



Kerangka Kerja Tatacara Pengauditan Teknologi Maklumat

NOORHIDAWATI ABDULLAH, IBRAHIM MOHAMED,
ABDUL RAZAK HAMDAN & KHAIRUDDIN OMAR

ABSTRAK

Kajian ini bertujuan untuk mencadangkan satu kerangka kerja pengauditan teknologi maklumat (TM) bagi kawalan keselamatan rangkaian. Kerangka kerja ini mengandungi dua sub-kerangka kerja iaitu sub-kerangka kerja polisi kawalan keselamatan rangkaian yang dinamakan PolisiNet, dan sub-kerangka kerja tatacara proses pengauditan TM yang dinamakan ProsedurNet. Sebagai sokongan kepada kerangka kerja yang dicadangkan, kajian ini telah membangunkan Sistem Sokongan Keputusan (SSK) Pengauditan TM yang dinamakan AuditNet. AuditNet mengetengahkan penggunaan konsep berasaskan pengetahuan. Ia dibangunkan berdasarkan kepada kerangka kerja tatacara pengauditan TM yang dicadangkan. Sistem AuditNet dibangunkan menggunakan perisian WinProlog versi 4.1 untuk enjin pentadbiran, Visual Basic versi 6.0 untuk antara muka, dan Microsoft Access versi 2000 untuk pangkalan data.

ABSTRACT

This study intends to propose an information technology (TM) auditing framework for network security controls. This framework consists of two sub-frameworks; a network security control policy sub-framework called PolisiNet, and a TM auditing process procedure sub-framework called ProsedurNet. To support the proposed framework, this research has developed a TM Auditing Decision Support System called AuditNet. AuditNet introduces the use of knowledge-based concept and it is developed based on the proposed IT auditing framework. The AuditNet system is developed using WinProlog version 4.1 for the inference engine, Visual Basic version 6.0 for the interface, and Microsoft Access version 2000 for the database.

PENGENALAN

Pada masa kini, penggunaan komputer semakin meluas dalam pemrosesan data dan pembuatan keputusan. Pengurusan harian sesebuah organisasi banyak



dilakukan menggunakan komputer. Lantaran itu, penggunaan komputer perlu disertai dengan proses kawalan kerana organisasi terpaksa berhadapan dengan risiko keselamatan seperti penggodam, serangan virus, kegagalan sistem komputer dan pembaziran sumber. Sementara itu, untuk memastikan risiko-risiko ini berada pada tahap yang minimum, proses kawalan ini perlu dinilai keberkesannya melalui suatu mekanisme yang dikenali sebagai pengauditan TM. Perkembangan teknologi sebenarnya banyak membantu juruaudit TM menjalankan tugas. Walau bagaimanapun bilangan juruaudit yang benar-benar mahir dalam pengauditan TM adalah kurang. Justeru, kepakaran yang ada pada juruaudit-juruaudit ini dimasukkan ke dalam Sistem Pakar (SP) supaya proses pengauditan boleh dijalankan tanpa kehadiran mereka serta boleh membantu juruaudit baru mempelajari proses pengauditan TM. Kajian ini bertujuan untuk mencadangkan suatu kerangka kerja tatacara pengauditan TM sebagai asas pembangunan SP dalam bidang pengauditan TM.

LATAR BELAKANG KAJIAN

Kajian mengenai pengauditan TM yang dijalankan di Malaysia telah bermula sejak tahun 1990-an lagi sehingga kini. Pada tahun 1990, kajian yang berkaitan dengan penggunaan SP dalam pengauditan Sistem Maklumat telah dijalankan oleh para penyelidik Fakulti Sains Komputer dan Sains Maklumat (FSKSM), Universiti Teknologi Malaysia (UTM). Kajian ini bertujuan untuk merekabentuk dan membangunkan SP Pengauditan Komputer UTM (UTM-CAES) (Zailani et al. 1992).

Pada peringkat awal dalam kajian pengauditan TM, lebih banyak tumpuan diberikan untuk mendapatkan maklumat mengenai status dan amalan pengauditan TM, serta kawalan dan keselamatan di Malaysia. Kemudian, ia berkembang kepada kajian mengenai sejauh mana tahap pelaksanaan pengauditan TM di sektor kerajaan, dan pengenalpastian faktor-faktor yang menyumbang ke arah kewujudan atau tidak pelaksanaan pengauditan TM.

