https://doi.org/10.17576/apjitm-2018-0702-07

http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 7 No. 2, December 2018: 85 - 98
e-ISSN: 2289-2192

INFORMATION SECURITY GOVERNANCE FRAMEWORK OF MALAYSIAN PUBLIC SECTOR

AMRI JAMIL
ZAWIYAH M. YUSOF

ABSTRACT

Information is one of the key assets in the organization other than employees and physical assets. Information should be protected so as not to be exposed to unauthorized individuals, especially competitors and spies. Previous studies have found that Information Security Governance (ISG) is divided into two that is technical security because of the use of information and communication technology (ICT) and non-technical information security. Implementation of ISG in the public sector in Malaysia is aimed at protecting information from technical aspects only without giving priority to information security issues that are not technical in nature, particularly in terms of content. Data analysis found that the public sector did not have guidelines on ISG in a single and integrated document form, making it difficult to implement the initiative. This study analyzes the ISG policy of Malaysian public sector agencies with the objective of developing a comprehensive ISG framework. The study employed a qualitative approach which comprises of document content analysis techniques and interviews with senior Malaysian public sector officials. The analysis of the study found that the Malaysian public sector already has a framework for governance of information security. However, the ISG framework is found in several separate documents by using different governance approaches between each one.

Keywords: information security, information security governance, information security governance framework

KERANGKA TADBIR URUS KESELAMATAN MAKLUMAT SEKTOR AWAM DI MALAYSIA

ABSTRAK

Maklumat merupakan salah satu aset penting dalam organisasi selain daripada pekerja dan aset fizikal. Maklumat perlu dilindungi supaya tidak terjatuh atau terdedah kepada individu yang tidak diberi hak untuk mengetahui dan memiliki maklumat tersebut terutamanya pesaing dan pengintip. Kajian terdahulu mendapati, Tadbir Urus Keselamatan Maklumat (TUKM) terbahagi kepada dua iaitu keselamatan yang bersifat teknikal hasil daripada penggunaan teknologi maklumat dan komunikasi (TMK) dan keselamatan maklumat yang bukan bersifat teknikal. Pelaksanaan TUKM dalam sektor awam di Malaysia menjurus kepada melindungi maklumat dari aspek teknikal sahaja tanpa memberi keutamaan yang sewajarnya kepada isu keselamatan maklumat yang bukan bersifat teknikal khususnya dari aspek kandungan. Analisis data mendapati sektor awam tidak mempunyai garis panduan tentang TUKM dalam satu bentuk dokumen tunggal dan bersepadu sehingga menyukar pelaksanaan inisiatif tersebut. Kajian ini menganalisis dasar TUKM agensi sektor awam Malaysia dengan objektif untuk membangun kerangka TUKM yang menyeluruh. Pendekatan kualitatif dipilih dengan teknik analisis kandungan dokumen dan temu bual bersama pegawai kanan sektor awam. Analisis data mendapati sektor awam mempunyai kerangka TUKM dan aspek keselamatan maklumat diberi perhatian bagi melindungi maklumat penting kerajaan. Namun kerangka TUKM tersebut didapati wujud dalam beberapa dokumen yang berasingan dengan mengguna pendekatan tadbir urus yang berbeza-beza di antara setiap satu daripadanya.

Kata kunci-keselamatan maklumat, tadbir urus keselamatan maklumat, kerangka tadbir urus keselamatan maklumat, sektor awam Malaysia

PENGENALAN

Organisasi pada hari ini mengiktiraf maklumat sebagai aset kritikal bagi menjana kekayaan dan kelebihan dalam persaingan (Roux, 2007; Webb, 2008). Maklumat berupaya menjadi penentu kepada kejayaan atau kegagalan sesebuah organisasi. Konsep maklumat sebagai aset diperkenal oleh Jawatankuasa Hawley di United Kingdom pada tahun 1994 bertujuan menggalak syarikat mengambil tanggungjawab tentang kepentingan pengurusan maklumat (Webb, 2008). Jawatankuasa ini menyedia panduan bagi melaksana pengurusan maklumat yang baik dengan melindungi maklumat daripada kecurian, kehilangan, capaian yang tidak diberi autoriti dan penyalahgunaan.

Selaras dengan kedudukannya sebagai aset, maklumat perlu ditadbir dengan mengguna pendekatan pengurusan maklumat yang melibatkan pengenalpastian, penciptaan, penyimpanan, penggunaan, penyebaran, keselamatan dan perkongsian maklumat yang cekap dan berkesan (Webb, 2008). Selain daripada meningkat produktiviti, pengurusan maklumat yang cekap dan berkesan adalah bagi memasti maklumat penting dan bernilai dapat dilindungi kerana sentiasa menjadi buruan pesaing dan pengintip maklumat.

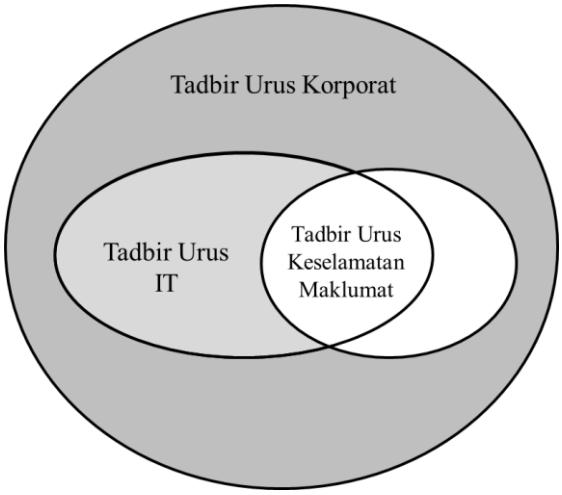
Pengendalian keselamatan ke atas maklumat penting dan bernilai merupakan tanggungjawab organisasi yang lazimnya dinyatakan dalam dasar pengurusan maklumat (Zawiyah & Robert, 2005). Namun, pengurusan keselamatan maklumat semakin mencabar kerana organisasi pada hari ini beralih kepada maklumat dalam format elektronik dan digital. Dalam era siber yang melibatkan penggunaan teknologi maklumat dan komunikasi (TMK) secara intensif menyebab Tadbir Urus Keselamatan Maklumat (TUKM) semakin mencabar kerana menyebab maklumat semakin terdedah kepada pelbagai risiko dan ancaman. Oleh yang demikian pengurusan keselamatan maklumat tidak boleh hanya memfokus kepada aspek teknikal semata-mata tanpa melibatkan aspek maklumat itu sendiri iaitu kandungan (Ohki et al., 2009; Solms & Solms, 2009).

