https://doi.org/10.17576/apjitm-2018-0701-09

http://www.ftsm.ukm.my/apjitm
Asia-Pacific Journal of Information Technology and Multimedia
Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik
Vol. 7 No. 1, June 2018: 99 - 117
e-ISSN: 2289-2192

MANAGING DATA SECURITY RISK IN MODEL SOFTWARE AS A SERVICE (SAAS)

NOORAIDANIZA JAFRI
MARYATI MOHD YUSOF

ABSTRACT

Software as a Service (SaaS) model has been frequently applied in organisation that used cloud services. SaaS is a new information technology that provides dynamic services through Internet to the user. Alhough this technology is beneficial and cost-effective for information technology hosting, it also introduced new threats and risks, particularly in user's information security. The paper identifies risk in data security of the SaaS Model and their respective mitigation control based on ISO/IEC 27001:2013 standard. A qualitative case study was conducted at a public sector agency involving three types of data collection, interviews, observations and document analysis. We identified seven risk of data security for SaaS Model namely data privacy, data integrity, data availability, data control, data encryption, data violation, and data access. The findings can be used to develop SaaS implementation guidelines or policies, particularly in data security.

Keywords: Risk management, data security, information security as a Service, SaaS, cloud computing

PENGURUSAN RISIKO KESELAMATAN DATA DALAM MODEL PERISIAN SEBAGAI PERKHIDMATAN (*SOFTWARE AS A SERVICE*)(SAAS)

ABSTRAK

Perisian sebagai Perkhidmatan (*Software as a Service*)(SaaS) merupakan salah satu model perkhidmatan dalam pengkomputeran awan yang paling kerap diguna dalam organisasi. SaaS adalah teknologi maklumat baharu yang menyediakan perkhidmatan secara dinamik kepada pengguna melalui Internet. Walaupun ia memberikan faedah dan pilihan kos yang efektif dalam pengehosan teknologi maklumat, ia memperkenalkan ancaman dan risiko baharu, terutamanya pada keselamatan data/maklumat pengguna. Kertas ini mengenalpasti risiko keselamatan data pada Model SaaS dan penentuan mitigasi berdasarkan kawalan yang bersesuaian mengikut standard ISO/IEC 27001:2013. Kajian kes secara kualitatif dilakukan di sebuah agensi sektor awam melibatkan temu bual, pemerhatian serta analisis dokumen. Tujuh risiko keselamatan data Model SaaS dikenalpasti iaitu iaitu kerahsiaan data, integriti data, ketersediaan data, kawalan data, enkripsi data, pelanggaran data dan capaian data. Dapatan kajian boleh diguna untuk membangunkan garis panduan atau polisi pelaksanaan SaaS khususnya dalam aspek keselamatan data.

Kata kunci: Pengurusan Risiko, Keselamatan Data, Keselamatan Maklumat, Model Perisian Sebagai Perkhidmatan, SaaS, Pengkomputeran Awan

PENGENALAN

Pengkomputeran awan diguna pakai oleh ramai individu dan organisasi untuk perkhidmatan yang cepat dan fleksibel, bayaran ke atas perkhidmatan yang diguna sahaja dan capaian melalui infrastruktur rangkaian. Faedah pengkomputeran awan termasuk pengurangan kos, keluwesan, kapasiti penggunaan dan kecekapan yang tinggi dan mobiliti. Pengkomputeran awan berasaskan internet membolehkan perkongsian sumber, perisian dan capaian maklumat disedia secara dalam talian. Pengkomputeran awan menjadi pusat sehenti bagi agensi Sektor Awam

mencapai pelbagai perkhidmatan yang disedia seperti Perisian sebagai Perkhidmatan (*Software as a Service* - SaaS), Platform sebagai Perkhidmatan (*Platform as a Service* - PaaS) dan Infrastruktur sebagai Perkhidmatan (*Infrastructure as a Service* - IaaS) (Unit Perancang Ekonomi, 2015). Perisian sebagai Perkhidmatan (SaaS) merupakan salah satu model perkhidmatan dalam pengkomputeran awan yang paling kerap diguna dalam organisasi. Pengguna awan boleh mengakses perisian melalui pelayar web tanpa terlibat dengan pembangunan, pemasangan dan penyelenggaraan perisian tersebut. Aplikasi SaaS dikenali sebagai perisian berasaskan web, perisian atas permintaan atau perisian *hosted*. Pembekal awan bertanggungjawab menjamin keselamatan, ketersediaan dan prestasi pada aplikasinya (Kumar 2014).

SaaS adalah sebahagian daripada anjakan paradigma ke arah pengkomputeran awan dalam perisian, perkakasan, dan perkhidmatan perolehan Teknologi Maklumat (IT). Walaupun ia memberikan faedah yang baik dan pilihan kos yang efektif dalam perkembangan pengehosan IT, namun wujud risiko baharu dan peluang untuk keselamatan dieksploitasi. Penggunaan SaaS menimbulkan isu keselamatan data dan integriti data kerana ia melibatkan interaksi dan perkongsian dengan ramai pengguna awan. Antara risiko utama SaaS ialah keselamatan data/ maklumat pengguna (Singh & Shaterjee, 2017; Hepsiba, 2016). Bagi mengurangkan kesan kebimbangan terhadap isu ini, pengenalpastian dan pengurangan risiko penting dalam memastikan keselamatan penggunaan perkhidmatan SaaS. Pihak pengurusan perlu memahami dan menganalisis risiko pengkomputeran awan bagi mengelakkan keselamatan data dan sistem organisasi dieksploitasi oleh pihak yang tidak bertanggungjawab. Kertas ini mengenalpasti risiko keselamatan data dalam Model SaaS, penentuan mitigasi berdasarkan kawalan yang bersesuaian mengikut standard ISO/IEC 27001:2013 dan dapatan penilaian kajian kes di sebuah sektor awam

RISIKO KESELAMATAN DATA

Terdapat pelbagai risiko yang terlibat semasa menghantar maklumat sensitif melalui penggunaan perkhidmatan SaaS. Konsep pengurusan risiko dijelaskan bagi memahami kepentingan pengurusan risiko SaaS,. Risiko ditakrif sebagai kebarangkalian dan impak sesuatu insiden yang berpunca dari kelemahan dan ancaman yang dikenal pasti. Pengurusan risiko adalah proses mengenal pasti risiko, menilai risiko dan mengambil langkah-langkah yang betul untuk mengurangkan risiko ke tahap yang boleh diterima.

Menurut Tang et al. (2015), 49% daripada informan menyatakan isu privasi data merupakan isu keselamatan yang utama dalam Model SaaS. Ini diikuti oleh isu pematuhan (17%) dan enam isu lain yang berkaitan dengan kawalan capaian, ketelusan, kepercayaan, penglihatan (*visibility*), tanggungjawab dan tindak balas insiden. Privasi data merujuk kepada bagaimana data/maklumat pengguna dilindungi pada setiap masa bagi mengekalkan kepercayaan dan keyakinan pengguna terhadap produk dan perkhidmatan SaaS. Privasi data melibatkan kerahsiaan, ketersediaan dan integriti sesuatu data/maklumat.

Terdapat pelbagai kajian berkaitan isu model perkhidmatan SaaS sama ada secara am atau perspektif tertentu. Jadual 1 menyenaraikan isu utama dalam Model SaaS berdasarkan kajian terdahulu iaitu keselamatan data, keselamatan rangkaian, penempatan data, keselamatan aplikasi web, pengasingan data, pelanggaran data, pengurusan identiti, salinan pendua, pelbagai-penyewaan, pelupusan data dan Perjanjian Tahap Perkhidmatan. Berdasarkan Jadual 1, isu keselamatan data merupakan isu yang kerap dibincang diikuti dengan isu keselamatan rangkaian, penempatan data dan keselamatan aplikasi web. Ini adalah kerana dalam Model SaaS, pelanggan bergantung kepada pembekal perkhidmatan untuk memastikan langkah-langkah keselamatan diberi perhatian pada sistem mereka (Fan & Chen 2012).

