

Model Pematuhan Penyedia Perkhidmatan Awan Terhadap Keselamatan Awan Berdasarkan ISO/IEC 27017:2015

Norhuda binti Abd Razak
chudayr@gmail.com

Ibrahim bin Mohamed
ibrahim@ukm.edu.my

ABSTRAK

Pengkomputeran awan merupakan salah satu teknologi yang kian diguna secara meluas. Keupayaan pengkomputeran awan untuk menyimpan data yang besar, kemudahan akses internet, serta pengguna tidak perlu melabur dalam pembangunan teknologi sendiri menjadikannya sesuai untuk individu dan organisasi. Bagaimanapun, kebanyakan organisasi berasa khuatir untuk memindahkan aplikasi kritikal dan pangkalan data legasi yang dipenuhi dengan maklumat sulit kepada penyedia perkhidmatan awan (CSP). Bagi meningkatkan keyakinan pengguna perkhidmatan awan (CSU) terhadap tahap keselamatan CSP, CSP hendaklah menggunakan standard keselamatan seperti standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001:2013 dan standard berkaitan keselamatan pengkomputeran awan seperti ISO/IEC 27017:2015 dalam menguruskan keselamatan maklumat mereka. Kajian ini bertujuan melihat domain yang mempengaruhi pematuhan kawalan keselamatan maklumat awan dan juga mengukur tahap keberkesanan dan kecekapan model penilaian audit keselamatan berdasarkan 37 kawalan standard keselamatan awan ISO/IEC 27017:2015. Metodologi kajian ini menggunakan gabungan kaedah kualitatif dan kuantitatif. Proses penghasilan dan penentusahan model awal kajian dilaksanakan dengan menggunakan kaedah kualitatif manakala proses pengesahan model kajian dilaksanakan dengan menggunakan kaedah kuantitatif. Kajian ini mendapati terdapat lima domain yang mempengaruhi penilaian pematuhan keselamatan agensi CSP iaitu Teknologi, Organisasi dan Proses, Budaya, Undang-undang dan Persekitaran. Berdasarkan 37 kawalan yang dipetakan kepada lima domain tersebut, satu model senarai semak tahap pematuhan kawalan keselamatan maklumat awan bagi CSP berdasarkan ISO/IEC 27017:2015 berjaya dihasilkan. Model ini diharap dapat membantu organisasi CSP sebagai garis panduan dalam melaksanakan audit keselamatan awan seterusnya meningkatkan kepercayaan CSU dalam menggunakan perkhidmatan mereka.

Kata kunci—pengkomputeran awan; keselamatan awan; pematuhan dan ISO/IEC 27017:2015

PENGENALAN

Pengkomputeran awan merupakan salah satu teknologi yang kian digunakan secara meluas yang mana pengguna mendapatkan sumber teknologi maklumat (TM) secara perkhidmatan melalui Internet. *National Institute of Standards (NIST)* mentakrifkan pengkomputeran awan sebagai satu model yang membenarkan capaian rangkaian secara permintaan kepada sumber TM (rangkaiannya, pelayan, ruang penyimpanan, aplikasi dan perkhidmatan) dengan pentadbiran atau interaksi yang minimum dengan penyedia perkhidmatan [1]. Penggunaan pengkomputeran awan memungkinkan data untuk diakses pada bila-bila masa dan seterusnya dapat menghasilkan penyampaian perkhidmatan yang lebih baik.

Bagaimanapun, terdapat lapan (8) isu dan cabaran utama berkaitan keperluan keselamatan dan keperluan privasi dalam pengurusan awan yang telah dikenalpasti oleh para penyelidik sebelum ini iaitu kepercayaan, keselamatan data, integriti, kebolehcapaian, kerahsiaan, pengesahan pengguna, ketersediaan dan pengurusan identiti [2]. Penggunaan pengkomputeran awan tidak dipercayai sepenuhnya oleh pengguna awan disebabkan oleh penggunaan sumber secara maya, replikasi dan migrasi secara global dan ketiadaan data dan mesin secara fizikal di dalam awan yang mana menyebabkan penyimpanan data di dalam awan dan hasil perhitungan berkemungkinan untuk tidak diurus dengan baik [3].