Selain itu, terdapat banyak kajian mengenai penggunaan konsep SP dalam bidang pengauditan TM. Ini adalah kerana kurangkannya bilangan juruaudit yang mahir dalam bidang pengauditan TM (Zailani et al. 1992). Oleh itu, kepakaran beberapa juruaudit TM dimasukkan ke dalam SP supaya proses pengauditan boleh dijalankan tanpa kehadirannya serta boleh membantu juruaudit baru mempelajari proses pengauditan TM (Noorhidawati 2003).

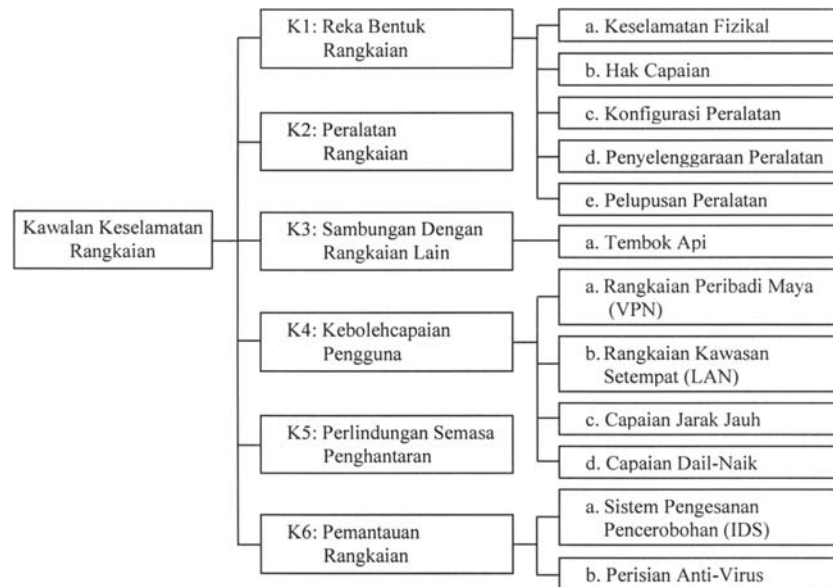
Justeru, kajian ini dijalankan sebagai kesinambungan kepada kajian-kajian yang lepas di dalam bidang pengauditan TM. Kajian ini walau bagaimanapun memberikan tumpuan khusus kepada pembentukan kerangka kerja tatacara pengauditan TM.

KERANGKA KERJA PENGAUDITAN TM BAGI KAWALAN
KESELAMATAN RANGKAIAN

Kerangka kerja ini mengandungi dua sub-kerangka kerja iaitu:

- i. Sub-kerangka kerja polisi kawalan keselamatan rangkaian (PolisiNet) sebagai panduan pengauditan TM untuk sektor awam Malaysia.
- ii. Sub-kerangka kerja tatacara proses pengauditan TM (ProsedurNet) bagi tujuan pembangunan perisian pengauditan TM yang berasaskan pengetahuan pada masa akan datang.

Kajian ini telah mengklasifikasikan PolisiNet kepada enam sub-kerangka kerja seperti yang ditunjukkan dalam Rajah 1. Sub-kerangka kerja ini mengandungi cadangan polisi kawalan keselamatan rangkaian sebagai panduan pengauditan TM untuk sektor awam di Malaysia.