JADUAL 1. Perbandingan Isu Utama dalam SaaS Berdasarkan Kajian Terdahulu

Isu-isu	**Sumber**									
	Singh & Chatterjee (2017)	Pharkkavi et al (2016)	Hepsiba (2016)	Bahekar (2016)	Thakare (2016)	Ahire et al (2015)	Abbas et al (2015)	Kaur et al (2015)	Chouhan et al (2015)	Soofi et al (2014)
Keselamatan Data • Integriti Data • Kerahsiaan Data • Ketersediaan Data	√	√	√	√	√		√	√	√	√
Keselamatan Rangkaian	√	√	√			√		√		√
Penempatan Data	√	√	√					√		
Keselamatan Aplikasi Web		√		√					√	√
Pengasingan Data	√							√		
Pelanggaran Data		√								√
Pengurusan Identiti	√	√								
Salinan pendua *(Backup)*		√								√
Pelbagai-Penyewaan				√						
Pelupusan Data			√							

Kajian ini menumpu kepada risiko keselamatan data pada Model SaaS kerana ia merupakan risiko yang kritikal (Kaur & Singh 2015). Keselamatan data merujuk kepada kerahsiaan, integriti dan ketersediaan. Kerahsiaan melindungi data sensitif dari individu yang tidak dibenarkan. Maklumat tidak boleh didedah sewenang-wenangnya atau dicapai tanpa kebenaran. Integriti merujuk kepada data dan maklumat yang tepat, lengkap dan terkini. Ia hanya boleh diubah dengan cara yang dibenarkan. Ketersediaan bermaksud data dan maklumat boleh dicapai pada bila-bila masa. Perkhidmatan SaaS yang selamat diperlukan untuk melindungi identiti pengguna, data dan pelayan privasi data kerana data boleh dicuri semasa penghantaran dan penyimpanan dalam pelayan (Aich et al. 2015).

Kitaran hayat data terdiri daripada fasa penjanaan, penyimpanan, penggunaan data, penghantaran data dan penghapusan data. Setiap pembekal awan harus menyokong semua fasa melalui mekanisma keselamatan yang sesuai (BSI 2011). Data pelanggan dalam SaaS biasanya disimpan dalam lokasi yang sama. Perbezaan antara pelanggan ~~dibeza~~ adalah melalui penggunaan ID yang biasanya dipanggil sebagai ID penyewa. Jika web aplikasi menggunakan program yang tidak selamat, pelanggan boleh menggunakan ancaman *SQL Injection* untuk mendapatkan capaian yang tidak dibenarkan untuk mendapatkan data pelanggan, menghapuskan atau memanipulasi data tersebut tanpa kebenaran (BSI 2011).

Menurut Peake (2012), keselamatan awan bukan sahaja perlu menjamin capaian maklumat dan ketersediaan, ia juga perlu menyediakan integriti dan kerahsiaan data yang

disimpan di dalam awan untuk memastikan operasi perkhidmatan yang berkesan. Keselamatan dan perlindungan data sangat penting bagi pembekal SaaS dan pengguna. Pembekal SaaS bertanggungjawab untuk melindungi dan menyediakan data dengan selamat dan mengikut undang-undang (Kumar 2014). Manakala pengguna SaaS perlu memastikan bahawa pembekal peralatan perlindungan data dan proses memenuhi piawaian organisasi bagi mengurangkan risiko pelanggaran peraturan keselamatan.

Menurut Munir (2013) pula, data boleh dikompromi melalui banyak cara termasuk manipulasi, penghapusan dan pengubahsuaian data. Oleh kerana sifatnya yang dinamik dan dikongsi dalam awan, ancaman merupakan risiko utama dalam kecurian data. Ancaman berlaku disebabkan oleh kelemahan pengesahan, kebenaran dan kawalan audit, kelemahan fungsi enkripsi, pusat data yang tidak boleh dipercayai dan kelemahan pemulihan bencana.

Selain itu, risiko ketersediaan data adalah bagaimana menentukan keutamaan pelanggan pada awan apabila had penggunaan dicapai. Jika kapasiti penggunaan mencapai had 80% dan menjejaskan sebahagian perkhidmatan atau prestasi yang diperlukan, pembekal awan lebih mengutamakan perkhidmatanya sendiri dan menurunkan prestasi perkhidmatan pelanggannya (Paquette et al. 2010). Risiko ini sekali lagi menunjukkan bahawa pelanggan perlu memahami keupayaan awan dan bagaimana akaun mereka diurus. Kebimbangan terhadap keselamatan data dan ketidakupayaan penyelesaian SaaS untuk memenuhi keperluan teknikal dan sokongan pelanggan merupakan salah satu punca organisasi menghentikan penggunaan SaaS (Heiser 2009).

Ketersediaan aplikasi SaaS bergantung kepada ketersediaan dan kebolehpercayaan rangkaian. Bagi Model SaaS, kebolehpercayaan rangkaian tidak boleh dijamin oleh kedua-dua pelanggan awan atau pembekal awan kerana Internet tidak berada di bawah kawalan kedua-duanya (NIST, 2012). Dalam Model SaaS, data sensitif diperolehi daripada organisasi, diproses oleh aplikasi SaaS dan disimpan dalam persekitaran awan pembekal SaaS. Aliran data yang melalui rangkaian perlu dipastikan selamat bagi mengelakkan kebocoran maklumat sensitif. Ini melibatkan penggunaan teknik enkripsi trafik rangkaian yang kukuh seperti *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) bagi tujuan keselamatan (Rashmi et al. 2013). Namun begitu, walaupun aspek keselamatan mampu ditangani, pengguna yang berniat jahat masih boleh mengeksploitasi kelemahan yang ada dalam konfigurasi rangkaian untuk mendapatkan data sensitif.

Menurut Bishnoi dan Sehrawat (2013), capaian melalui rangkaian awam dan perkhidmatan yang dihos meningkatkan pendedahan perisian kepada lebih banyak risiko. Hak capaian istimewa perlu diberi kepada pengguna yang perlu sahaja dan perlu dipantau secara berkala. Pengurusan identiti (IdM) atau pengurusan ID boleh mengenal pasti individu dalam sistem dan mengawal capaian kepada sumber sistem dengan menetapkan sekatan ke atas identiti yang ditetapkan. Tugas ini dianggap sebagai salah satu cabaran terbesar dalam keselamatan maklumat kerana pembekal SaaS perlu tahu mengawal pengguna, had capaian dan sistem organisasi (Rashmi et al. 2013). Sekiranya tugas ini diambil mudah, kebarangkalian berlakunya kecurian maklumat adalah tinggi dan memberi risiko kepada pelanggan lain.

Dalam Model SaaS, pelanggan bergantung sepenuhnya kepada pembekal perkhidmatan. Pelanggan tidak boleh mencapai perisian atau perkakasan dan perkhidmatan yang diguna secara langsung. Pelanggan hanya berupaya untuk memantau ketersediaan perkhidmatan yang diguna melalui antara muka web atau *Application Programming Interface* (API) yang disedia oleh pembekal perkhidmatan. Oleh itu, pengguna memberi sepenuh kepercayaan kepada pembekal perkhidmatan dan secara tidak langsung, isu seperti kehilangan data, data tidak dapat dipulih dan disalah guna oleh pembekal perkhidmatan (Mosco 2014). Senarai risiko keselamatan data Model SaaS disenaraikan pada Jadual 2:

JADUAL 2. Ringkasan Risiko Keselamatan Data dalam Model SaaS

Risiko	Perincian Risiko
Kerahsiaan Data	▪ Capaian yang tidak dibenarkan
Integriti Data	▪ Ancaman kelemahan pada aplikasi ▪ Data boleh dimanipulasi, diubah atau dihapus oleh pengguna yang tidak sah
Ketersediaan Data	▪ Kelemahan prosedur pemulihan data ▪ Aplikasi yang disedia oleh penyedia perkhidmatan tidak berfungsi ▪ Prestasi rangkaian perlahan kerana terlalu bergantung kepada internet sebagai medium utama untuk menyimpan data /menggunakan aplikasi
Kawalan Data	▪ Tiada kawalan ke atas data dan aplikasi seperti kecurian identiti dan jenayah siber ▪ Penyalahgunaan Id pelanggan perkhidmatan ▪ Kakitangan tidak kompeten
Enkripsi Data	▪ Penggunaan enkripsi yang tidak memadai oleh penyedia perkhidmatan ▪ Perlindungan yang tidak efektif semasa pemindahan data
Pelanggaran Data	▪ Penyalahgunaan Id pelanggan perkhidmatan ▪ Serangan ke atas maklumat pelanggan lain dalam awan
Capaian Data	▪ Pencerobohan data oleh pengguna yang tidak dibenarkan ▪ Capaian yang tidak dibenarkan

PENGURUSAN RISIKO KESELAMATAN DATA

Terdapat pelbagai risiko dalam penghantaran maklumat sensitif melalui perkhidmatan SaaS. Untuk memahami kepentingan pengurusan risiko SaaS, konsep pengurusan risiko ditakrif. Merujuk Rangka Kerja Keselamatan Siber Sektor Awam (MAMPU 2016), risiko merupakan kebarangkalian dan impak sesuatu insiden berlaku berpunca daripada kelemahan dan ancaman yang dikenal pasti. Secara umumnya, pengurusan risiko merupakan proses mengurus risiko yang berpotensi dengan mengenal pasti, menganalisis dan menangani risiko tersebut. Merujuk kepada dokumen standard ISO/IEC 27005 (2011), pengurusan risiko melibatkan dua proses utama iaitu penilaian dan rawatan risiko. Penilaian risiko merangkumi proses pengenalpastian risiko, analisis risiko dan menilai risiko yang ditakrif sebagai:

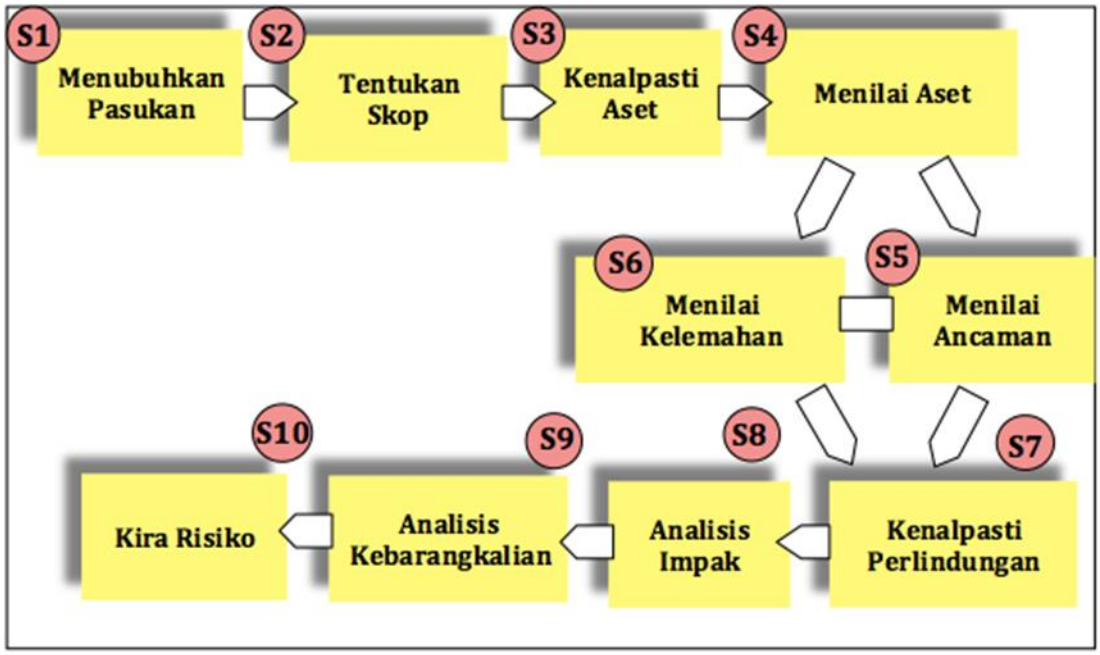
1. Pengenalpastian risiko - proses mencari, mengenal pasti dan menerangkan risiko.
2. Analisis risiko - menilai kebarangkalian risiko bagi setiap risiko yang dikenal pasti.
3. Menilai risiko - membandingkan risiko yang dikenal pasti berdasarkan kriteria risiko yang ditetapkan untuk menentukan kepentingan risiko.

Rawatan risiko melibatkan proses perancangan pengurusan risiko, penyelesaian risiko dan pemantauan risiko. Antara rangka kerja yang diguna dalam melaksanakan penilaian risiko berasaskan persekitaran pengkomputeran awan adalah Rangka Kerja Pengurusan Risiko Enterpris oleh *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) dan rangka kerja risiko bagi domain IT, amalan dan model proses seperti ISO 27001 dan ITIL (Cole 2012). Garis panduan khusus bagi pengkomputeran awan juga wujud dari pelbagai organisasi seperti *Cloud Security Alliance* (CSA), *European Network and Information Security Agency* (ENISA) dan *National Institute of Standards and Technology* (NIST) (Gadia 2011; Al-Musawi et al. 2015). Kajian ini mengaplikasi gabungan metod *The Malaysian Public Sector Information Security Risk Assessment* (MyRAM) dan dokumen standard ISO/IEC 27001

(2013) untuk mengenal pasti risiko dan mitigasi pada Model SaaS. Metodologi MyRAM adalah sangat relevan dan bersesuaian untuk mengenal pasti dan menilai risiko dalam keselamatan maklumat manakala ISO/IEC 27001 merupakan standard antarabangsa amalan terbaik bagi ISMS.

PENILAIAN RISIKO KESELAMATAN MAKLUMAT SEKTOR AWAM MALAYSIA (THE MALAYSIAN PUBLIC SECTOR INFORMATION SECURITY RISK ASSESSMENT - MYRAM)

MyRAM merupakan metodologi penilaian risiko terhadap aset iaitu perkakasan, perisian, data/maklumat, sumber manusia dan perkhidmatan. Ia menyediakan kaedah bagi melaksanakan penilaian risiko terperinci secara kualitatif terhadap aset ICT seperti ancaman, kelemahan, impak dan kemungkinan berlaku musibah bagi setiap aset dalam skop yang dipersetujui. Metodologi MyRAM dibangun dan disesuai daripada metodologi penilaian risiko antarabangsa iaitu German Baseline, ISO/IEC 27000 series dan menepati keperluan standard baharu pensijilan ISMS ISO/IEC 27001:2013. Pendekatan proses penilaian risiko yang diguna oleh MyRAM melibatkan sepuluh langkah aktiviti (Rajah 1) yang mana setiap aktiviti berhubung antara satu sama lain. Aktiviti tersebut dijelaskan dalam Jadual 3.



RAJAH 1. Proses Penilaian Risiko (MAMPU 2005)

Lima proses yang dikenal pasti mempunyai kesan secara langsung terhadap penentuan risiko iaitu 1) Tentukan Skop; 2) Kenal Pasti Aset; 3) Analisis Impak; 4) Analisis Kebarangkalian; dan 5) Kira Risiko. Proses ini merupakan sebahagian daripada sepuluh proses keseluruhan pengurusan risiko seperti yang dinyata dalam dokumen MyRAM dan Jadual 3.

JADUAL 3. Aktiviti Proses Penilaian Risiko

Langkah	Aktiviti Terlibat
Menubuhkan Pasukan	▪ Tentukan ahli pasukan MyRAM yang terlibat ▪ Tentukan peranan dan tanggungjawab ahli pasukan, struktur organisasi pasukan dan jadual pelaksanaan MyRAM

Langkah	Aktiviti Terlibat
Tentukan Skop	▪ Kenal pasti sempadan skop MyRAM yang sesuai dan wajar ▪ Kenal pasti maklumat aset ICT dalam skop MyRAM ▪ Dapatkan persetujuan dan kelulusan daripada pengurusan kanan
Kenal pasti Aset	▪ Kenal pasti aset yang berkaitan ▪ Kenal pasti penjaga dan pemilik aset ▪ Kaedah pengumpulan aset menggunakan soal selidik
Menilai Aset	▪ Memberikan nilai kepada aset berdasarkan nilai tertinggi bagi setiap aspek Kerahsiaan, Integriti dan Ketersediaan
Menilai Ancaman	▪ Menentukan ancaman umum iaitu senarai ancaman yang berkemungkinan besar akan berlaku disebabkan kurang/tiada langkah pengukuhan semasa ▪ Padankan ancaman yang berkaitan kepada setiap aset
Menilai Kelemahan	▪ Menentukan kelemahan sedia ada pada aset yang berkemungkinan besar akan menyebabkan ancaman berlaku ▪ Padankan kelemahan kepada setiap ancaman pada aset
Kenal pasti Perlindungan	▪ Menentukan langkah pengukuhan sedia ada dan yang dirancang (telah ada peruntukan/kajian) bagi setiap aset ▪ Langkah pengukuhan yang hendak dilaksana adalah mengikut: o Kawalan standard ISO/IEC 27001:2013; o Klausa 4 -10 standard ISO/IEC 27001:2013; atau o Lain-lain kawalan yang berkaitan (Contoh MyMIS) ▪ Padankan langkah pengukuhan kepada setiap ancaman pada asset
Analisis Impak	▪ Menentukan impak kepada organisasi jika aset terjejas (rosak, musnah atau hilang) ▪ Berikan satu nilai Tahap Kerugian Perniagaan setiap aset ▪ Berikan nilai impak setiap asset
Analisis Kebarangkalian	▪ Mengukur ketepatan kebarangkalian aset yang terjejas ▪ Merujuk semula nilai ancaman, kelemahan, perlindungan yang telah dikenal pasti ▪ Berikan nilai Rendah, Sederhana atau Tinggi
Kira Risiko	▪ Menentukan tahap risiko aset dengan nilai Rendah, Sederhana atau Tinggi dengan memadankan nilai impak dan nilai kebarangkalian. ▪ Menentukan Pemilik Risiko ▪ Tahap risiko bernilai Sederhana dan Tinggi mestilah dikurangkan