Sejak awal abad ke-21, persepsi yang menyatakan bahawa keselamatan maklumat bukan isu TMK semata-mata diterima dengan meluas dalam mewujud persekitaran maklumat yang selamat (Posthumus & Solms, 2004). Keselamatan maklumat merupakan tanggungjawab pelbagai pihak serta perlu diurus secara menyeluruh dengan mengambil kira semua sudut supaya sebarang risiko yang mungkin berlaku dapat diatasi (Posthumus & Solms, 2004). Oleh yang demikian, konsep TUKM mula diperkenal pada awal tahun 2001 oleh Solms bagi mewujud kesedaran dalam kalangan pengurusan atasan organisasi tentang kepentingannya.

Kajian lampau tentang keselamatan maklumat mendapati organisasi tidak mengintegrasi budaya dan tingkah laku menyeluruh yang sepatutnya diaplikasi kepada keselamatan maklumat (Veiga & Eloff, 2010). Dakwaan sedemikian turut disokong oleh Ernst & Young (2013) yang mendapati TMK terus menjadi agenda utama keselamatan maklumat organisasi tanpa memberi tumpuan kepada strategi keselamatan maklumat secara keseluruhannya. Dalam erti kata lain pendekatan yang diambil adalah tidak holistik dengan menggabung aspek teknikal dan bukan teknikal. Justeru, TUKM dapat menawar satu penendekatan yang menyeluruh kepada organisasi bagi menangani isu keselamatan maklumat dengan mengambil kira perspektif tadbir urus korporat yang mencakupi pelbagai aspek dari kepimpinan (strategi, penilaian risiko, metrik), pengurusan (program, undang-undang dan peraturan), Dasar (garis panduan, amalan terbaik, prosedur, piawaian), teknologi (operasi teknikal, pembangunan sistem, pengurusan insiden) yang menuntut pengoptimuman peranan pengurusan atasan (Warkentin & Johnson, 2006).

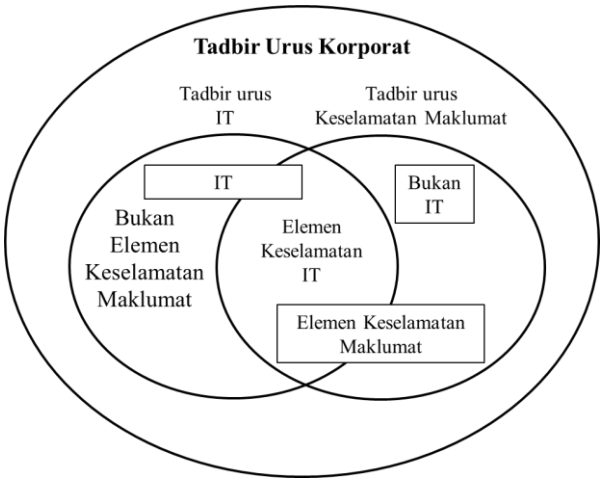
Sarjana dalam bidang keselamatan maklumat, menyatakan TUKM adalah terletak di bawah tadbir urus korporat dan berkait dengan tadbir urus teknologi maklumat (Solms & Solms, 2009) seperti yang ditunjuk dalam Rajah 1 hubungan antara tadbir urus korporat,

tadbir urus Teknologi Maklumat (IT) dan TUKM adalah saling lengkap melengkapi antara satu dengan yang lain.



RAJAH 1. Hubungan antara tadbir urus korporat, tadbir urus IT dan TUKM
Sumber: (Solms & Solms, 2009)

Konsep hubungan antara tadbir urus korporat, tadbir urus IT dan TUKM Solms dan Solms (2009) turut disokong dan dipersetujui oleh Ohki et al. (2009). Model hubungan tadbir urus Ohki et al. menyatakan TUKM terbahagi kepada dua elemen iaitu keselamatan maklumat IT dan keselamatan maklumat bukan IT yang merujuk kepada maklumat itu sendiri seperti yang ditunjuk dalam Rajah 2.



RAJAH 2. Hubungan antara tadbir urus korporat, tadbir urus IT dan TUKM
Sumber : (Ohki et al., 2009)

Elemen bukan IT adalah maklumat dalam bentuk medium kertas dan keselamatan fizikal. Sehingga kini, kertas masih diguna sebagai medium untuk tujuan bukti bertulis (kontrak, kelulusan pembelian, dan borang) serta disimpan dalam bilik kebal (Ohki et al., 2009). Kedua-dua model hubung kait Solms dan Solms (2009) dan Okhi et al. (2009) jelas memapar TUKM adalah menyeluruh dan tidak hanya menekan aspek keselamatan TMK sahaja tetapi turut meliputi elemen yang tidak bergantung kepada TMK.

Keselamatan maklumat dalam sektor awam di Malaysia tidak dipinggir malah diberi perhatian yang wajar oleh kerajaan. Kerajaan mengeluar dokumen Arahan Keselamatan yang mengandungi peraturan kawalan keselamatan perlindungan kepada ketua jabatan dalam semua Kementerian, Jabatan, Badan Berkanun dan Agensi Kerajaan. Arahan keselamatan mengaris tafsiran dan panduan bagi mengendali maklumat rasmi kerajaan. Justeru, semua agensi sektor awam perlu mematuhi peraturan yang ditetap dalam dokumen arahan keselamatan (Jabatan Perdana Menteri, 1985).

Kemajuan pesat TMK, menyebab TMK memain peranan sebagai medium pentadbiran dan penyampaian perkhidmatan kerajaan elektronik. Keadaan yang sedemikian secara tidak langsung mengubah lanskap ke atas perlindungan keselamatan maklumat. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU) mengambil inisiatif mengeluar pekeliling rangka dasar keselamatan TMK kerajaan. Pekeliling ini dirumus bagi memenuhi keperluan penguatkuasaan, kawalan dan langkah yang menyeluruh untuk melindungi aset TMK Kerajaan (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, 2000).