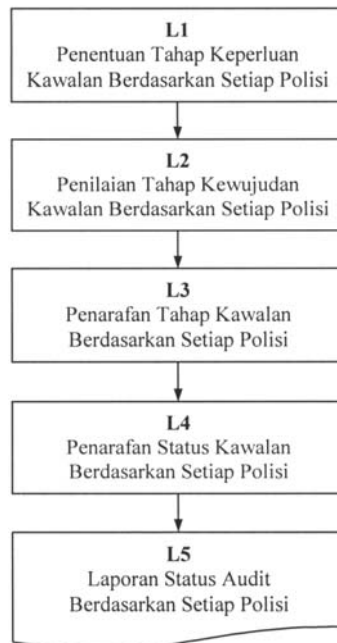
RAJAH 1. PolisiNet

Manakala sub-kerangka kerja tatacara proses pengauditan pula melibatkan:

- i. Proses penentuan tahap keperluan kawalan keselamatan bagi setiap polisi di dalam kerangka kerja yang dicadangkan.
- ii. Proses penilaian tahap kewujudan kawalan keselamatan bagi setiap polisi di dalam kerangka kerja yang dicadangkan.
- iii. Proses penarafan tahap kawalan bagi setiap polisi tersebut.

- iv. Proses penarafan status audit kawalan keselamatan berdasarkan keputusan tahap kawalan (rujuk Rajah 1).

Rajah 2 menunjukkan carta alir bagi ProsedurNet. Langkah L1 iaitu penentuan tahap keperluan kawalan keselamatan dijalankan berdasarkan kepada setiap polisi kawalan keselamatan yang wujud di sesebuah organisasi. Penentuan tahap keperluan kawalan ini dilakukan oleh pihak pengurusan dan Pegawai Sistem Maklumat organisasi terbabit. Mereka perlu menentukan sejauh mana tahap keperluan kawalan keselamatan TM organisasi masing-masing berdasarkan kepada tiga kategori tahap keperluan (rujuk Jadual 1).



RAJAH 2. Carta alir ProsedurNet

JADUAL 1. Kategori tahap keperluan

Tahap Keperluan	Takrifan
Amat Perlu	Sesuatu kawalan keselamatan itu sangat diperlukan di organisasi.
Perlu	Sesuatu kawalan keselamatan itu diperlukan pada tahap yang kurang secara relatifnya dari kategori amat perlu.
Tidak Perlu	Sesuatu kawalan keselamatan itu tidak diperlukan langsung di organisasi.



Kemudian langkah L2, penilaian tahap kewujudan kawalan keselamatan dijalankan berdasarkan kepada setiap polisi sesebuah organisasi. Penilaian ini dilakukan oleh juruaudit yang bertanggungjawab menjalankan proses pengauditan di organisasi terbabit. Tahap kewujudan kawalan akan dapat ditentukan setelah juruaudit menjalankan proses temu ramah, perbincangan, pemerhatian, penyemakan dokumentasi, serta aktiviti-aktiviti lain seperti yang terkandung di dalam fasa pengauditan. Proses penilaian ini adalah berdasarkan kepada dua kategori tahap kewujudan kawalan (rujuk Jadual 2).

JADUAL 2. Tahap kewujudan kawalan

Tahap Kewujudan	Takrifan
Wujud	Kawalan keselamatan wujud sebahagian atau keseluruhannya.
Tidak Wujud	Kawalan keselamatan tidak wujud langsung.

Seterusnya langkah L3, penarafan tahap kawalan berdasarkan setiap polisi akan dilaksanakan mengikut matriks penarafan tahap kawalan, seperti yang ditunjukkan dalam Rajah 3 (Noorhidawati et al. 2002).

		Tahap Keperluan Kawalan		
		Amat Perlu	Perlu	Tidak Perlu
Tahap Kewujudan Kawalan	Wujud	Amat Baik	Baik	Pembaziran Sumber
	Tidak Wujud	Kritikal	Tidak Memuaskan	Tiada Komen

RAJAH 3. Matriks penarafan tahap kawalan keselamatan

Penarafan ini menghasilkan 6 kategori tahap kawalan yang diubahsuai daripada Ibrahim (1999), rujuk Jadual 3.

Seterusnya, penarafan keputusan-keputusan tahap kawalan di atas akan dilaksanakan dalam langkah L4 untuk menentukan status kawalan keselamatan rangkaian organisasi terlibat. Terdapat 7 kategori status kawalan keselamatan yang akan dihasilkan, seperti yang ditunjukkan dalam Jadual 4. Sila rujuk Jadual 5 bagi melihat status kawalan keselamatan.