Hanya lima proses diguna kerana ia telah disesuai mengikut skop kajian. Proses pertama iaitu menubuhkan pasukan tidak terpakai dalam kajian kerana hanya penyelidik yang melaksanakan kajian pengurusan risiko. Manakala bagi proses menilai aset, menilai ancaman, menilai kelemahan dan kenal pasti perlindungan, proses tersebut sesuai diguna sekiranya skop penilaian risiko dilakukan ke atas keseluruhan aset iaitu perkakasan, perisian, data/maklumat, sumber manusia dan perkhidmatan disebabkan banyak faktor ancaman dan kelemahan yang perlu dipertimbang ke atas aset. Memandangkan kaedah pengenalpastian risiko yang diguna bagi kajian adalah berdasarkan isu dan skop kajian hanya tertumpu kepada data/maklumat, maka lima proses utama yang diguna telah mencukupi untuk kajian. Selain itu, kaedah MyRAM hanyalah panduan yang boleh diguna pakai mengikut kesesuaian skop penilaian risiko sesebuah organisasi yang hendak melaksanakan pengurusan risiko. Oleh itu, lima proses yang dikenal pasti mempunyai kesan secara langsung terhadap pengurusan risiko keselamatan data.

ISO/IEC 27001 (PENGURUSAN KESELAMATAN MAKLUMAT)

Standard ini menentukan keperluan untuk mewujudkan, melaksanakan, mengendalikan, memantau, menyemak, menyelenggara dan menambah baik ISMS yang didokumen dalam sesebuah organisasi (Al-Musawi et al. 2015). ISMS adalah pendekatan yang sistematik untuk menguruskan maklumat sensitif syarikat supaya ia kekal selamat. Ia merangkumi manusia, proses dan sistem teknologi maklumat dengan menggunakan proses pengurusan risiko. Bagi melindungi maklumat dan sistem maklumat organisasi, standard ISO 27000, ISO 27001 dan ISO 27002 menyediakan objektif kawalan, kawalan tertentu, keperluan dan garis panduan bagi keselamatan maklumat yang mencukupi (Disterer 2013). Dokumen ini juga menyediakan konsep umum untuk melaksanakan pengurusan risiko keselamatan maklumat dalam sesebuah organisasi (Alebrahim et al. 2014). Dokumen standard ISO/IEC 27001 diguna dengan jayanya untuk menilai risiko yang berkaitan dengan pengkomputeran awan.

Sebagai pembekal awan, salah satu cara untuk mendapatkan keyakinan pelanggan adalah dengan mewujudkan mekanisma keselamatan apabila menggunakan awan dengan mendapatkan pensijilan ISMS bagi sistem pengkomputeran awan mereka (Alebrahim et al. 2014). Atas sebab ini, proses dalam standard diguna sebagai asas kepada mitigasi risiko kerana ianya mengandungi kawalan yang bersesuaian bagi pengurangan risiko. Berdasarkan kajian ke atas metodologi MyRAM dan dokumen standard ISO/IEC 27001, kelebihan dan kelemahan penggunaan metodologi dianalisis dalam Jadual 4.

JADUAL 4. Kelebihan dan Kelemahan MyRAM dan Standard ISO/IEC 27001

MyRAM	
Kelebihan	**Kelemahan**
Merangkumi semua pengguna yang terlibat dalam proses pengurusan risiko	Penglibatan semua pengguna dalam setiap proses pengurusan risiko boleh menjadi rumit apabila ramai pengguna yang terlibat
Memperkemaskan operasi keselamatan dalaman sesebuah agensi Sektor Awam	Kaedah penilaian risiko secara kualitatif menjadikan pemilihan kawalan bagi analisis kos dan faedah sukar ditentukan
Menjadi rujukan dan meningkatkan kesedaran dan pengetahuan dalam keselamatan ICT	
ISO/IEC 27001	
Kelebihan	**Kelemahan**
Menyediakan panduan pelaksanaan pengurusan risiko yang sistematik bersesuaian dengan keselamatan maklumat	Terdapat kesukaran dalam menerapkan standard ini di organisasi disebabkan kurangnya perhatian terhadap pengurusan keselamatan maklumat (terutama Pengurusan Atasan)
Pengguna lebih percaya bahawa maklumat pengguna dan kerahsiaan dilindungi	
Ia merupakan standard antarabangsa yang diguna di kebanyakan negara dalam pengurusan keselamatan maklumat	

Kajian ini menggunakan proses penilaian risiko MyRAM bersama dokumen standard ISO/IEC 27001:2013 sebagai asas kepada penilaian risiko dan penentuan mitigasi risiko yang dikenal pasti kerana metodologi MyRAM memberikan gambaran untuk memahami, menilai dan menentukan risiko maklumat yang ada. Manakala dokumen standard ISO/IEC 27001:2013 boleh diguna sebagai asas kepada mitigasi risiko kerana ianya menyediakan keperluan untuk

mewujudkan, melaksanakan, mengekalkan dan menambah baik sistem pengurusan keselamatan maklumat dalam konteks organisasi.

METODOLOGI KAJIAN

Kajian kes secara kaedah kualitatif dijalankan di Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU). Kajian kes ini: 1) menggunakan analisis risiko bagi menentukan risiko keselamatan data dalam penggunaan SaaS; 2) memahami risiko keselamatan data dalam penerapan SaaS dan perspektif pengguna melalui pelaksanaan pengurusan risiko. Kajian melibatkan empat fasa utama yang terdiri daripada Fasa 1: Kajian Awal, Fasa 2: Pembangunan (senarai risiko dan protokol kajian kes, Fasa 3: Penilaian (pengumpulan data dan analisis kajian kes) dan Fasa 4: Laporan dan Rumusan.

Kaedah persampelan bertujuan (*purposeful sampling*) digunakan dengan memilih informan berdasarkan kepada keupayaan mereka dalam menjawab persoalan kajian, pengetahuan dan pengalaman menggunakan SaaS (Miles dan Huberman 1994). Data dikumpul melalui temu bual, pemerhatian dan analisis dokumen. Teknik temu bual secara berkumpulan diguna bagi mendapatkan pandangan dan sikap pengguna terhadap penggunaan SaaS di MAMPU. Teknik ini lebih cepat dan kos efektif dalam mendapatkan data dalam bidang yang agak baharu seperti SaaS. Informan terdiri daripada sepuluh orang pegawai Kerajaan yang mempunyai pengalaman di antara 7 hingga 30 tahun dan terlibat secara langsung sebagai perunding keselamatan ICT, pengurusan risiko keselamatan maklumat dan pengguna perkhidmatan SaaS (Jadual 5).

Pelbagai aspek pemerhatian dilakukan seperti perbualan, bahasa badan, emosi, persekitaran organisasi secara am, interaksi sesama ahli organisasi dan lain-lain yang relevan. Pemerhatian dan analisis dokumen iaitu minit mesyuarat, pelan pengurusan risiko, dokumen *The Malaysian Public Sector Information Security High-Level Risk Assessment* (HiLRA), dokumen MyRAM, dokumen Standard ISO/IEC 27001:2013 dan garis panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam turut dilakukan untuk memahami dengan lebih jelas kaedah dan teknik dalam proses penilaian risiko maklumat bagi memastikan proses penilaian dapat dilaksana dengan sistematik dan berkesan.

Proses pengumpulan dan analisis data adalah secara induktif iaitu dengan mengumpulkan maklumat secara berterusan bagi menjelaskan masalah yang dikaji. Seterusnya data dhubungkan untuk menentukan ketepatan risiko. Data dianalisis menggunakan kaedah analisis kandungan dan analisis kiraan. Hasil analisis dibentang dalam ilustrasi grafik. Semua informan faham mengenai proses pengurusan risiko. Data temu bual direkod secara audio dan ditranskrib. Saringan dan pembersihan data dilakukan sebelum menjalankan analisis data bagi memeriksa kesilapan data yang dikumpul untuk menghasilkan keputusan analisis data yang lebih tepat (Pallant, 2011). Analisis kandungan melibatkan tiga aktiviti berikut: pengurangan data; paparan data; dan membuat kesimpulan dan pengesahan (Miles dan Huberman (1994).