Kebanyakan organisasi berasa khuatir untuk memindahkan aplikasi kritikal dan pangkalan data legasi mereka yang dipenuhi dengan maklumat sulit kepada penyedia perkhidmatan awan (Cloud Service Provider (CSP)) disebabkan penggunaan pengkomputeran awan ini akan menyebabkan organisasi kehilangan kawalan terhadap data mereka [4]. Untuk mengurangkan tahap kekhuatiran ini, CSP hendaklah memastikan bahawa mereka sentiasa menyediakan tahap kawalan dan keselamatan yang sama kepada aplikasi dan data sensitif organisasi sebagaimana yang diperolehi oleh organisasi dalam menggunakan sistem tanpa awan. Sehubungan itu, CSP hendaklah membuktikan kepada organisasi/pelanggan bahawa semua perjanjian peringkat perkhidmatan (SLA) dipenuhi dan pematuhan keselamatan dapat dibuktikan kepada juruaudit.

Bagi meningkatkan keyakinan pengguna perkhidmatan awan (Cloud Service User (CSU)) terhadap tahap keselamatan CSP, CSP hendaklah menggunakan standard keselamatan sebagai pendekatan untuk menangani keselamatan TM yang membolehkan CSU menilai CSP yang paling sesuai untuk keperluan keselamatan mereka [5]. Di antara standard keselamatan TM yang banyak digunakan adalah Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001 yang mentakrifkan keperluan dan prosedur untuk pelaksanaan, penyelenggaraan, dan peningkatan Sistem Pengurusan Keselamatan Maklumat (ISMS). Bagaimanapun, ISO/IEC 27001 merupakan satu standard umum berkaitan pengurusan keselamatan maklumat dan tidak meliputi keselamatan pengkomputeran awan. CSP perlu memastikan penilaian keselamatan awan mereka turut mengambil kira standard berkaitan keselamatan pengkomputeran awan seperti ISO/IEC 27017, *Cloud Security Alliance (CSA)* dan *The Federal Risk and Authorization Management Program (FedRAMP)*.

Oleh itu, tujuan kajian ini adalah untuk mencadangkan pembangunan satu model keselamatan awan kepada CSP ketika sesi audit keselamatan berdasarkan standard keselamatan awan. Model ini akan dibangunkan berdasarkan standard keselamatan konvensional iaitu ISO/IEC

27001 dan juga standard keselamatan awan iaitu ISO/IEC 27017 yang merupakan garis panduan amalan terbaik berkaitan keselamatan awan yang didapati paling sesuai untuk tujuan ini.

KAJIAN BERKAITAN

A. Pengkomputeran Awan

Pengkomputeran awan adalah model yang membenarkan capaian rangkaian dilaksanakan secara mudah, di mana-mana sahaja secara atas permintaan kepada sumber pengkomputeran yang dikongsi bersama (contohnya: rangkaian, pelayan, ruang penyimpanan, aplikasi dan perkhidmatan) yang boleh dibekalkan dengan pantas melalui pengurusan atau interaksi yang minima dengan penyedia perkhidmatan [1]. Pengkomputeran awan terdiri daripada lima ciri asas, tiga model perkhidmatan dan empat model penyebaran. Lima ciri asas pengkomputeran awan adalah: perkhidmatan secara layan diri, akses rangkaian yang meluas, penyatuan sumber, keanjalan pantas, dan perkhidmatan yang diukur. Bergantung kepada tahap perkhidmatan yang disediakan, tiga jenis model perkhidmatan awan yang dikenal pasti adalah: Perisian Sebagai Perkhidmatan (SaaS), Platform Sebagai Perkhidmatan (PaaS) dan Infrastruktur Sebagai Perkhidmatan (IaaS). Manakala empat model penyebaran awan adalah: awan peribadi, awan komuniti, awan awam dan awan hibrid.