Pada tahun 2016, MAMPU mengeluar dokumen yang dikenali sebagai Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA) (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, 2000). RAKKSSA dibangun kerana semakin banyak maklumat kerajaan disimpan dalam bentuk digital dalam ruang siber. Dokumen tersebut bertujuan memberi panduan asas serta merangkumi semua komponen keselamatan yang perlu diambil kira oleh kementerian dan agensi sektor awam untuk melindungi maklumat dalam ruang siber. Semua komponen keselamatan siber perlu diambil kira oleh kementerian dan agensi kerajaan dalam melindungi maklumat dalam ruang siber. Natijahnya, dasar keselamatan siber perlu dibangun pada peringkat jabatan dengan berpandu kepada dokumen RAKKSSA. Namun dokumen tersebut tidak mencakupi maklumat yang dipindah dari ruang siber ke ruang fizikal (melalui cetakan, salinan tulisan tangan, rakaman foto mengguna peralatan fotografik) dan hendaklah ditangani dengan peraturan sedia ada (Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia, 2000). Ini bererti belum ada satu kerangka tadbir urus yang menyeluruh melibatkan keselamatan maklumat TMK dan bukan TMK atau keselamatan maklumat dari aspek teknikal dan bukan teknikal.

Kertas ini membincang tentang TUKM dalam organisasi awam di Malaysia. Pelaksanaan inisiatif pengurusan keselamatan maklumat jika tidak didasarkan kepada tadbir urus yang betul serta tanpa kerangka, menyebab sesebuah organisasi tidak mempunyai matlamat yang jelas (Umi & Zawiyah, 2009). Kajian keselamatan maklumat banyak tertumpu kepada isu melindungi sistem maklumat daripada ancaman siber yang menjurus kepada aspek teknikal (Hovav & D'Arcy, 2003; ISO/IEC 27001, 2005; Tassabehji, 2005; Suhazimah & Ali, 2012).

Bagaimanapun keselamatan maklumat bukan hanya tertumpu kepada aspek TMK tetapi turut melibatkan aspek lain. Malah badan ilmu sejagat (*common body of knowledge*) menyaran supaya isu keselamatan maklumat yang bukan bersifat TMK perlu diberi perhatian namun saranan tersebut diabai Ohki et al. (2009). Justeru, TUKM hendaklah melibatkan semua aspek dalam sesebuah organisasi (Ohki et al., 2009; Solms & Solms, 2009).

Persoalan kajian (PK) yang diutara dalam kajian ini adalah terdiri daripada tiga iaitu:

PK1: Mengapakah sektor awam di Malaysia perlu kepada kerangka tadbir urus keselamatan maklumat?

PK2: Adakah kerangka tadbir urus keselamatan maklumat dalam sektor awam Malaysia bersepadu?

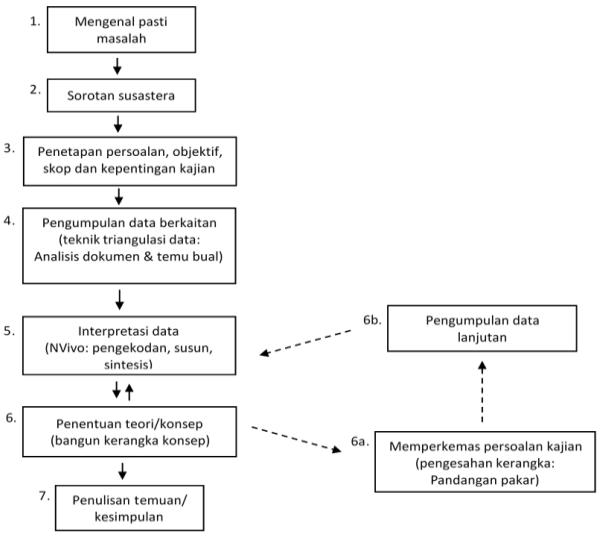
PK3: Adakah komponen kerangka tadbir urus keselamaatn maklumat dalam sektor awam perlu bersifat menyeluruh?

KAEDAH KAJIAN

Kajian ini mengguna reka bentuk kajian kualitatif dan kajian kes sebagai strategi kajian. Teknik pengumpulan data yang diguna ialah analisis kandungan dokumen dan temu bual soalan terbuka. Data yang dikumpul daripada kedua-dua teknik kemudiannya dianalisis mengguna kaedah induktif. Kaedah induktif memboleh penyelidik membuat tafsiran pengertian kajian dengan struktur yang fleksibel (Creswell, 2014; Silverman, 2011).

Justifikasi pemilihan reka bentuk kajian adalah untuk membincang motif asas mengapa kajian kualitatif sesuai dilaksana dalam kajian ini. Sorotan susastera mendapati tidak terdapat kajian tentang TUKM dalam sektor awam baik di Malaysia mahupun pada peringkat global. Oleh itu, bagi bidang yang belum diteroka, maka kaedah kajian berbentuk penerokaan adalah pilihan yang tepat (Connaway & Powell, 2010; Mokmin et al., 2013). Kajian yang menjurus kepada sektor awam Malaysia pula adalah sesuai mengguna strategi kajian berbentuk kajian kes.

Kajian berbentuk pendekatan kualitatif diguna dalam kajian ini berdasarkan persoalan kajian, populasi sampel yang terhad dan reka bentuk kajian tabii dalam keselamatan maklumat. Pendekatan kajian secara kualitatif yang dicadang diadaptasi daripada Creswell (2014) yang melibatkan tujuh langkah. Reka bentuk kajian ini adalah seperti dalam Rajah 3 dan Jadual 1.