JADUAL 5. Profil Ringkas Informan

Kod	Jawatan	Bidang Kepakaran	Pengalaman Berkhidmat (Tahun)	Pendedahan kepada SaaS	Penglibatan dalam Pengurusan Risiko
I1	Perunding (Jusa C)	Pengurusan Keselamatan ICT	34	myMesyuarat, MyPrestasi, DDMS & *Dropbox*	▪ Pasukan Pelaksana
I2	Perunding (Jusa C)	Pengurusan Pusat Data	29	myMesyuarat, MyPrestasi, DDMS, *Dropbox, Google App & Google Doc*	▪ Pasukan Pelaksana
I3	Timbalan Pengarah (F54)	Pengurusan Keselamatan ICT	29	myMesyuarat, DDMS, *Gmail & Dropbox*	▪ Pasukan Pelaksana ▪ Pasukan Penyelaras
I4	Ketua Penolong Pengarah Kanan (F48)	Pengurusan Keselamatan ICT	18	myMesyuarat, MyPrestasi, DDMS, *Gmail, Yahoo, Dropbox & Google Doc*	▪ Pasukan Pelaksana ▪ Pasukan Penyelaras ▪ Juru Audit
I5	Penolong Pengarah Kanan (F44)	Pengurusan Keselamatan ICT	12	myMesyuarat, DDMS, *Microsoft 365, Gmail, Facebook, Dropbox, Google App, Google Doc & UTM One Drive*	▪ Pasukan Pelaksana ▪ Pasukan penyelaras ▪ Juru Audit
I6	Penolong Pengarah Kanan (F44)	Pengurusan Keselamatan ICT	9	myMesyuarat , MyPrestasi, DDMS, *Gmail, Facebook, Dropbox, Google App & Google Doc*	▪ Pasukan Pelaksana ▪ Pasukan penyelaras ▪ Juru Audit
I7	Penolong Pengarah (F41)	Pengurusan Keselamatan ICT	8	myMesyuarat, MyPrestasi, DDMS, *Gmail, Facebook, Dropbox, Google App & Google Doc*	▪ Pasukan Pelaksana
I8	Penolong Pengarah (F41)	Pengurusan Keselamatan ICT	8	myMesyuarat, *Gmail, Facebook, Dropbox, Google App & Google Doc*	▪ Pasukan Pelaksana
I9	Penolong Pengarah (F41)	Pengurusan Keselamatan ICT	7	myMesyuarat, *Gmail, Facebook, Microsoft 365, Google App & Google Doc*	▪ Pasukan Pelaksana ▪ Pasukan penyelaras ▪ Juru Audit
I10	Penolong Pengarah (F41)	Pengurusan Keselamatan ICT	7	myMesyuarat, DDMS, *MiCloud, Gmail, Yahoo, Facebook, Dropbox & Google App*	▪ Pasukan Pelaksana

Langkah pertama, proses pengurangan data merupakan proses memilih, memfokus, memperinci dan menstruktur data. Pengurangan data dilakukan berdasarkan kepada pemilihan rangka kerja yang diikuti dan persoalan kajian yang dikemukakan. Langkah yang kedua merupakan paparan data yang melibatkan aktiviti seperti mengendali serta melengkapkan maklumat bagi memudahkan kesimpulan dan tindakan dilakukan. Proses pengekodan

dilakukan dan mengelaskan data yang kompleks kepada bentuk yang lebih mudah difahami. Langkah yang terakhir ialah membuat kesimpulan dan mengemukakan bukti bagi pengesahan nilai impak risiko yang dicadangkan. Analisis kiraan diguna bagi menilai risiko keselamatan data yang berpotensi tinggi dan menentukan mitigasi yang bersesuaian bagi risiko tersebut.

DAPATAN

Kesemua informan menggunakan metodologi MyRAM bersama dokumen standard ISO/IEC 27001 sebagai pendekatan dalam melaksanakan pengurusan risiko. Ia selaras dengan Surat Pekeliling Am Bilangan 6 Tahun 2005 – Garis Panduan Penilaian Risiko Keselamatan Maklumat Sektor Awam. MyRAM merupakan metodologi pengurusan risiko yang lebih menyeluruh terhadap setiap aset iaitu perkakasan, perisian, sumber manusia, perkhidmatan dan data/maklumat. Bagi memudahkan pelaksanaan pengurusan risiko keselamatan maklumat, informan menggunakan Sistem Aplikasi MyRAM yang dibangun oleh MAMPU. Informan mengesahkan keberkesanan pengurusan risiko dan kemantapan sistem MyRAM sebagai satu komponen penting tadbir urus organisasi yang baik. Pihak Pengurusan Tertinggi sentiasa memastikan bahawa rangka kerja pengurusan risiko, menerusi metodologi MyRAM diterap ke dalam budaya, proses dan struktur organisasi. Informan juga mengesahkan bahawa pengurusan risiko penting kepada pencapaian objektif organisasi.

Antara isu pelaksanaan pengurusan risiko di organisasi adalah kurang kefahaman dan kesedaran tentang risiko dan bahaya di kalangan kakitangan dalam melaksanakan tugasan harian. Ini menjadikan mereka kurang memberi perhatian terhadap kepentingan pengurusan risiko. Informan berpendapat pengurusan risiko harus dilakukan oleh pasukan individu yang kompeten yang mempunyai pengetahuan kerja yang baik di tempat kerja. Penglibatan pihak pengurusan dan pegawai pelaksana adalah penting bagi menjayakan pelaksanaan pengurusan risiko. Organisasi bertanggungjawab melaksana dan mengurus risiko keselamatan maklumat bagi membolehkan organisasi mengukur, menganalisis tahap risiko aset maklumat dan seterusnya mengambil tindakan untuk merancang dan mengawal risiko.

Dari segi penilaian risiko, keputusan yang sama diperoleh daripada temu bual dan kajian teoritikal yang dijalankan. Risiko utama dalam SaaS adalah keselamatan data dan senarai risiko pada Jadual 2 disahkan. Semasa sesi temu bual, informan diminta menilai risiko secara individu mengikut kebarangkalian dan impak risiko dengan nilai Rendah (R), Sederhana (S) atau Tinggi (T). Nilai kebarangkalian dan impak ditentu menggunakan kriteria seperti di Jadual 6.

JADUAL 6. Kriteria Nilai Kebarangkalian dan Impak Risiko

Nilai	Kebarangkalian	Impak
Rendah (R)	Tidak berlaku ancaman	Tidak memberi kesan kepada operasi organisasi
Sederhana (S)	Terdapat kemungkinan berlaku ancaman	Memberi kesan sederhana kepada operasi organisasi
Tinggi (T)	Kerap berlaku ancaman	Memberi kesan yang tinggi kepada operasi organisasi

Hasil penilaian informan dianalisis menggunakan kaedah analisis kiraan. Pengukuran kebarangkalian dan impak adalah seperti di Jadual 7 (Analisis Kebarangkalian) dan Jadual 8 (Analisis Impak). Berdasarkan Jadual 7, nilai kebarangkalian ditentukan berdasarkan kekerapan penilaian informan. Bagi risiko kerahsiaan data, sembilan informan menilai sebagai T dan seorang informan menilai Sederhana (S). Oleh itu, nilai kebarangkalian risiko ditentukan sebagai Tinggi (T). Nilai kebarangkalian risiko integriti data adalah T (sembilan informan menilai sebagai T dan seorang informan menilai S). Nilai kebarangkalian risiko ketersediaan

data ditentukan sebagai T (sembilan informan menilai sebagai T dan dua informan menilai S). Bagi risiko kawalan data ditentukan sebagai S (sembilan informan menilai sebagai S dan seorang informan menilai T). Risiko enkripsi data ditentukan sebagai S (enam informan menilai sebagai S, tiga informan menilai sebagai T dan seorang informan menilai R). Risiko pelanggaran data pula ditentukan sebagai T (lima informan menilai sebagai T, empat informan menilai sebagai S dan seorang informan menilai R). Manakala bagi risiko capaian data ditentukan sebagai S (enam informan menilai sebagai S dan empat informan menilai T).

JADUAL 7. Analisis Nilai Kebarangkalian

Risiko	Kebarangkalian										Jumlah
	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	
Kerahsiaan Data	T	T	T	T	T	T	S	T	T	T	T=9 S=1
Integriti Data	T	T	T	T	T	T	S	T	T	T	T=9 S=1
Ketersediaan Data	T	T	S	T	T	T	S	T	T	T	T=8 S=2
Kawalan Data	S	S	T	S	S	S	S	S	S	S	T=1 S=9
Enkripsi Data	T	T	R	S	T	S	S	S	S	S	T=3 S=6 R=1
Pelanggaran Data	S	S	R	T	S	T	S	T	T	T	T=5 S=4 R=1
Capaian Data	S	S	S	T	S	T	S	T	T	S	T=4 S=6

Analisis menunjukkan hanya I3 menilai kebarangkalian risiko enkripsi data dan pelanggaran data sebagai rendah kerana I3 berpendapat bahawa pelbagai teknik enkripsi data sedia ada boleh digunakan dan beberapa polisi berkaitan pelanggaran data seperti Dasar Keselamatan ICT, Akta Perlindungan Data Peribadi 2010 dan sebagainya boleh diguna pakai. Oleh itu, sebarang pelanggaran polisi boleh diambil tindakan undang-undang dan tatatertib di bawah Akta Rahsia Rasmi 1972 dan Perintah-Perintah Am Bab "D" - Peraturan-Peraturan Pegawai Awam (Kelakuan Dan Tatatertib). Jika polisi ini dikuatkuasakan sepenuhnya, kebarangkalian berlaku ancaman disebabkan risiko enkripsi data dan pelanggaran data menjadi rendah.