Terdapat dua pengguna yang memainkan peranan utama di dalam perkhidmatan pengkomputeran awan iaitu penyedia perkhidmatan awan (CSP) dan pengguna perkhidmatan awan (CSU). CSP merupakan satu entiti yang bertanggungjawab kepada operasi keseluruhan persekitaran awan yang ditawarkan kepada CSU dengan menyediakan dan menguruskan keseluruhan infrastruktur perkakasan dan perisian yang sesuai untuk menjalankan perkhidmatan [6][7]. CSP juga bertanggungjawab terhadap keseluruhan fungsi dan kekurangan persekitaran awan dengan menyediakan kakitangan untuk mengurus dan menyelenggara infrastruktur tersebut. CSU pula adalah individu atau organisasi yang membeli atau mendapatkan perkhidmatan pengkomputeran awan yang bersetuju dengan CSP dalam beberapa bentuk penggunaan persekitarannya, yang biasanya disahkan melalui dokumen perjanjian tahap perkhidmatan (Service Level Agreement (SLA)). CSP menyediakan aplikasi melalui internet yang diakses dari pelayar web, desktop dan aplikasi mudah alih oleh CSU sementara perisian perniagaan dan data disimpan pada pelayan di lokasi terpencil bergantung kepada jenis model perkhidmatan awan yang digunakan [8].

B. Isu dan Cabaran Keselamatan Pengkomputeran Awan

Perkhidmatan pengkomputeran awan telah banyak digunakan oleh individu serta organisasi awam dan swasta kerana manfaatnya yang banyak seperti akses yang boleh dikembangkan, fleksibel, dan cekap kosnya kepada perkhidmatan infrastruktur dan aplikasi [9]. Pengguna perkhidmatan pengkomputeran awan dapat mengakses maklumat di mana sahaja lokasi yang mempunyai capaian internet. Perkhidmatan awan seperti IaaS, PaaS dan SaaS yang disediakan CSP membolehkan CSU mengakses infrastruktur, platform dan perisian yang dilanggan berdasarkan keperluan mereka.

Walaupun terdapat manfaat yang banyak dalam penggunaan perkhidmatan pengkomputeran awan ini, CSU masih mempunyai kebimbangan terhadap tahap keselamatan data dan privasi [10][11] serta pematuhan [12] [13] dalam perkhidmatan pengkomputeran awan yang diuruskan dan ditawarkan oleh CSP. CSU sukar untuk menentukan kriteria dalam pemilihan CSP kerana terdapat pelbagai CSP yang menawarkan kepelbagaian yang luas dalam perkhidmatan awan kepada CSU dengan pelbagai tahap kekuatan keselamatan maklumat. Dalam konteks pengkomputeran awan, apabila CSU menggunakan perkhidmatan awan, mereka telah menghadkan kawalan mereka ke atas aspek keselamatan utama dan memberikan tahap kepercayaan yang besar kepada CSP dalam aspek kawalan ke atas data, keselamatan dan privasi data, kualiti data dan jaminan serta pengawasan data [10][14]. Terdapat pandangan yang mengatakan bahawa penggunaan pengkomputeran awan adalah tidak selamat kerana tidak ada jaminan ke atas maklumat yang dikawal dan dikendalikan oleh CSP [15]. Dalam hal ini, adalah menjadi tanggungjawab CSP ke atas keselamatan dan kepatuhan perkhidmatan pengkomputeran awan yang disediakan [13].