JADUAL 3. Kategori tahap kawalan

Kategori	Takrifan
Amat Baik	Tahap kawalan keselamatan berada pada tahap paling baik. Keadaan ini diperolehi jika tahap keperluan adalah 'Amat Perlu' dan tahap kewujudan adalah 'Wujud'.
Baik	Tahap kawalan keselamatan berada pada tahap yang agak baik tetapi secara relatifnya tahap ini kurang daripada tahap paling baik seperti yang dinyatakan di atas. Keadaan ini diperolehi jika tahap keperluan adalah 'Perlu' dan tahap kewujudan adalah 'Wujud'.
Pembaziran Sumber	Tahap kawalan keselamatan mengakibatkan sesebuah organisasi mengalami pembaziran sumber. Ini adalah kerana tahap keperluan adalah 'Tidak Perlu' tetapi tahap kewujudan adalah 'Wujud'.
Kritikal	Tahap kawalan keselamatan berada dalam keadaan yang merbahaya kerana tidak wujud kawalan keselamatan tertentu sedangkan ia amat diperlukan. Keadaan ini berlaku jika tahap keperluan adalah 'Amat Perlu' dan tahap kewujudan adalah 'Tidak Wujud'.
Tidak Memuaskan	Tahap kawalan keselamatan berada dalam keadaan yang agak merbahaya tetapi pada tahap yang kurang secara relatifnya daripada keadaan kritikal seperti yang dinyatakan di atas. Keadaan ini wujud jika tahap keperluan adalah 'Perlu' dan tahap kewujudan adalah 'Tidak Wujud'.
Tiada Komen	Tiada penilaian dilakukan terhadap tahap kawalan keselamatan kerana keadaan tahap keperluan adalah 'Tidak Perlu' dan tahap kewujudan adalah 'Tidak Wujud'.

Langkah terakhir (L5) di dalam sub-kerangka kerja tatacara ini ialah penghasilan laporan status kawalan sebagai suatu laporan audit.

REKA BENTUK AUDITNET

AuditNet dibangunkan sebagai suatu sokongan kepada kerangka kerja yang dicadangkan. Aliran fungsinya adalah berdasarkan kepada tatacara pengauditan TM seperti yang telah dinyatakan secara terperinci. AuditNet adalah sebuah sistem sokongan keputusan (SSK) yang menetengahkan penggunaan konsep sistem berasaskan pengetahuan atau dikenali sebagai sistem sokongan keputusan pakar (SSKP).

AuditNet dibangunkan dengan menggunakan metodologi *Software Development Life Cycle* (SDLC). Pembangunan sistem ini bertujuan untuk membantu juruaudit TM membuat penilaian terhadap kawalan keselamatan sesebuah organisasi. Rajah 4 menunjukkan struktur AuditNet yang terdiri daripada 5 komponen utama iaitu enjin pentadbiran, pangkalan pengetahuan,





JADUAL 4. Kategori status kawalan keselamatan

Status	Takrifan
Amat Baik	Keadaan ini berlaku apabila kombinasi kesemua tahap kawalan adalah “Amat Baik”. Sila rujuk Rajah 3.
Baik	Keadaan ini berlaku apabila kombinasi tahap kawalan adalah “Amat Baik”, “Baik” dan “Tiada Komen”.
Sederhana Baik	Keadaan ini berlaku apabila kombinasi tahap kawalan adalah “Amat Baik”, “Baik”, “Pembaziran Sumber” dan “Tiada Komen”.
Tiada Komen	Keadaan ini berlaku apabila kombinasi kesemua tahap kawalan adalah “Tiada Komen”. Selain itu, jika kombinasi tahap kawalan terdiri daripada keenam-enam tahap kawalan iaitu “Amat Baik”, “Baik”, “Kritikal”, “Tidak Memuaskan”, “Pembaziran Sumber” dan “Tiada Komen” keadaan ini juga akan berlaku.
Kurang Memuaskan	Keadaan ini berlaku apabila kombinasi tahap kawalan adalah “Pembaziran Sumber” dan “Tiada Komen”.
Tidak Memuaskan	Keadaan ini berlaku apabila kombinasi tahap kawalan adalah “Kritikal”, “Tidak Memuaskan”, “Pembaziran Sumber” dan “Tiada Komen”.
Amat Tidak Memuaskan	Keadaan ini berlaku apabila kombinasi semua tahap kawalan adalah “Kritikal”.