Sumber: (Creswell, 2014)

RAJAH 3. Reka Bentuk Kajian

JADUAL 1. Reka Bentuk Kajian

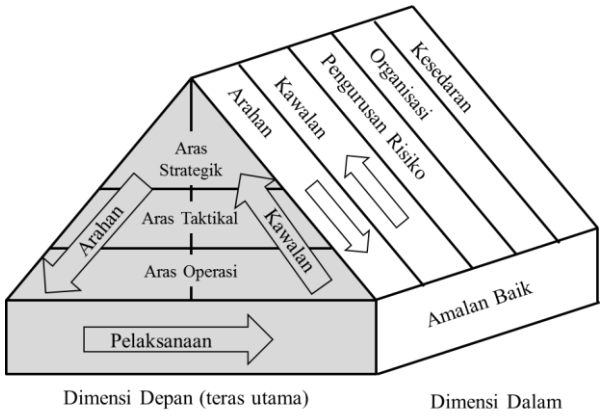
Reka bentuk Kajian	Strategi Kajian Kualitatif	Teknik Kajian	Responden/Sampel
Kualitatif	Kajian Kes (sektor awam Malaysia)	Temu bual dan analisis dokumen	Temu bual: 7 orang berpengalaman dalam bidang kajian Analisis dokumen: Dokumen yang diperoleh semasa temu bual dan dalam talian

Kajian ini bermula dengan mengenal pasti masalah daripada pengkaji lampau dalam bidang TUKM. Aktiviti sorotan susastera dilaku bagi mendapat maklumat dan gambaran berkaitan masalah tersebut. Seterusnya persoalan, objektif, skop dan kepentingan kajian

dikenalpasti. Kombinasi teknik iaitu analisis kandungan dokumen dan temu bual dipilih (Creswell, 2014) bagi memasti data yang dikutip boleh dipercayai dan dapat memberi gambaran yang jelas tentang teori dan amalan dalam bidang yang dikaji.

Analisis ke atas model kerangka keselamatan maklumat terdahulu dilaksana bagi menetapkan model yang akan diguna. Enam buah kerangka keselamatan maklumat yang dikaji ialah model Posthumus & Solms (2004), Roux, 2007, Veiga & Eloff (2010), Solms & Solms (2009), Ohki et al. (2009), dan Ahmad (2010). Berdasar enam buah model kerangka TUKM yang dikaji, model Solms dan Solms (2009) mempunyai kerangka TUKM lengkap serta menyeluruh berbanding dengan model yang lain. Menurut Solms dan Solms (2009) berdasarkan amalan baik serta pengalaman dalam bidang keselamatan maklumat, keselamatan maklumat adalah displin pelbagai dimensi yang meliputi aspek strategi, taktikal dan operasi.

Menurut Solms dan Solms (2009) tidak terdapat satu pendekatan tunggal bagi keselamatan maklumat. Ini bermaksud keselamatan maklumat hanya boleh dicapai sekiranya organisasi melaksana semua dimensi secara holistik dan komprehensif. Walaupun, Solms dan Solms (2009) membahagi tadbir urus kepada lima belas dimensi disiplin, namun model teras TUKM mempunyai dua dimensi sahaja iaitu dimensi depan dan dimensi dalam seperti Rajah 4.



Sumber: (Solms & Solms, 2009)
RAJAH 4. Model Solms dan Solms

Dimensi depan dibahagi kepada tiga aras pengurusan iaitu aras pengurusan strategik, taktikal dan operasi. Aras strategik terdiri daripada pengurusan tertinggi dalam sesebuah organisasi bagi menggubal dasar TUKM, mengarah pengurusan peringkat taktikal serta mengawal pelaksanaan inisiatif TUKM. Manakala aras pengurusan taktikal mengarah pengurusan peringkat operasi bagi melaksana program dan prosedur TUKM.

Dimensi dalam adalah sebagai teras utama dimensi depan. Dimensi dalam mengguna pendekatan amalan baik sebagai kaedah pelaksanaan menerusi pendekatan mengarah, mengawal, pengurusan risiko, organisasi dan kesedaran. Komponen kerangka TUKM dalam model Solms dan Solms (2009) adalah Pendekatan tadbir urus, Amalan baik, Pengurusan risiko, Pengurusan Organisasi, Latihan dan kesedaran, Metod pelaksanaan, Undang-undang dan peraturan.

Sampel kajian yang dipilih terdiri daripada empat (4) buah agensi pusat yang berperanan membuat dasar. Agensi tersebut adalah seperti berikut:

1. Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)

2. Pejabat Ketua Pegawai Keselamatan Kerajaan (KPKK)
3. Jabatan Arkib Negara (ANM)
4. Kementerian Sains, Teknologi dan Inovasi (MOSTI)

Justifikasi pemilihan empat (4) buah agensi kerajaan sebagai sampel kajian adalah kerana agensi berkaitan merupakan agensi yang mengeluar dasar dan peraturan untuk agensi sektor awam di Malaysia.

ANALISIS DAN INTERPRETASI DATA

A. Analisis Kandungan Dokumen

Analisis tiga dokumen dasar dan garis panduan sektor awam dengan komponen Solms dan Solms (2009) adalah seperti Jadual 2.

JADUAL 2. Analisis Kandungan Dokumen

Bil.	Komponen Solms & Solms	Dokumen Arahan Keselamatan	Dokumen Rekod Elektronik & Akta Arkib Negara	Dokumen RAKKSSA
1	Pendekatan tadbir urus	√	√	√
2	Amalan baik	√	√	√
3	Pengurusan risiko	x	x	√
4	Pengurusan Organisasi	√	√	√
5	Latihan dan kesedaran	√	√	√
6	Metod laksana	x	x	x
7	Undang-undang & peraturan	√	√	√
	Jumlah	5	5	6

Dapatan analisis dokumen (Jadual 2) antara komponen Solms dan Solms (2009) dengan Arahan Keselamatan (Jabatan Perdana Menteri, 1985) serta Rekod Elektronik dan Akta Arkib Negara (2011) mendapati sebanyak 71% dokumen ini mempunyai komponen tadbir urus seperti komponen Solms dan Solms (2009). Manakala analisis dokumen antara komponen Solms dan Solms (2009) dengan Rangka Kerja Keselamatan Siber Sektor Awam (MAMPU, 2016) mendapati sebanyak 85% dokumen ini mempunyai komponen tadbir urus seperti komponen Solms & Solms (2009). Walaupun ketiga-tiga dokumen polisi dan garis panduan mempunyai komponen tadbir urus keselamatan maklumat, namun ciri-ciri tadbir urus keselamatan yang lengkap seperti yang disaran Solms dan Solms (2009) tidak ditemui. Setiap dokumen memapar pendekatan tadbir urus yang berbeza.

Dapatan ini bermakna dasar TUKM wujud dalam beberapa dokumen secara terpisah-pisah serta mengguna pendekatan yang berbeza-beza. Meskipun analisis mendapati terdapat satu dokumen dasar berkaitan dengan TUKM namun dokumen tersebut tidak menyentuh tentang keselamatan maklumat secara eksplisit. Dokumen dalam bentuk pekeliling yang dikeluarkan oleh MAMPU hanya memberi tumpuan kepada keselamatan TMK atau ruang siber sahaja (MAMPU, 2016).