Pematuhan bagi keselamatan data dan aplikasi di persekitaran pengkomputeran awan adalah penting bagi memastikan keselamatan data terjamin oleh CSP. Insiden keselamatan dan pelanggaran data bukan sahaja melibatkan kerugian wang ringgit, malah boleh mengakibatkan kehilangan pelanggan, kerosakan reputasi dan pengurangan keyakinan pelabur [16]. Oleh itu, kebanyakan organisasi akan melaksanakan program keselamatan maklumat bagi mengurangkan kemungkinan dan kesan berlakunya insiden keselamatan dan pelanggaran data [16]. Objektif utama program keselamatan maklumat adalah untuk melindungi integriti, kerahsiaan dan ketersediaan maklumat dan aplikasi sambil memastikan bahawa keperluan undang-undang dan peraturan juga dipatuhi [17]. Sehubungan itu, organisasi yang mahu melaksanakan pengkomputeran awan hendaklah melaksanakannya berdasarkan dasar, standard dan garis panduan mereka. Walaupun *European Network and Information Security Agency* dan *Cloud Security Alliance* telah menentukan dokumentasi keselamatan untuk persekitaran pengkomputeran awan, sangat sedikit penyelidikan

yang menyelidiki penerapan dokumentasi ini untuk mengurangkan insiden keselamatan yang berkaitan dengan awan dan pelanggaran data [16]. Bagi mengatasi isu keselamatan maklumat adalah penting dan berguna untuk CSP melaksanakan standard Sistem Pengurusan Keselamatan Maklumat (Information Security Management System (ISMS)) bagi meningkatkan kepercayaan CSU dan seterusnya dapat memperluaskan lagi pasaran penggunaan pengkomputeran awan [11].

Di Malaysia, Kementerian Komunikasi dan Multimedia Malaysia turut telah mengeluarkan Garis Panduan Pemilihan Penyedia Keselamatan Awan [18] yang mengesyorkan beberapa kriteria pemilihan CSP berdasarkan amalan terbaik yang digariskan.

C. Pematuhan dan Pengauditan Pengkomputeran Awan

Bagi perkhidmatan pengkomputeran awan, pengawal selia awan (cloud regulators) seperti pegawai penguatkuasa undang-undang, juruaudit, jabatan/organisasi standard, jabatan kerajaan dan penggubal undang-undang teknologi maklumat antarabangsa kebiasaannya menjadi perantara di antara CSP dan CSU. Juruaudit awan misalnya bertanggungjawab untuk melaksanakan pemeriksaan terhadap pematuhan kawalan keselamatan CSP bagi mengesahkan pematuhan CSP tersebut terhadap standard melalui tinjauan bukti objektif [13]. Kerajaan pula bertanggungjawab untuk membuat kerangka undang-undang berdasarkan standard antarabangsa yang meliputi isu-isu seperti perlindungan data dan privasi, peraturan dalam peruntukan bidang kuasa, tanggungjawab dan liabiliti serta perlindungan pengguna. Penglibatan pihak berkepentingan iaitu pengawal selia awan, CSP dan CSU adalah penting untuk memastikan kejayaan penggunaan perkhidmatan pengkomputeran awan. Pengawal selia awan bertanggungjawab untuk menguatkuasakan undang-undang dan peraturan berkaitan pengurusan keselamatan maklumat manakala CSP dan CSU bertanggungjawab untuk memberikan jaminan bagi keselamatan dan pematuhan awan [13].

Standard pematuhan seperti siri ISO/IEC 27001 dirangka untuk membantu organisasi meningkatkan tahap keselamatan siber mereka dengan menyediakan prosedur dan proses bagi pencegahan, pengesanan dan pemulihan. Dengan memenuhi dan mematuhi standard yang digariskan tersebut, ia dapat membantu organisasi mewujudkan budaya kerja yang mementingkan pengendalian risiko keselamatan [19].

Bagaimanapun, masih terdapat organisasi awam dan swasta yang masih bimbang dan ragu-ragu untuk menggunakan perkhidmatan awan disebabkan faktor keselamatan, privasi dan kebolehpercayaan terhadap jaminan keselamatan yang disediakan oleh CSP [20]. Sehubungan itu, pensijilan perkhidmatan awan kepada CSP adalah satu kaedah yang baik untuk mengatasi masalah ini untuk mewujudkan kepercayaan dan meningkatkan ketelusan perkhidmatan awan. Penyelidikan

yang meluas telah mencadangkan pensijilan dan audit sebagai salah satu kaedah yang baik untuk menilai kualiti dan prestasi perkhidmatan TM dalam proses perolehan. Beberapa badan pensijilan perkhidmatan awan seperti CSA STAR dan ISO 27017 telah muncul untuk menjamin tahap keselamatan yang tinggi, kebolehpercayaan dan kepatuhan undang-undang terhadap perkhidmatan awan [20].