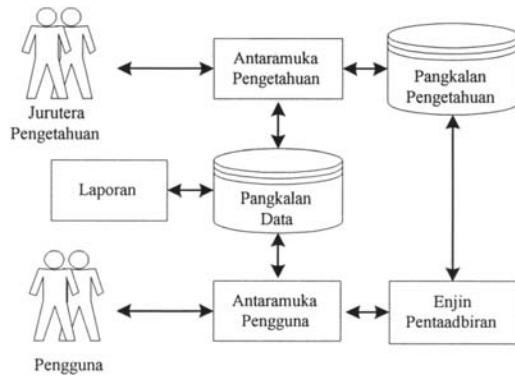
JADUAL 5. Status kawalan keselamatan

Status Kawalan Keselamatan	Tahap Kawalan					
	Amat Baik	Baik	Kritikal	Tidak Memuaskan	Pembaziran Sumber	Tiada Komen
1. Amat Baik	Semua kawalan					
2. Baik	✓	✓				✓
3. Sederhana Baik	✓	✓			✓	✓
4. Tiada Komen	✓	✓	✓	✓	✓	Semua kawalan
5. Kurang Memuaskan					✓	✓
6. Tidak Memuaskan			✓	✓	✓	✓
7. Amat Tidak Memuaskan			Semua kawalan			





antara muka, pangkalan data, dan laporan. Penjelasan terperinci berhubung Rajah 4 ini diterangkan dalam tajuk-tajuk kecil di bawah, merangkumi enjin pentadbiran, pangkalan pengetahuan, pangkalan data, antara muka dan laporan.

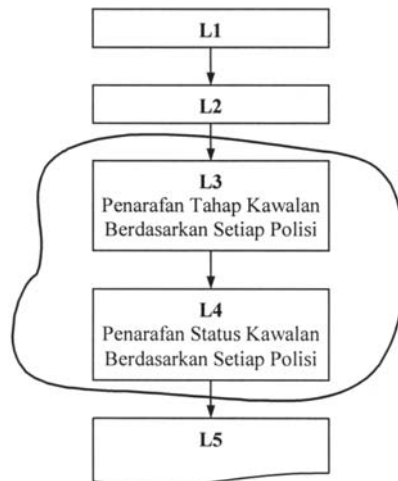


RAJAH 4. Struktur AuditNet

ENJIN PENTADBIRAN

Enjin pentadbiran AuditNet menjalankan langkah L3 dan L4 ProsedurNet seperti yang ditunjukkan pada Rajah 5 iaitu:

- Langkah L3: Penarafan tahap kawalan berdasarkan setiap polisi kawalan keselamatan.
- Langkah L4: Penarafan status kawalan keselamatan berdasarkan keputusan penarafan tahap kawalan dalam langkah L3.