Merujuk Jadual 8, nilai impak risiko juga ditentukan berdasarkan kekerapan penilaian informan. Bagi risiko kerahsiaan data, lapan informan menilai sebagai T dan dua informan menilai S. Oleh itu, nilai impak risiko ditentukan sebagai Tinggi (T). Tahap impak risiko integriti data, ketersediaan data dan pelanggaran data dinilai sebagai T (semua informan menilai T). Bagi risiko kawalan data ditentukan sebagai T (tujuh informan menilai sebagai T dan tiga informan menilai S). Risiko enkripsi data ditentukan sebagai T (lapan informan menilai sebagai T dan dua informan menilai sebagai S). Manakala bagi risiko capaian data ditentukan sebagai T (sembilan informan menilai sebagai T dan seorang informan menilai S). Ringkasan penilaian kebarangkalian dan impak risiko adalah seperti di Jadual 9.

JADUAL 8. Analisis Nilai Impak

Risiko	Impak										Jumlah
	I1	I2	I3	I4	I5	I6	I7	I8	I9	I10	
Kerahsiaan Data	T	T	T	T	T	S	T	T	S	T	T=8 S=2
Integriti Data	T	T	T	T	T	T	T	T	T	T	T=10
Ketersediaan Data	T	T	T	T	T	T	T	T	T	T	T=10
Kawalan Data	T	T	T	T	S	S	T	T	S	T	T=7 S=3
Enkripsi Data	T	T	T	T	T	S	T	T	S	T	T=8 S=2
Pelanggaran Data	T	T	T	T	T	T	T	T	T	T	T=10
Capaian Data	T	T	T	T	S	T	T	T	T	T	T=9 S=1

JADUAL 9. Analisis Penilaian Kebarangkalian dan Impak Risiko

Risiko	Kebarangkalian	Impak
Kerahsiaan Data	T	T
Integriti Data	T	T
Ketersediaan Data	T	T
Kawalan Data	S	T
Enkripsi Data	S	T
Pelanggaran Data	T	T
Capaian Data	S	T

Nilai kebarangkalian dan impak yang diperoleh seterusnya diukur menggunakan kaedah matrik risiko (Jadual 10) bagi menentukan tahap risiko.

JADUAL 10. Matrik Risiko (MAMPU 2005)

Impak	**Kebarangkalian**		
	Rendah	**Sederhana**	**Tinggi**
Rendah	R	R	S
Sederhana	R	S	T
Tinggi	S	T	T

Keutamaan:	
Rendah	R
Sederhana	S
Tinggi	T

Jadual 11 menunjukkan bahawa semua risiko keselamatan data mempunyai nilai tahap risiko yang Tinggi. Apabila risiko Tinggi, adalah penting untuk mengurangkan tahap risiko. Berdasarkan metodologi MyRAM, tahap risiko Sederhana dan Tinggi mestilah dikurang kepada tahap rendah mengikut kawalan yang bersesuaian bagi mengurangkan impak risiko atau kebarangkalian risiko atau kedua-duanya.

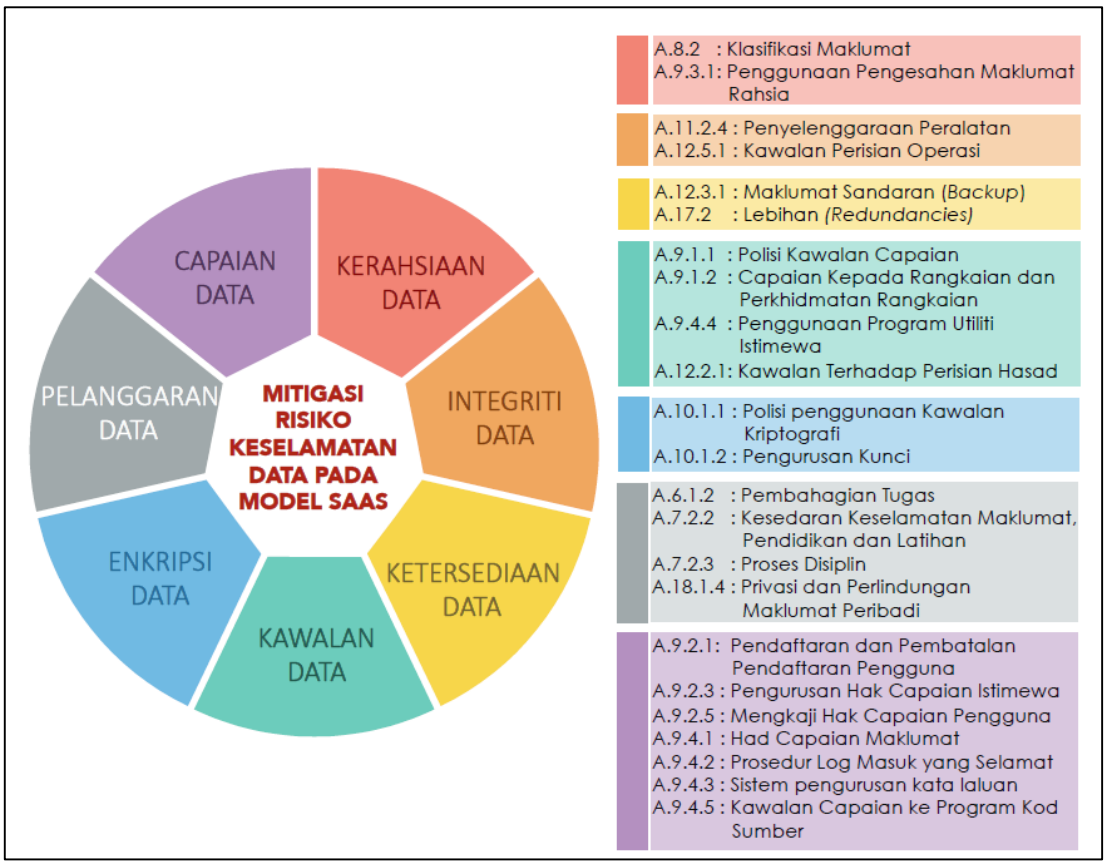
JADUAL 11. Tahap Risiko

Risiko	Kebarangkalian	Impak	Tahap Risiko
Kerahsiaan Data	T	T	T
Integriti Data	T	T	T
Ketersediaan Data	T	T	T
Kawalan Data	S	T	T
Enkripsi Data	S	T	T
Pelanggaran Data	T	T	T
Capaian Data	S	T	T

Senarai mitigasi risiko keselamatan data pada Model SaaS (Rajah 2) dihasilkan menggunakan kawalan yang terdapat pada dokumen standard ISO/IEC 27001:2013. Sebanyak 14 klausa, 35 kategori dan 114 kawalan berkaitan keselamatan maklumat dikenalpasti. Sembilan klausa telah dipilih berdasarkan kesesuaian risiko yang telah dikenal pasti iaitu klausa pengurusan aset, pengurusan capaian pengguna, keselamatan fizikal dan persekitaran, keselamatan operasi, kriptografi, organisasi keselamatan maklumat, keselamatan sumber manusia, pematuhan dan tindandan. Kawalan yang dipilih adalah kombinasi kaedah kawalan, jenis, elemen dan kategori.

Beberapa perkara perlu dipertimbang ketika melaksanakan pengurusan risiko dalam persekitaran pengkomputeran awan iaitu:

1. Penglibatan pengguna dalam proses pengurusan risiko penting kerana hanya mereka yang mengetahui nilai aset mereka;
2. Penentuan skop dan pengenalpastian risiko merupakan proses penting dalam pengurusan risiko;
3. Penglibatan pengguna SaaS dalam proses pengurangan risiko penting kerana mereka adalah sebahagian daripada masalah, oleh itu mereka juga perlu menjadi sebahagian daripada penyelesaian; dan
4. Pelaksanaan penilaian risiko bagi setiap perkhidmatan sesuai dilakukan secara berasingan supaya masalah keperluan keselamatan pengguna dapat diatasi.