Sehubungan dengan itu, tadbir urus keselamatan maklumat di bawah polisi RAKKSSA adalah bertumpu kepada ruang siber sahaja. Tabdir urus keselamatan maklumat seharusnya adalah menyeluruh meliputi ruang bukan siber seperti yang disaran oleh Ohki et al. (2009) dan Solms & Solms (2009). Justeru, sektor awam mempunyai dasar tadbir urus keselamatan maklumat, namun pelaksanaan inisiatif tersebut mengguna pendekatan yang pelbagai dan tidak seragam. Pendekatan tadbir urus yang tidak seragam menyebab agensi yang melaksana dasar mengguna pendekatan tadbir urus yang tidak generik.

Setiap dokumen dasar mempunyai pendekatan tadbir urus yang tersendiri. Sebagai contoh, elemen dalam dokumen dasar keselamatan TMK tidak ditemui dalam dasar pengurusan rekod dan arkib eletronik.

B. Analisis Temu Bual

Analisis data temu bual ke atas tujuh orang responden mendapati maklumat merupakan aset yang penting kepada organisasi khususnya sektor awam. Ini mengesah bahawa pegawai kanan kerajaan menyedari bahawa maklumat merupakan satu aset yang perlu diberi perhatian dan perlindungan yang sewajarnya.

Penemuan ini adalah selari dengan kajian (Suhazimah & Ali, 2012). Bagi melindungi maklumat, aset ini perlu ditadbir urus berdasarkan peruntukan undang-undang, dasar dan pekeliling yang dikeluar oleh MAMPU, KPKK dan ANM. Analisis data temu bual juga mengesah bahawa kerangka menyeluruh TUKM yang melibatkan TMK dan bukan TMK bagi sektor awam Malaysia belum wujud. Jadual 3 menggambar hasil temu bual ke atas tujuh orang responden.

JADUAL 3. Hasil Temu Bual

Bilangan	Jabatan	Responden	Soalan temu bual : Kerangka menyeluruh TUKM dalam Sektor Awam di Malaysia belum wujud.
1.	MAMPU	Responden 1	Ya
		Responden 2	Ya
2.	KPKK	Responden 3	Ya
3.	ANM	Responden 4	Ya
		Responden 5	Ya
4.	MOSTI	Responden 6	Ya
		Responden 7	Ya

Analisis data ini mendapati sektor awam di Malaysia tidak mempunyai garis panduan tentang tadbir urus maklumat dalam satu dokumen tunggal dan bersepadu. Ini menyukar pelaksanaan inisiatif tersebut. Justeru, satu kerangka TUKM dalam sektor awam perlu digubal. Penggubalan ini dapat memudah pengurusan atasan mengatur strategi pelaksanaan keselamatan maklumat yang merentasi keselamatan maklumat TMK dan bukan TMK.

C. Rumusan Analisis Data

Berdasarkan kepada analisis kandungan dokumen dan temu bual di rumus bagi menjawab persoalan kajian seperti berikut:

PK1: Mengapakah sektor awam di Malaysia perlu kepada kerangka tadbir urus keselamatan maklumat?

PK2: Adakah kerangka tadbir urus keselamatan maklumat dalam sektor awam Malaysia bersepadu?

PK3: Adakah komponen kerangka tadbir urus keselamaatn maklumat dalam sektor awam perlu bersifat menyeluruh?

Data-data yang dikumpul di analisis mengguna teknik triangulasi data seperti rumusan analisis di Jadual IV.

JADUAL 4. Rumusan Analisis

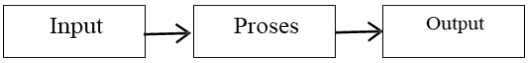
Persoalan Kajian	Analisis kandungan dokumen	Analisis temu bual
PK1	Perlu	Perlu
PK2	Tidak	Tidak
PK3	Ya	Ya

Jadual IV merumus bahawa bagi persoalan kajian pertama (PK1) sektor awam di Malaysia perlu sebuah kerangka TUKM supaya menjadi rujukan utama perlaksanaan TUKM dalam agensi kerajaan. Bagi persoalan kajian kedua (PK2), analisis berdasarkan komponen kerangka tadbir urus wujud dalam dokumen yang dikaji, namun komponen tadbir urus tersebut terpisah dan tidak bersepadu. TUKM terdapat dalam dokumen yang dikeluarkan oleh agensi kerajaan yang berbeza. Analisis temu bual turut menyokong bahawa TUKM adalah tidak bersepadu kerana wujud berapa agensi bagi TUKM dalam kerajaan.

Bagi persoalan kajian ke tiga (PK3), berdasarkan analisis kandungan dokumen dan temu bual mengesah bahawa kerangka TUKM dalam sektor awam di Malaysia perlu bersifat menyeluruh.

CADANGAN KERANGKA TUKM SEKTOR AWAM

Pembangunan sesebuah kerangka lazimnya mempunyai tiga fasa iaitu *input*, proses dan *output.* Kerangka TUKM sektor awam dibangun dengan mengguna pendekatan yang diguna pakai oleh Lin (2007), Fadillah et al. (2011) dan Mohd Bakhari et al. (2013). Pendekatan tersebut adalah seperti dalam Rajah 5.