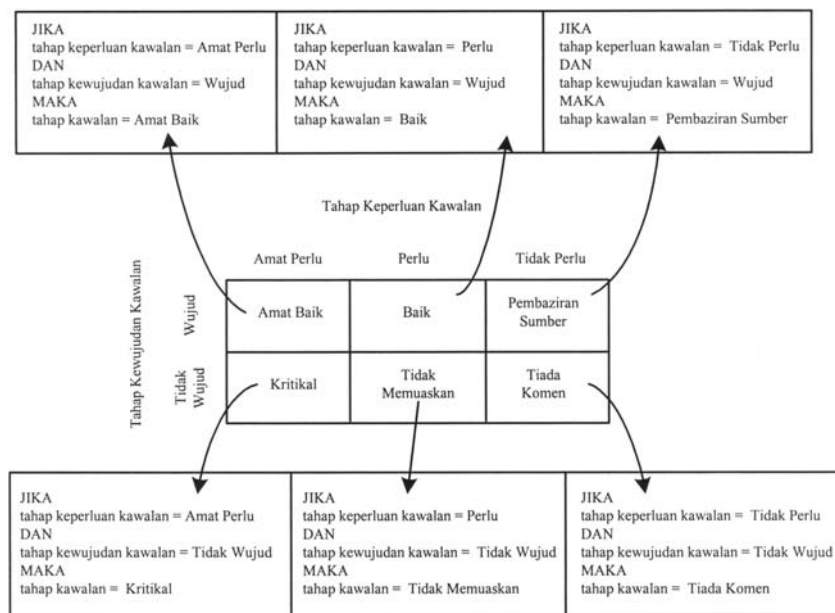
RAJAH 5. Langkah L3 dan L4 ProsedurNet





PANGKALAN PENGETAHUAN

Pangkalan pengetahuan AuditNet mengandungi polisi-polisi kawalan keselamatan TM (PolisiNet). Pengetahuan ini diwakili dalam bentuk petua JIKA <situasi> MAKA <tindakan>. AuditNet menggunakan teknik perwakilan pengetahuan berbentuk petua berdasarkan sistem rantai ke depan. Berikut adalah beberapa contoh petua yang digunakan di dalam pembangunan AuditNet (sila rujuk Rajah 6).



RAJAH 6. Petua berdasarkan matriks penarafan tahap kawalan keselamatan

PANGKALAN DATA

Pangkalan data AuditNet menyimpan maklumat organisasi yang telah diaudit, maklumat pengguna sistem dan juga laporan status audit. Ia terdiri daripada 3 buah jadual iaitu:

- i. Jadual Maklumat Organisasi: Menyimpan maklumat organisasi yang diaudit.
- ii. Jadual Pengguna: Menyimpan rekod pengguna yang menggunakan AuditNet.
- iii. Jadual Laporan: Menyimpan rekod laporan audit untuk organisasi yang telah diaudit.





ANTARA MUKA

Terdapat 2 jenis antara muka AuditNet iaitu:

i. Antara muka pengguna

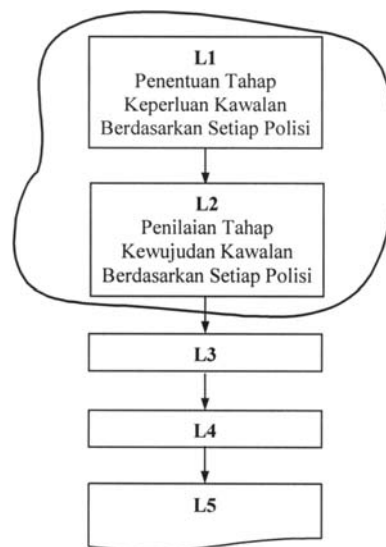
Antara muka merupakan subsistem yang membolehkan pengguna melihat serta berinteraksi dengan sistem. Terdapat 2 kategori pengguna AuditNet iaitu:

a. Pegawai Sistem Maklumat atau pihak pengurusan organisasi yang diaudit

Mereka bertanggungjawab melaksanakan langkah pertama (L1) ProsedurNet iaitu menentukan tahap keperluan kawalan berdasarkan setiap polisi di dalam kerangka kerja yang dicadangkan.

b. Juruaudit TM yang menjalankan proses pengauditan

Juruaudit TM bertanggungjawab melaksanakan langkah kedua (L2) ProsedurNet iaitu menentukan tahap kewujudan kawalan berdasarkan setiap polisi di dalam kerangka kerja yang dicadangkan. Rujuk Rajah 7.