Selain daripada peraturan dan undang-undang, terdapat juga masalah dalam pematuhan dalam senario perkhidmatan awan. Kamus Merriam-Webster mentafsirkan pematuhan sebagai “perbuatan atau proses mematuhi keinginan, permintaan, cadangan, atau rejimen atau paksaan dan; kesesuaian dalam memenuhi syarat rasmi.” Definisi dalam literatur menakrifkan pematuhan TM sebagai penyesuaian sistem TM dengan polisi, prosedur, standard, panduan, spersifikasi atau perundangan yang telah ditetapkan [21]. Pematuhan merupakan tanggungjawab bersama di antara CSP dan CSU.

Keperluan kepada pematuhan keselamatan TM adalah bergantung kepada peraturan dalaman dan luaran. Peraturan dalaman terdiri daripada panduan atau prosedur operasi. Peraturan luaran pula terdiri daripada undang-undang, peraturan dan kontrak sivil. Terdapat keperluan untuk mengenal pasti pematuhan yang perlu dipatuhi berdasarkan keperluan khusus industri seperti perbankan, kesihatan atau sektor awam bagi memastikan kebolehlaksanaan pengurusan risiko. Bagaimanapun, dalam senario perkhidmatan awan, keperluan ini agak sukar untuk dilaksanakan kerana terdapat pergantungan kepada jenis data dan struktur perkhidmatan awan. Pematuhan juga menjadi rumit disebabkan terdapat banyak peraturan dan undang-undang yang perlu dipatuhi oleh CSP dan CSU [21].

Audit keselamatan teknologi maklumat dapat menentukan sama ada sistem maklumat dan penyelenggaranya memenuhi kedua-dua jangkaan undang-undang perlindungan data pelanggan dan standard organisasi untuk mencapai kejayaan kewangan daripada pelbagai ancaman keselamatan [22]. Melalui pelaksanaan audit, tindakan pengesanan, pencegahan, penambahbaikan dan peningkatan kualiti yang berterusan dapat diambil ke atas sebarang kelemahan, ketidakpatuhan atau kekurangan kepada sistem pengurusan keselamatan ICT sedia ada.

Organisasi yang melaksanakan pemakaian standard dapat membantu organisasi tersebut ke arah mewujudkan sistem penyampaian yang memenuhi tuntutan dan kepuasan pelanggan. Melalui pematuhan sesuatu standard, organisasi dapat menyediakan rangka kerja yang memenuhi keperluan-keperluan yang ditetapkan oleh standard dan amalan terbaik industri. Di antara amalan standard keselamatan maklumat yang biasa diamalkan bagi organisasi adalah ISO/IEC 27001:2013 Sistem Pengurusan Keselamatan Maklumat (ISMS). ISMS membolehkan sistem penyampaian beroperasi

dalam keadaan baik, selamat dan terkawal di samping memantapkan lagi perlindungan ke atas maklumat dan aset ICT berasaskan prinsip kerahsiaan, integriti dan kebolehsediaan.

1) *Sistem Pengurusan Keselamatan Maklumat*

Sistem Pengurusan Keselamatan Maklumat (ISMS) merupakan suatu pendekatan yang bersistematik dan berstruktur dalam pengurusan maklumat yang meliputi polisi, proses, prosedur, struktur organisasi dan juga fungsi sesuatu perisian dan perkakasan bagi memastikan keselamatan maklumat di dalam sesebuah organisasi. Pelaksanaan ISMS dipengaruhi secara langsung oleh objektif, keperluan keselamatan, proses yang digunakan, saiz dan struktur organisasi [24].