RAJAH 5. Fasa Pembangunan Kerangka Tadbir Urus
Sumber: Lin (2007), Fadillah et al. (2011), Mohd Bakhari et al. (2013)

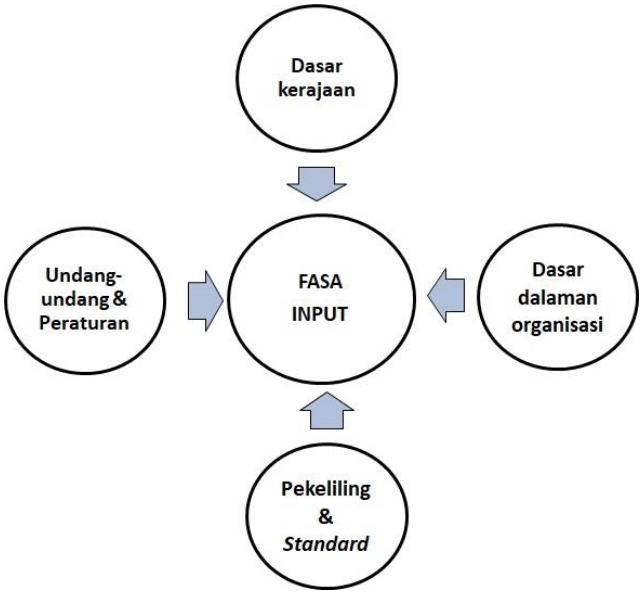
Cadangan Kerangka TUKM sektor awam Malaysia adalah seperti Rajah 6:

INPUT +	→	**PROSES**	→	**+ OUTPUT**	→	Inisiatif
Dasar Kerajaan		Pendekatan tadbir urus		Kerangka TUKM sektor awam		TUKM sektor awam
Dasar dalaman organisasi		Amalan baik				
Pekeliling & piawaian		Pengurusan risiko				
Undang-undang & peraturan		Pengurusan organisasi				
		Latihan & kesedaran				
		Metod pelaksanaan				
		Undang-undang & peraturan				

RAJAH 6. Cadangan Kerangka TUKM Sektor Awam

FASA INPUT

Rajah 6 menggambar fasa input adalah fasa pertama dalam pembangunan sebuah kerangka. Fasa ini penting kerana pembangunan kerangka melibatkan pengumpulan dokumen dan membuat analisis dokumen dasar dan garis panduan yang berkaitan. Input dasar dan garis panduan juga perlu mengambil kira persekitaran keselamatan maklumat di dalam dan luar skop TMK seperti yang disaran oleh Solms & Solms (2009) dan Ohki et al. (2009). Ini bermakna input bukan sahaja dari dokumen TMK tetapi juga dokumen bukan TMK. Bagi melengkapi aktiviti dalam fasa input, aspek personel, proses dan teknologi diambil kira. Aktiviti fasa input ditunjuk dalam Rajah 7.



RAJAH 7. Fasa Input
Sumber: (Solms & Solms, 2009; MAMPU, 2016)

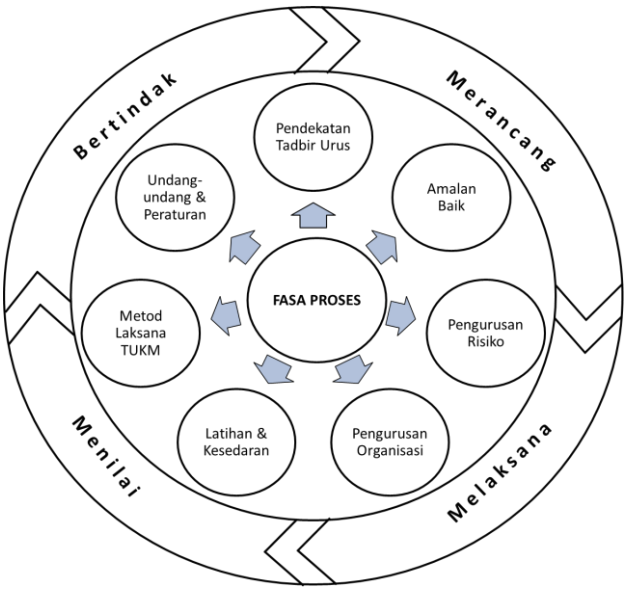
Komponen fasa input diadaptasi dari Solms dan Solms (2009) dan RAKKSSA (MAMPU, 2016). Dalam konteks kajian ini, dasar yang dikaji adalah dari KPKK adalah Arahan Keselamatan yang digubal tahun 1985. Dasar ini merupakan dokumen penting bagi memberi panduan kepada agensi dalam pelaksanaan tadbir urus maklumat. Analisis kandungan dokumen mengenal pasti dasar ini memenuhi 66% komponen yang disaran dalam kajian ini.

Walaupun tidak memenuhi keperluan komponen sebagai sebuah dokumen tadbir urus keselamatan maklumat seperti yang disaran oleh Solms dan Solms (2009), namun dokumen ini membukti KPKK adalah agensi yang diberi peranan bagi memasti maklumat penting kerajaan dikawal dengan baik. Dasar yang dikaji dari ANM adalah sebuah dokumen berkaitan dengan Dasar Pengurusan Rekod dan Arkib Elektronik. Dasar ini digubal pada tahun 2011. Analisis kandungan dokumen mendapati sebanyak 66% daripada kandungan dokumen memenuhi keperluan sebagai sebuah dokumen tadbir urus keselamatan maklumat seperti yang disaran oleh Solms dan Solms (2009). Namun kandungan dokumen ini menjurus kepada maklumat arkib yang kebanyakan maklumatnya adalah untuk tujuan rujukan awam.

Dasar yang dikaji dari MAMPU adalah sebuah dokumen RAKKSSA (MAMPU, 2016) yang digubal pada tahun 2016. Analisis kandungan dokumen mendapati sebanyak 77% daripada kandungan dokumen ini memenuhi keperluan sebagai sebuah dokumen tadbir urus keselamatan maklumat seperti disarankan oleh Solms dan Solms (2009). Namun kandungan rangka dasar ini memberi tumpuan kepada TMK.

FASA PROSES

Rajah 8 menggambarkan fasa proses adalah fasa kedua dalam pembangunan sebuah kerangka tadbir urus. Fasa ini adalah lanjutan dari fasa input bagi menganalisis semua sumber yang diperoleh. Aktiviti analisis sumber berpandu kepada tujuh komponen seperti yang disaran oleh Solms & Solms (2009). Komponen tersebut ialah pendekatan tadbir urus, amalan baik, risio, pengurusan organisasi, latihan dan kesedaran, metod pelaksanaan dan undang-undang dan peraturan.



RAJAH 8. Fasa Proses

Rajah 8 menunjukkan pembangunan kerangka dalam fasa proses. Dalam fasa proses komponen pertama iaitu pendekatan tadbir urus menjelas bahawa sesebuah kerangka perlu mempunyai arahan yang jelas tentang pendekatan yang perlu diguna dalam melaksana tadbir urus. Kajian ini menyaran supaya pendekatan tadbir urus perlu mempunyai elemen seperti peringkat arahan, peringkat pelaksanaan dan kawalan.