RAJAH 7. Langkah L1 dan L2 ProsedurNe

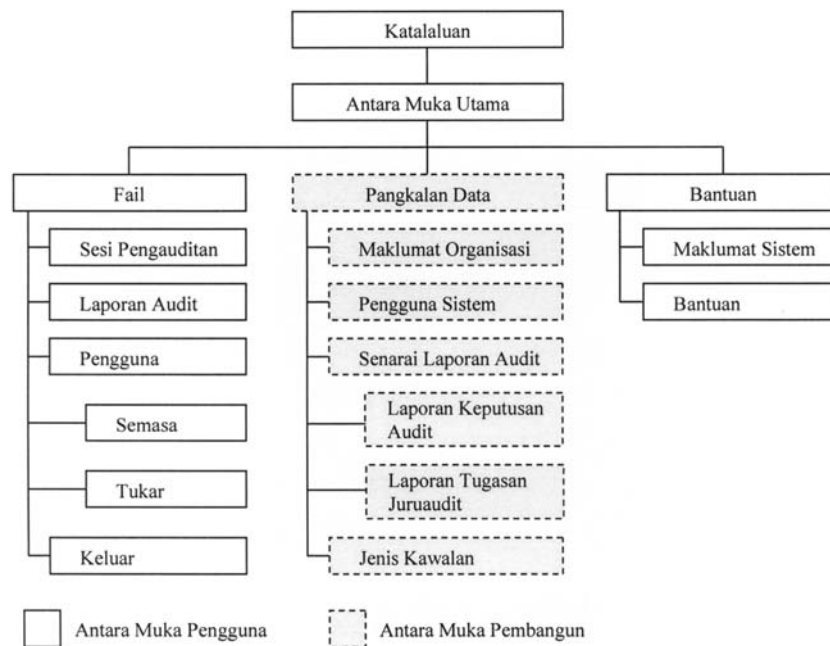
ii. Antara muka pembangun

Antara muka pembangun ini digunakan oleh jurutera pengetahuan untuk membangunkan sistem. Jurutera pengetahuan merupakan individu yang dibenarkan membuat capaian ke pangkalan pengetahuan untuk mengubah polisi-polisi kawalan keselamatan TM.





Rajah 8 adalah struktur antara muka AuditNet. Pengguna (juruaudit dan pengurus) hanya boleh membuat capaian ke atas antara muka pengguna sahaja. Manakala pembangun sistem boleh membuat capaian ke atas kedua-dua antara muka pembangun dan antara muka pengguna. Had capaian ini dilaksanakan melalui penggunaan kata laluan.



RAJAH 8. Struktur antara muka AuditNet

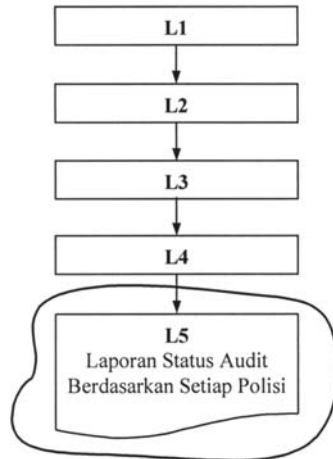
LAPORAN

Struktur laporan terbahagi kepada dua kategori. Pertama, laporan keputusan audit dan kedua, laporan tugas juruaudit. Kedua-dua kategori laporan ini boleh dicetak sebagai laporan yang lengkap atau ringkas, atau berdasarkan kueri. Penghasilan laporan merupakan langkah L5 ProsedurNet seperti yang digambarkan dalam Rajah 9.

HASIL

Sebagai kesimpulannya, kajian ini telah berjaya mencadangkan suatu kerangka kerja pengauditan TM bagi kawalan keselamatan rangkaian untuk sektor awam. Kerangka kerja ini mengandungi sub-kerangka kerja polisi kawalan keselamatan rangkaian yang dinamakan PolisiNet. PolisiNet mengandungi





RAJAH 9. Langkah L5 ProsedurNet

polisi-polisi kawalan keselamatan bagi reka bentuk rangkaian, peralatan rangkaian, sambungan dengan rangkaian lain, kebolehcapaian pengguna, perlindungan semasa penghantaran, dan pemantauan rangkaian.