Dengan melaksanakan ISMS, organisasi dapat meningkatkan tahap keselamatan maklumat di samping melindungi maklumat mereka secara sistematik. Selain daripada itu, pelaksanaan ISMS juga menyediakan cara yang tersusun untuk menguruskan keselamatan maklumat dalam organisasi, memberi penilaian bebas mengenai kesesuaian organisasi dengan amalan terbaik yang dipersetujui oleh komuniti pakar untuk ISMS, memberi bukti dan jaminan bahawa organisasi telah mematuhi syarat standard, meningkatkan tadbir urus keselamatan maklumat dalam organisasi dan meningkatkan kedudukan dan reputasi global organisasi [24].

Siri ISO/IEC 27001 adalah sebahagian daripada sekumpulan panduan keselamatan maklumat yang menyediakan kawalan tambahan dan dipertingkatkan. Siri ISO/IEC 27001 merupakan standard antarabangsa bagi keselamatan maklumat yang bertujuan mewujudkan sistem pengurusan keselamatan maklumat agar objektif organisasi kekal relevan dan terkini dan proses, polisi serta kawalan organisasi sentiasa ditambahbaik [26]. Di antara standard di dalam siri ISO 27001 adalah ISO 27002 (perincian kawalan bagi ISO 27001), ISO 27005 (Penilaian Risiko), ISO 27017 (Penggunaan Perkhidmatan Awan) dan ISO 27018 (Perlindungan PII di Awan).

Standard ISO/IEC 27001:2013 merupakan keperluan untuk Sistem Pengurusan Keselamatan Maklumat. Ia mengandungi keperluan untuk membangun, melaksana, mengoperasi, memantau, mengkaji semula, memelihara dan menambahbaik ISMS yang didokumentasi dalam konteks risiko perniagaan keseluruhan organisasi.

Standard ISO / IEC 27002: 2013 pula merupakan kod amalan atau garis panduan Pengurusan Keselamatan Maklumat yang mengandungi katalog kawalan yang dilaksanakan untuk ISMS. Standard ini mengandungi 14 kausa kawalan keselamatan yang merangkumi 35 kategori keselamatan utama dan 114 kawalan.

Standard ISO/IEC 27017:2015 pula melengkapi standard sedia ada ISO/IEC 27002:2013 dengan menyediakan panduan khusus untuk penggunaan perkhidmatan awan yang tidak dinyatakan secara terperinci di dalam standard ISO/IEC 27002:2013.

Pasaran pengkomputeran awan berkembang pesat sehingga tahun 2014. Namun demikian, beberapa siri insiden keselamatan dan serangan terhadap pengkomputeran awan menyebabkan pengguna perkhidmatan awan terutamanya organisasi berkaitan kewangan mempunyai gambaran negatif terhadap perkhidmatan awan [11]. Sehubungan itu, sekiranya penyedia perkhidmatan awan menggunakan standard seperti ISO/IEC 27001, maka kawalan keselamatan dapat diperkukuhkan dan kebarangkalian berlaku pelanggaran atau insiden keselamatan dapat direndahkan seterusnya meningkatkan keyakinan CSU untuk menggunakan perkhidmatan awan.

2) *Standard Khusus Pengkomputeran Awan*

Bagi memastikan penyedia perkhidmatan awan sentiasa melindungi dan menguruskan keselamatan data pelanggan dengan baik, maka pematuhan terhadap standard khusus awan adalah amat digalakkan dan merupakan amalan terbaik yang patut dilaksanakan oleh CSP. Pensijilan berdasarkan audit menyeluruh oleh pihak ketiga terhadap sistem dan prosedur dalaman CSP dapat meyakinkan CSU mengenai jaminan ke atas tahap keselamatan perkhidmatan pengkomputeran awan yang disediakan oleh CSP [5].