RAJAH 2 . Mitigasi Risiko Keselamatan Data Pada Model SaaS

PERBINCANGAN

Metodologi MyRAM sesuai diguna untuk melaksanakan pengurusan risiko keselamatan data pada Model SaaS dengan mengambil kira proses berkaitan iaitu penentuan skop, pengenalpastian aset/ risiko, analisis impak; analisis kebarangkalian dan pengiraan risiko. Selain itu, Metodologi MyRAM sesuai kerana:

1. Ia menyediakan pendekatan yang sistematik dan berstruktur bagi mengenal pasti, menilai, mengawal dan meminimumkan kebarangkalian dan kesan risiko;
2. Penilaian risiko mengikut piawaian antarabangsa berkesan untuk mengurus dan meningkatkan keselamatan maklumat organisasi;
3. Penilaian risiko yang lebih menyeluruh terhadap setiap aset merangkumi perkakasan, perisian, data/maklumat, sumber manusia dan perkhidmatan;
4. Menepati keperluan standard baharu pensijilan ISMS ISO/IEC 27001:2013;

Namun begitu, beberapa perkara perlu dipertimbang ketika menggunakan metodologi dalam persekitaran pengkomputeran awan seperti berikut:

1. Penglibatan pengguna dalam proses pengurusan risiko adalah penting kerana hanya mereka yang mengetahui nilai aset mereka;
2. Penentuan skop dan pengenalpastian risiko merupakan proses penting dalam pengurusan risiko;
3. Penglibatan pengguna SaaS dalam proses pengurangan risiko adalah penting kerana mereka adalah sebahagian daripada masalah, oleh itu mereka juga perlu menjadi sebahagian daripada penyelesaian; dan
4. Adalah lebih baik untuk menilai risiko secara berasingan bagi setiap perkhidmatan SaaS yang disedia untuk menangani konflik dalam keperluan keselamatan pengguna, disebabkan ciri SaaS yang pelbagai.

Bagi memastikan pengurusan risiko yang dilakukan berkesan, semua maklumat berkaitan hendaklah: a) Jelas dan ringkas: maklumat dapat difahami oleh semua yang terlibat; b) berguna: segala komunikasi berkaitan risiko adalah relevan; c) masa: komunikasi yang berkesan membolehkan keputusan dan tindakan dapat diambil tepat pada masanya. Tujuh risiko utama keselamatan data pada Model SaaS dikenal pasti seperti berikut:

1. Kerahsiaan Data: Perkongsian infrastruktur awan boleh menyebabkan masalah privasi dan kerahsiaan data terdedah kepada orang lain. Data yang disimpan di awan memberi peluang untuk dicapai dan disalin oleh orang lain dan ancaman daripada pengguna dalaman (penyedia awan, pengguna awan lain atau pengguna pihak ketiga yang berniat jahat). Selain itu, kebocoran data boleh berlaku disebabkan kegagalan pengurusan hak capaian ke atas data.
2. Integriti Data: Perubahan tanpa kebenaran kepada data dan sistem oleh pembekal perkhidmatan boleh menjejaskan integriti dan ketersediaan data dan aplikasi. Integriti data dalam persekitaran awan yang kompleks boleh memberikan ancaman terhadap integriti data jika sumber sistem tidak diasing dengan baik antara pelanggan. Selain itu, integriti rangkaian, aplikasi, pangkalan data dan perisian sistem dalam persekitaran awan yang dicapai secara global memberi risiko dan ancaman kelemahan sekiranya tidak dikemaskini dengan perisian terkini dari semasa ke semasa.
3. Ketersediaan Data: Ketersediaan data perlu dilindungi bagi memastikan penyampaian perkhidmatan tidak terganggu. Pelan pemulihan bencana sangat penting sekiranya berlaku bencana untuk memastikan ketersediaan perkhidmatan dan data. Disebabkan SaaS berasaskan perkhidmatan yang disewa, sekiranya penyedia perkhidmatan menamatkan perkhidmatannya, data sedia ada bagi pengguna mempunyai risiko tidak

boleh diambil semula atau hilang. Selain itu, kebergantungan proses capaian dan pemindahan data pada internet memberi risiko disebabkan batasan sambungan dan kelajuan jalur lebar.

4. Kawalan Data: Organisasi tidak mempunyai kawalan ke atas data yang ditempatkan di awan kerana sukar untuk menguatkuasakan polisi kepada penyedia perkhidmatan awan. Perkongsian sumber dengan organisasi lain menyebabkan data terdedah kepada ancaman.
5. Enkripsi Data: Pengurusan enkripsi dan kunci data yang tidak mencukupi menyebabkan risiko kebocoran data atau capaian tidak sah kepada data yang diletak dalam awan, ini kerana persekitaran awan dikongsi dengan penyewa lain dan penyedia perkhidmatan memiliki capaian istimewa ke atas data. Selain itu, kesilapan penggunaan algoritma kriptografi boleh menjadikan enkripsi yang kuat menjadi enkripsi yang sangat lemah.
6. Pelanggaran Data: Konsep pelbagai penyewa dalam persekitaran awan memberi risiko ancaman pelanggaran data ke atas maklumat semua pelanggan di awan, di mana pengguna awan lain boleh mencapai data pengguna lain. Penyedia perkhidmatan perlu mematuhi polisi yang ditetap oleh organisasi mereka sendiri atau industri/badan kerajaan untuk mendapatkan data atau aplikasi dalaman dan luaran. Pematuhan perlu dibukti tanpa mengira lokasi data.
7. Capaian Data: Mekanisma pengesahan yang lemah meningkatkan risiko capaian tidak sah ke data dan aplikasi yang dapat dicapai secara global melalui awan dan dikongsi dengan pelanggan lain (seperti penggunaan kata laluan lemah atau penggunaan semula kata laluan). Capaian terhadap data hanya diberi untuk tujuan spesifik dan dihad kepada pengguna tertentu atas dasar "perlu mengetahui" sahaja. Ini bermakna capaian hanya diberi sekiranya peranan atau fungsi pengguna memerlukan maklumat tersebut. Pertimbangan untuk capaian adalah berdasarkan kategori maklumat seperti yang dinyata di dalam dokumen Arahan Keselamatan.

Selain daripada risiko yang dinyatakan, kajian mendapati sangkalan terhadap data (*repudiation*) juga merupakan ancaman dalam keselamatan data. Dapatan menunjukkan bahawa tiada sangkalan (*non-repudiation*) terhadap data menjamin penghantaran mesej antara pengguna dan memberikan jaminan bahawa seseorang tidak dapat menafikan sesuatu. Tiada sangkalan terhadap data sering diguna dalam tandatangan, kontrak digital dan mesej e-mel. Ia memastikan bahawa pengguna tidak dapat menafikan ketulenan tandatangan pada dokumen atau penghantaran mesej mereka. Memandangkan MAMPU menyediakan perkhidmatan *Public Key Infrastructure* (PKI) kepada agensi Sektor Awam, maka ancaman kepada sangkalan terhadap data perlu diberi perhatian.

Kajian memilih kawalan yang terdapat dalam dokumen standard ISO/IEC 27001:2013 di mana ia mengandungi 14 klausa, 35 kategori dan 114 kawalan berkaitan keselamatan maklumat (ISO/IEC 2013, 2013). Namun begitu hanya sembilan klausa yang dipilih berdasarkan kesesuaian risiko iaitu klausa pengurusan aset, pengurusan capaian pengguna, keselamatan fizikal dan persekitaran, keselamatan operasi, kriptografi, organisasi keselamatan maklumat, keselamatan sumber manusia, pematuhan dan tindanan. Pemilihan kawalan boleh diambil daripada standard, kerangka dan garis panduan yang sedia ada, atau mereka bentuk kawalan baharu untuk memenuhi keperluan tertentu. Kawalan yang dipilih adalah kombinasi kaedah kawalan, jenis, elemen dan kategori. Oleh itu, kajian mencadangkan supaya pemilihan kawalan diambil daripada pelbagai sumber sedia ada selain daripada standard ISO/IEC 27001:2013 seperti ENISA, COBIT, NIST dan PCI-DSS supaya kawalan terhadap risiko dapat dilihat secara menyeluruh.