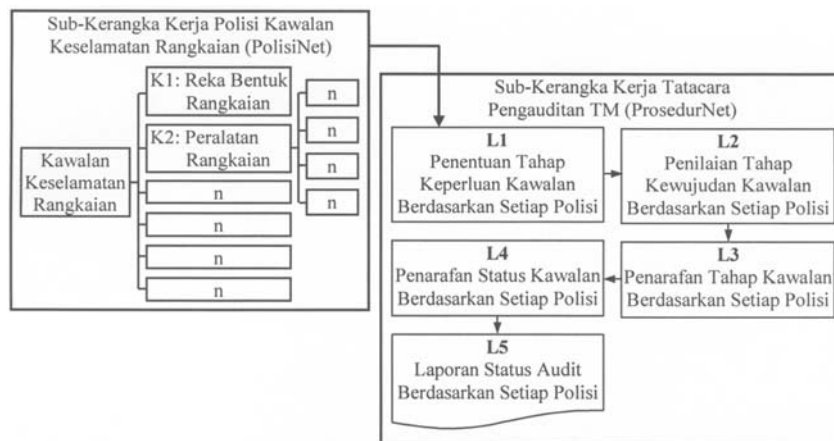
Selain itu, kerangka kerja ini juga mengandungi sub-kerangka kerja tata cara proses pengauditan TM yang dinamakan ProsedurNet. ProsedurNet dihasilkan dengan tujuan untuk membangunkan perisian pengauditan TM yang berasaskan pengetahuan. Rajah 10 menunjukkan kerangka kerja yang dihasilkan.

Kajian ini juga telah membangunkan sistem AuditNet sebagai sokongan penggunaan kerangka kerja yang dicadangkan. AuditNet adalah sistem sokongan keputusan (SSK) berasaskan pengetahuan atau dikenali sebagai SSK Pintar (SSKP). Secara umumnya struktur sistem AuditNet terdiri daripada enjin pentadbiran, pangkalan pengetahuan dan antara muka.

Pembangunan sistem ini bertujuan untuk membantu juruaudit membuat penilaian terhadap kawalan keselamatan sesebuah organisasi. Sistem yang dibangunkan dengan menggunakan metodologi SDLC ini menggunakan perisian WinProlog versi 4.1 untuk membangunkan enjin pentadbirannya, Visual Basic versi 6.0 untuk antara muka dan Microsoft Access versi 2000 untuk pangkalan data.

Kerangka kerja yang dihasilkan diharap dapat menjadi panduan pembangun-pembangun sistem membangunkan sistem pengauditan TM yang berasaskan SP. Penekanan yang diberikan oleh kajian ini adalah pembangunan sesebuah SP pengauditan bukanlah untuk menggantikan juruaudit tetapi untuk membantu juruaudit menjalankan tugasnya dengan lebih cekap.





RAJAH 10. Kerangka kerja pengauditan TM bagi kawalan keselamatan rangkaian

RUJUKAN

Ibrahim Mohamed. 1999. Penilaian ke atas tahap penggunaan perisian audit di sektor awam Malaysia. Tesis Sarjana Teknologi Maklumat. Universiti Kebangsaan Malaysia.

Ibrahim Mohamed, Suhaila Zainudin, Zaihosnita Hood, Kamaruzzaman Matharsha, Noorhidawati Abdullah, Norasmadi Yaacob, Nor Jannah Jaafar & Nor Baiti Omar. 2003. Sistem audit bersepadu (SAB). *Prosiding Seminar IRPA RMK-7*. Jilid ke-2. 17-19 Januari 2003.

Noorhidawati Abdullah, Abdul Razak Hamdan, Ibrahim Mohamed & Khairuddin Omar. 2002. Rangka kerja pengauditan TM bagi sektor awam Malaysia untuk kawalan keselamatan rangkaian. *Seminar Pengauditan Sistem Maklumat 2002*, 22 April. UKM, Bangi, 23-28.

Noorhidawati Abdullah. 2003. Suatu rangka kerja pengauditan TM bagi kawalan keselamatan rangkaian untuk sektor awam Malaysia. Tesis Sarjana. Universiti Kebangsaan Malaysia.

Zailani Mohamed Sidek, Zuraini Ismail & Tajaludin Sharif. 1992. Expert system's development in computer auditing: the UTM experience. *Proceedings of the Seminar on EDP audit and controls*, 27-28 April. UKM, Bangi.

Noorhidawati Abdullah, Ibrahim Mohamed,
Abdul Razak Hamdan & Khairuddin Omar



Ibrahim Mohamed
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi
Selangor
e-mail: ibrahim@ftsm.ukm.my

Abdul Razak Hamdan
e-mail: arh@ftsm.ukm.my

Khairuddin Omar
e-mail: ko@ftsm.ukm.my

Noorhidawati Abdullah
e-mail: n-hida95@hotmail.com