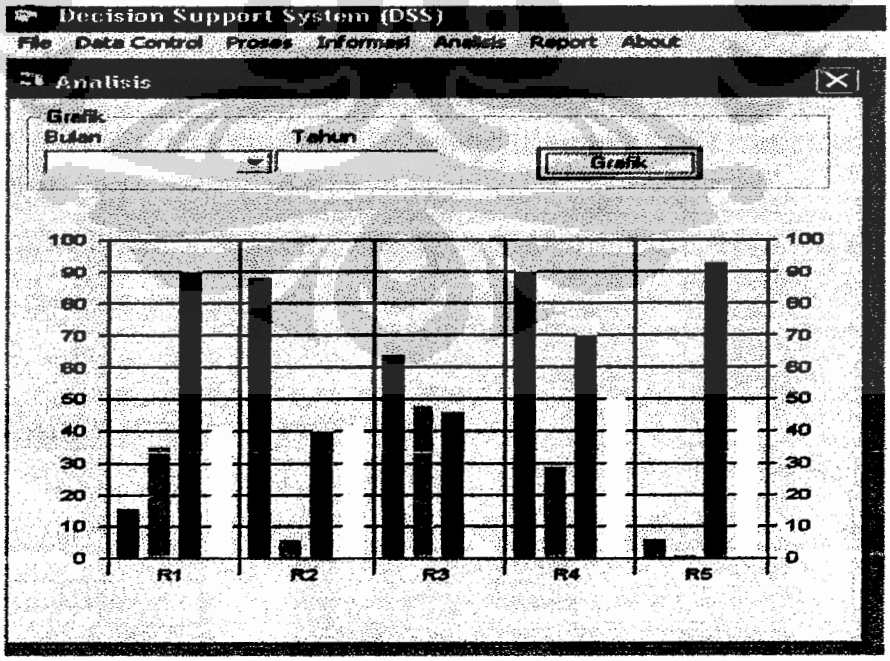


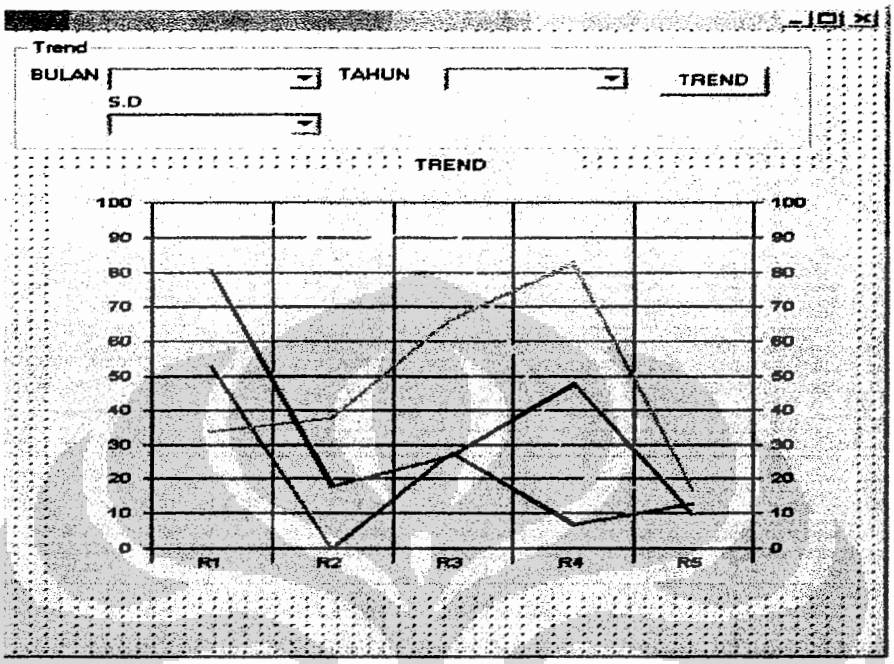
Proses

6. Informasi

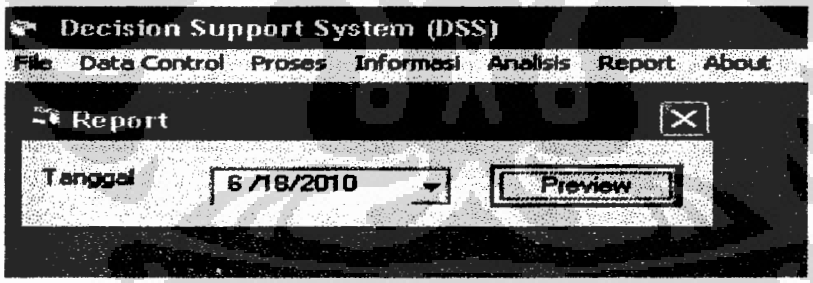


7. Analisis





8. ***Report***



9. ***About***