Di antara standard khusus awan sedia ada adalah seperti ISO/IEC 27017:2015, *Cloud Security Alliance (CSA)* dan *The Federal Risk and Authorization Management Program (FedRAMP)*. Organisasi seperti *Cloud Security Alliance (CSA)* menawarkan standard untuk meningkatkan keselamatan awan dan juga mempunyai senarai daftar kawalan keselamatan vendor awan untuk membantu pengguna membuat pilihan yang tepat di bidang keselamatan [27].

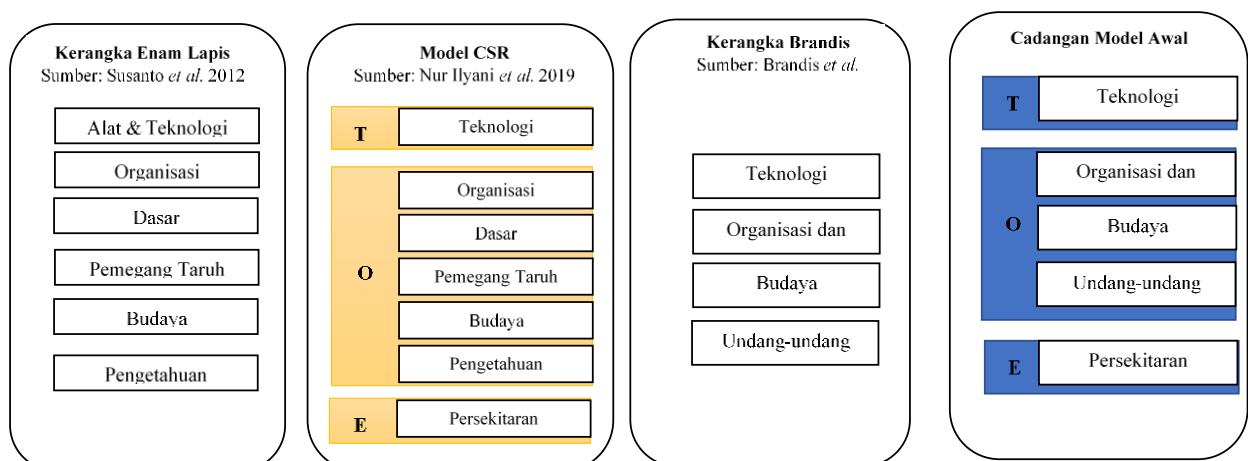
Standard khusus awan ISO/IEC 27017:2015 adalah standard keselamatan yang dibangunkan untuk CSP dan CSU untuk memastikan keselamatan persekitaran perkhidmatan pengkomputeran awan di samping mengurangkan risiko masalah keselamatan. Ia adalah sebahagian daripada kumpulan standard ISO/IEC 27000 yang memberikan cadangan amalan terbaik mengenai pengurusan keselamatan maklumat. Standard khusus awan ISO/IEC 27017:2015 dibina berdasarkan dari standard ISO/IEC 27002 dan mengandungi kawalan keselamatan tambahan untuk awan yang tidak sepenuhnya ditentukan di dalam ISO/IEC 27002. Standard khusus awan ini menyediakan garis panduan pelaksanaan tambahan yang diperincikan mengikut peranan CSP dan CSU bagi 37 kawalan yang dinyatakan di dalam ISO/IEC 27002. Standard ini menekankan tanggungjawab bersama oleh CSP dan CSU ke atas keselamatan perkhidmatan pengkomputeran awan.

D. Cadangan Model Awal

Cadangan model awal bagi kajian ini adalah berdasarkan Kerangka Enam (6) Lapis [28], Model Kesediaan Perkhidmatan Awan (CSR) [29] dan kerangka pematuhan keselamatan awan [21]. Berdasarkan kajian kesusasteraan yang dilaksanakan kepada kerangka dan model dalam kajian lepas, sebanyak lima (5) domain telah dipilih bagi cadangan pembangunan model awal kajian ini. Domain yang telah dikenal pasti kemudiannya dipetakan ke atas 37 kawalan dalam standard ISO/IEC 27017:2015. Dengan memetakan kawalan dalam ISO/IEC 27017:2015 dengan lima (5) domain ini, ia berupaya membantu CSP bagi memahami kawalan keselamatan dengan cara yang lebih tersusun mengikut domain-domain tersebut. Perincian bagi setiap domain adalah seperti di Jadual 1 manakala cadangan model awal adalah seperti di Rajah 1.