KESIMPULAN

Kebanyakan organisasi melaksanakan perkhidmatan SaaS dalam pengkomputeran awan kerana ~~ianya~~ banyak memberi manfaat dan keuntungan seperti pengurangan kos penyelenggaraan. Namun begitu, semakin banyak maklumat diletak di awan, semakin banyak risiko yang perlu dipertimbangkan tentang keselamatan data. Berdasarkan kepada penilaian dan penemuan kajian kes, metodologi MyRAM sesuai diguna dalam pengurusan risiko keselamatan data dalam Model SaaS dengan mengambil kira proses berkaitan iaitu penentuan skop, pengenalpastian aset/risiko, analisis impak; analisis kebarangkalian dan pengiraan risiko. Pengguna MAMPU menerima baik penggunaan SaaS dari segi penjimatan kos dan membantu memudahkan tugas harian mereka. Namun begitu daripada segi risiko yang perlu dipertimbang, keselamatan data merupakan risiko utama dalam pelaksanaan SaaS. Data/maklumat adalah aset yang sangat berharga dalam organisasi, sama ada ia dicetak atau ditulis, disimpan secara elektronik atau dihantar melalui pos atau secara elektronik. Organisasi bertanggungjawab mengurus bagaimana maklumat dikawal selia, diguna dan dilindungi oleh pembekal dan jangkaan pengguna tanpa menjejaskan proses pengurusan maklumat semasa.

Tujuh risiko keselamatan data dikenal pasti iaitu iaitu kerahsiaan data, integriti data, ketersediaan data, kawalan data, enkripsi data, pelanggaran data dan capaian data merupakan risiko keselamatan data yang paling utama pada Model SaaS. Berdasarkan pengenalpastian risiko dan analisis risiko yang dilakukan, kawalan perlu dilaksana bagi memastikan tindakan yang dilakukan boleh mengatasi risiko dan mencapai objektif organisasi. Mitigasi yang disenarai mengunakan kawalan sedia ada yang terdapat pada dokumen standard ISO/IEC 27001:2013. Pendapat informan turut diambil kira dalam penyusunan senarai mitigasi bagi memastikan ianya dapat dipraktik dan diterima pakai oleh pengguna SaaS. Namun begitu, mitigasi risiko yang dihasilkan hanya terhad kepada risiko keselamatan data dan Model SaaS sahaja.

Garis panduan pengurusan risiko keselamatan data SaaS yang dihasilkan menyumbang kepada peningkatan pengetahuan organisasi dalam pelaksanaan pengurusan risiko dengan mempertimbangkan risiko yang ada sebelum menggunakan SaaS. Selain itu, ia dapat membantu organisasi lain dalam mempertimbangkan pengurusan risiko di organisasi masing-masing dan ia boleh diguna oleh kajian lain sebagai input untuk menghasilkan kerangka atau model risiko keselamatan datta dalam organisasi yang berbeza.

RUJUKAN

Abbas, R., Farooq, A. & Afghan, S. 2015. A Security Model for SaaS in Cloud Computing. Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan 20(IV): 103–110.

Ahire, R. M. & Kadam, G. 2015. Review on Security Issues of SaaS Clouds. International Journal Of Engineering And Computer Science 4(7): 13422–13425.

Aich, A., Sen, A. & Dash, S. R. 2015. A Survey on Cloud Environment Security Risk and Remedy. Proceedings - 1st International Conference on Computational Intelligence and Networks, CINE 2015 192–193. doi:10.1109/CINE.2015.45

Alebrahim, A., Hatebur, D. & Goeke, L. 2014. Pattern-based and ISO 27001 Compliant Risk Analysis for Cloud Systems. IEEE 1st International Workshop on Evolving Security and Privacy Requirements Engineering, ESPRE 2014 - Proceedings 42–47.

Al-Musawi, F., Al-Badi, A. H. & Ali, S. 2015. A Road Map to Risk Management Framework for Successful Implementation of Cloud Computing in Oman. International Conference on Intelligent Networking and Collaborative Systems 417–422. doi:10.1109/INCoS.2015.80

Bahekar, T. & Holey, A. S. 2016. Study : Issues in Cloud Computing. International Journal of Research in Computer & Information Technology (IJRCIT) 1(2): 276–282.

Bishnoi, N. & Sehrawat, A. 2013. Cloud And Its Security Concerns. International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR) 3(3): 79–84

BSI (British Standards Institution). 2011. White Paper: Security Recommendations for Cloud Computing Providers (Minimum Information Security Requirements). https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Cloud Computing/SecurityRecommendationsCloudComputingProviders.pdf [11 Mac 2017]

Chouhan, P. K., Yao, F. & Sezer, S. 2015. Software as a Service : Understanding Security Issues. Science and Information Conference 2015 162–170. doi:10.1109/SAI.2015.7237140.

Cole, B. 2012. ISACA: Update to CobiT 5 Governance Framework Maximizes IT Assets. http://searchcompliance.techtarget.com/news/2240148924/ISACA- Update-to-COBIT-5-governance-framework-maximizes-IT-assets [11 Mac 2017].

Disterer, G. 2013. ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security 4(April): 92–100

Fan, C. K. & Chen, T. 2012. The Risk Management Strategy of Applying Cloud Computing. International Journal of Advanced Computer Science and Applications 3(9): 18–27.

Gadia, S. 2011. Cloud Computing Risk Assessment a Case Study. Information Systems Audit and Control Association (ISACA) Journal 4: 6. http://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Cloud-Computing-Risk-Assessment-A-Case-Study.aspx [11 Mac 2017].

Heiser J. 2009. What You Need To Know About Cloud Computing Security And Compliance, Gartner. https://www.gartner.com/doc/1071415/need-knowcloud-computing-security [8 April 2017]

Hepsiba, C. L. & Sathiaseelan, J. G. R. 2016. Security Issues in Service Models of Cloud Computing. International Journal of Computer Science and Mobile Computing 5(3): 610–615.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 2011. ISO/IEC 27005 - Information Security Risk Management.

International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). 2013. ISO/IEC 27001 - Information Security Management.

Kumar, K. V. K. M. 2014. Software as a Service for Efficient Cloud Computing. International Journal of Research in Engineering and Technology 3(1):178-181

Kaur, M. & Singh, H. 2015. A Review of Cloud Computing Security Issues. International Journal of Education and Management Engineering (IJEME) 5(5): 32.

MAMPU. 2005. The Malaysian Public Sector Information Security Risk Assessment Methodology (MyRAM) Handbook. Putrajaya: MAMPU, JPM

MAMPU. 2016. Rangka Kerja Keselamatan Siber Sektor Awam. versi 1.0. http://www.mampu.gov.my/images/suara_anda/RAKKSSA-VERSI-1-APRIL-2016-BM.pdf [3 April 2017]

Miles, M.B. & Huberman, M. a. 1994. Qualitative Data Analysis: An Expanded Sourcebook (2nd ed.). 20(1): 159–160. doi:10.1016/S1098-2140(99)80125-8.

Mosco, V. 2014. To the Cloud, Big Data in a Turbulent World. Paradigm Publisher. doi:10.1017/CBO9781107415324.004

Munir, K. & Palaniappan, S. 2013. Framework For Secure Cloud Computing. International Journal on Cloud Computing: Services and Architecture 3(2): 21–35. doi:10.5121/ijccsa.2013.3202

National Institute of Standards and Technology (NIST). 2002. Risk Management Guide for Information Technology Systems. NIST. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [2 April 2017]

Pallant, J. 2011. SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS. McGraw-Hill Education.

Pharkkavi D & Maruthanayagam D. 2016. An Comprehensive Study on Security Issues of Cloud Computing and Its Data. International Journal of Contemporary Research in Computer Science and Technology 2(2): 448–454.

Paquette, S., Jaeger, P. T. & Wilson, S. C. 2010. Identifying The Security Risks Associated With Governmental Use Of Cloud Computing. Government Information Quarterly 27(3): 245–253.

Rashmi, Sahoo, G. & Mehfuz. 2013. Securing Software as a Service Model of Cloud Computing: Issues and Solutions. International Journal on Cloud Computing: Services and Architecture (IJCCSA) 3(4): 1–11. doi:10.5121/ijccsa.2013.3401

Singh, A. & Chatterjee, K. 2017. Cloud Security Issues and Challenges : A Survey 79(August 2016): 88–115. doi:10.1016/j.jnca.2016.11.027.
Soofi, A. A., Khan, M. I., Talib, R. & Sarwar, U. 2014. Security Issues in SaaS Delivery Model of Cloud Computing 3(3): 15–21.
Tang, C. & Liu, J. 2015. Selecting a Trusted Cloud Service Provider for your SaaS Program. Computers and Security 50: 60–73. doi:10.1016/j.cose.2015.02.001.
Thakare, V. R. & John S, K. 2016. A Study of Security and Privacy Issues at Service Models of Cloud Computing. Indian Journal of Science and Technology 9(38): 1–14.

Nooraidaniza Jafri
Maryati Mohd Yusof
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia
maryati.yusof@ukm.edu.my, ezine19@yahoo.com

Corresponding author. Email: maryati.yusof@ukm.edu.my

Received: 27 December2017
Accepted: 28 February 2018
Published: 29 June 2018