Tiga peringkat ini boleh memberi panduan tentang peranan yang perlu ada dalam sesebuah organisasi. Misalnya, pembuat dasar agensi, pelaksanaan oleh pegawai dan personel yang terlibat dan aktiviti kawalan supaya pelaksanaan inisiatif dapat dikaji semula dan dipantau secara berterusan sama ada oleh pengurusan atasan atau unit khas pemantauan.

Bagi komponen kedua iaitu amalan baik, komponen ini merujuk kepada amalan mengguna piawaian keselamatan maklumat. Piawaian ISO/IEC 27001 (2005) iaitu Sistem Pengurusan Keselamatan Maklumat adalah piawaian antarabangsa yang perlu dipatuhi. Walaupun piawaian ini memberi tumpuan kepada teknologi TMK, namun turut boleh diguna dalam persekitaran maklumat yang bukan TMK.Bagi komponen ketiga iaitu pengurusan risiko, komponen ini menjadi syarat wajib dalam piawaian ISO/IEC 27001 (2005). Program pengurusan risiko diperlu bagi memasti ancaman ke atas aset maklumat dan kaedah bagi mengurangi risiko menerusi program perlindungan.

Komponen keempat iaitu Pengurusan organisasi. Komponen ini menggaris keperluan mewujud struktur organisasi dalaman yang mempunyai fungsi khas melaksana program pematuhan kepada tadbir urus. Fungsi khusus dalam tadbir urus ialah dengan mewujud jawatan ketua pegawai maklumat (CIO), pegawai keselamatan jabatan (PKJ) dan Pegawai Keselamatan TMK (PKTMK).

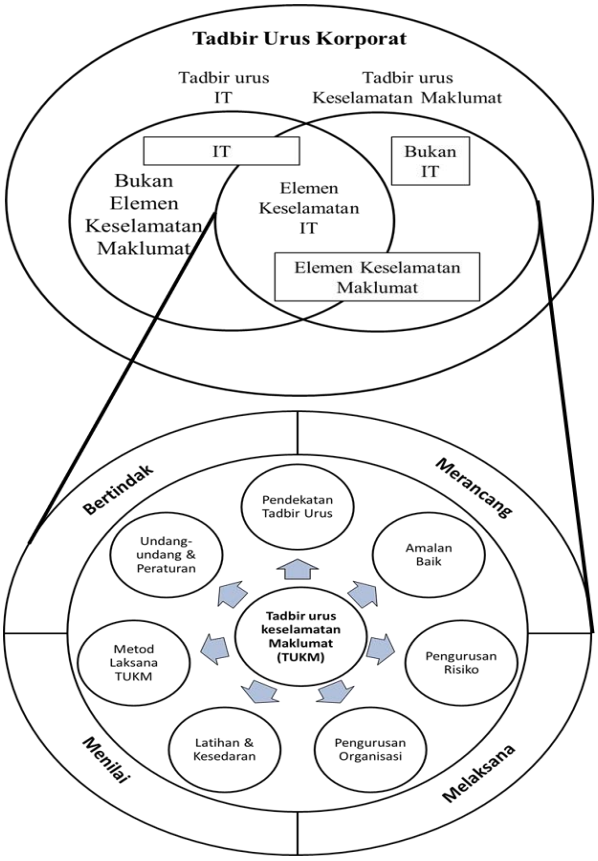
Analisis kandungan dokumen mendapati dasar mewujud jawatan khusus ini dilaksana dalam sektor awam. Kewujudan jawatan khusus ini memboleh tadbir urus keselamatan maklumat dapat dilaksana dengan berkesan. Model yang dicadang telah mendapat pandangan pakar. Pakar menyaran supaya pengurusan organisasi perlu bersifat tindakan. Oleh yang demikian, peranan dan tanggungjawab pengurusan atasan, ketua bahagian, pengurusan kanan dan PKJ dan PKTMK yang jelas dinyata dalam kerangka.

Komponen seterusnya ialah Latihan dan Kesedaran. Program latihan dan kesedaran perlu dilaksana agar personel dalam organisasi menyedari kepentingan tadbir urus maklumat yang baik. Menurut Solms dan Solms (2009) terdapat ancaman dalam organisasi yang perlu diberi perhatian berkaitan dengan keselamatan maklumat. Melalui program latihan dan kesedaran yang berterusan boleh menerap amalan melindungi maklumat penting organisasi dari mengalami ketirisan atau kebocoran.

Komponen yang seterusnya ialah metod pelaksanaan. Dalam sesebuah dokumen tadbir urus tindakan yang harus dilaksana seperti mendapat pengesahan pelaksanaan dari pengurusan atasan, langkah melaksana tadbir urus, pematuhan kepada undang-undang dan peraturan serta program lain yang berkaitan perlu diperjelas (Solms & Solms, 2009). Kerangka TUKM yang dihasil perlu memenuhi empat (4) ciri iaitu merancang, melaksana, menilai dan bertindak.

FASA OUTPUT

Rajah 9 menggambar fasa output adalah fasa ketiga dalam pembangunan sebuah kerangka. Output adalah berupa hasil terakhir dan utama dalam pembangunan sesebuah kerangka, Output kajian ini adalah hasil kerangka TUKM sektor awam berasaskan kepada kepada komponen Solms & Solms (2009) dan Ohki et al. (2009).



RAJAH 9. Fasa Output

Rajah 9 menggambar bahawa cadangan kerangka TUKM sektor awam dibangun mengambil aspek keselamatan IT dan bukan IT berlandaskan model Ohki at el. (2009) dan model Solms dan Solms (2009).

Kerangka dibangun dengan mengguna pendekatan tiga fasa pembangunan dengan tujuan menghasil dokumen yang komprehensif meliputi semua aspek keselamatan maklumat dalam sesebuah organisasi. Pembangunan kerangka turut mengambil kira dasar dan peraturan sedia ada dalam perkhidmatan awam, adaptasi piawaian keselamatan pengurusan maklumat serta amalan baik pada peringkat antarabangsa supaya dapat membantu meningkat tahap tadbir urus keselamatan maklumat.

KESIMPULAN

Data yang dikumpul melalui analisis dokumen dan temu bual, mengesahkan bahawa TUKM wujud dalam beberapa dokumen sektor awam Malaysia. Namun elemen TUKM tersebut mengguna pendekatan yang berbeza-beza. Meskipun analisis mendapati terdapat satu dasar berkaitan dengan TUKM namun dasar tersebut tidak menyentuh tentang keselamatan maklumat bukan TMK. Sesebuah dasar TUKM tidak lengkap serta pincang apabila elemen keselamatan maklumat TMK dan bukan TMK dipisahkan.

Kajian mencadang satu kerangka TUKM dibangun dengan mengambil kira aspek keselamatan maklumat TMK dan bukan TMK (Ohki et al., 2009). Dengan demikian segala elemen keselamatan maklumat diambil kira seperti yang disaran oleh (Solms et al., 2011). Pembangunan kerangka TUKM adalah program bersepadu melibatkan agensi-agensi pembuat dasar dalam pentadbiran sektor awam di Malaysia. Pembangunan bersepadu dapat menghasil satu kerangka TUKM menyeluruh untuk digunapakai oleh agensi sektor awam di Malaysia.

PENGHARGAAN

Kajian ini dibiayai oleh Geran Penyelidikan GUP-2017-046, Universiti Kebangsaan Malaysia.

RUJUKAN

Ahmad, A. M. 2010. Information security governance in Saudi organizations: an empirical study. *Information Management & Computer Security* 18(4):226-276.

Creswell, J.W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches 4th Edition*. Los Angeles: SAGE Publications, Inc.

Connaway, L.S, & Powell, R.R. 2010. *Basic Research Methods for Librarians 5th Edition*. Santa Barbara: ABC-CLIO, LLC.

Ernst & Young. 2013. *Fighting to close the gap. Year 2012 Global Information Security Survey*. London: EYGM Limited.

Fadillah, Y., Noraidah, S. & Juhana, S. 2011. A Framework of Knowledge Sharing through ICT for Teachers in Malaysia. *Proceedings of the 2011 International Conference on Electrical Engineering and Informatics International Conference on Electrical Engineering and Informatics*. Bandung, Indonesia, 17-19 Julai: 1-5

Hovav, A., & D'Arcy, J. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management & Insurance Review* 6(2):97-121.

ISO/IEC 27001. 2005. *Information Technology – Security Techniques – Information Security Management Systems – Requirements, International Organization for Standardization*. Geneva: ISO copyright office.

Jabatan Perdana Menteri.1985. *Arahan Keselamatan*. Kuala Lumpur: Pejabat Ketua Pegawai Keselamatan Kerajaan.

Kritzingera, E. & Smith, E. 2008. Information security management: An information security retrieval and awareness model for industry. *Computers & Security* 27 (5-6): 224–231.
Lin, H. 2007. Knowledge Sharing and Firm Innovation Capability: An Empirical Study. *International Journal of Manpower* 28(3/4): 315 – 332.
Malaysia. 2011. *Rekod Elektronik dan Akta Arkib Negara*. Kuala Lumpur: Arkib Negara Malaysia.
Mohd Bakhari, I., Zawiyah, M. Y., Kamsuriah, A. & Maryati, M. Y. 2013. *Pengurusan dan Perkongsian Pengetahuan Sektor Awam*. Bangi: Universiti Kebangsaan Malaysia.
Mokmin, B., Zawiyah M.Y. & Nor Azan M.Z. 2013. *Dasar Maklumat Nasional di Malaysia*. Bangi: Universiti Kebangsaan Malaysia.
Ohki, E., Harada, Y., Kawaguchi, S., Shiozaki, T. & Kagaua, T. 2009. Information Security Governance Framework. *WISG '09 Proceedings of the first ACM workshop on Information security governance*. Chicago, USA, 13 November: 1-6.
Posthumus, S., & Solms, R. 2004. A framework for the governance of information security. *Computers & Security* 23(8): 638-646.
Roux, Y.L. 2007. Information Security Governance for Executive Management. *ISSE/SECURE 2007 Securing Electronic Business Processes* :136-146.
Silverman, D. 2011. *Interpreting Qualitative Data 4th Edition*. California: SAGE Publication Ltd.
Solms, B. 2001. Information Security – A Multidimensional Discipline. *Computers & Security* 20(6): 504-508.
Solms, R., Thomson, K.L. & Maninjwa, M. 2011. Information security governance control through comprehensive policy architectures. *Information Security South Africa (ISSA)*. University of Pretoria, University of South Africa & University of Johannesburg, Johannesburg, 15-17
Solms, S.H., & Solms, S.R. 2009. *Information Security Governance*. New York: Springer.
Tassabehji, R. 2005. *Information Security: From evolution to prominence*. Las Vegas: Net Industries, http://encyclopedia.jrank.org/articles/pages/6627/Information-Security-Threats.html [2 April 2014].
Suhazimah, D. & Ali, H.Z. 2012. Assessment of information security maturity: An exploration study of Malaysian public service organizations. *Journal of Systems and Information Technology* 14(1): 23-57.
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). 2016. *Rangka Kerja Keselamatan Siber Sektor Awam (RAKKSSA)*. Putrajaya: Jabatan Perdana Menteri.
Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia. 2000. *Pekeliling Am Bil. 3. Rangka Dasar Keselamatan Teknologi Maklumat dan Komunikasi Kerajaan. Putrajaya: Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia*. Putrajaya: Jabatan Perdana Menteri.
Umi, A. M., & Zawiyah, M.Y. 2009. Electronic records management in the Malaysian public sector: the existence of policy. *Records Management Journal* 19(3): 231-244.
Veiga, A.D. & Eloff, J.H.P. 2010. A framework and assessment instrument for information security culture. *Computers & Security* 29(2): 196-207.
Webb, J. 2008. *Strategic Information Management: A Practitioner's Guide.* Oxford: Chandos Publishing.
Warkentin, M. & Johnson, A.C. 2006. *Information Security Policies and Practices*. New York: M.E. Sharpe.
Zawiyah, M. Y., & Robert, W. C. 2005. *Issues in records management*. Bangi: Universiti Kebangsaan Malaysia.

Amri Jamil
Zawiyah M. Yusof
Faculty of Information Science and Technology,
Universiti Kebangsaan Malaysia
amri@kehakiman.gov.my, zawiy@ukm.edu.my

Received: 13 June 2018
Accepted: 19 August 2018
Published: 26 December 2018