JADUAL 1 PERINCIAN DOMAIN KESEDIAAN DARI KAJIAN LEPAS

Domain	Perincian dari Kajian Lepas
Teknologi	Perkhidmatan berasaskan teknologi dan penggunaan aplikasi yang merangkumi reka cipta, pengeluaran, penggunaan barangan dan perkhidmatan [28][29]. Aktiviti atau kajian yang menggunakan pengetahuan sains untuk tujuan praktis dlm industri, pertanian, perubatan, perniagaan dan lain-lain [30].
Budaya	Perkara yang menentukan apa yang boleh diterima atau tidak boleh diterima, penting atau tidak penting, betul atau salah dan samada boleh dilaksanakan atau tidak. Budaya organisasi ditakrifkan sebagai nilai dan tingkah laku yang menyumbang kepada persekitaran sosial dan psikologi yang unik dalam organisasi tersebut [28].
Undang-undang	Peraturan dan ketentuan yang digubal oleh sesuatu badan pemerintah atau perbadanan yang perlu dipatuhi oleh ahlinya [30].
Persekitaran	Merangkumi semua faktor di sekitar organisasi termasuk dari struktur ekonomi dan persaingan kepada persekitaran [31].



PENDEKATAN KAJIAN

Pendekatan kajian ini menggunakan gabungan kaedah kualitatif dan kuantitatif. Kajian ini dijalankan dalam tiga fasa utama yang terdiri daripada fasa kajian awal, fasa penentusahan dan fasa pengesahan. Teknik Delphi digunakan ketika fasa penentusahan manakala teknik pensampelan dilaksanakan ketika fasa pengesahan.

A. Pembangunan Model Awal

Pembangunan model awal dilaksanakan pada fasa kajian awal yang melibatkan kajian kesusasteraan melalui pembacaan dan menganalisis jurnal, artikel, prosiding dan sebarang maklumat yang berkaitan dengan pematuhan terhadap standard berkaitan pengkomputeran awan dan standard berkaitan sistem pengurusan keselamatan maklumat.

Terdapat lima (5) domain yang terbentuk hasil daripada model awal yang telah dibina berdasarkan kajian kesusasteraan. Lima (5) domain yang terdapat dalam model awal tersebut adalah teknologi, organisasi dan proses, budaya, undang-undang dan persekitaran. Model yang dibangunkan ini kemudiannya dibuat pemetaan dengan 37 kawalan berdasarkan standard khusus awan ISO/IEC 27017:2015.

B. Penentusahan Model Awal

Terdapat dua (2) proses yang dilalui di dalam fasa penentusahan iaitu proses mengumpul serta menentusahkan maklumat dan proses menganalisis data. Proses mengumpul dan menentusahkan maklumat dijalankan melalui kaedah kualitatif iaitu dengan menjalankan proses temu bual bersama pakar di dalam bidang pengurusan keselamatan maklumat dan pengkomputeran awan.

Analisis dan penilaian data dilaksanakan berdasarkan dapatan temu bual bersama dengan pakar. Data dikumpulkan daripada teknik Dephi dua (2) pusingan menggunakan panel pakar seramai tiga (3) orang. Teknik Delphi membolehkan persetujuan pakar diperoleh dalam menentukan domain dan pemetaan kawalan ke atas domain yang dipilih. Model awal tersebut akan diperbaiki mengikut cadangan penambahbaikan pakar dan seterusnya terhasil model yang telah ditambah baik. Model yang telah ditentusahkan ini adalah terdiri daripada domain dan senarai semak pematuhan penyedia perkhidmatan awan berdasarkan 37 kawalan ISO/IEC 27017:2015. Output bagi fasa penentusahan ini adalah pembangunan prototaip model akhir bersama senarai semak pematuhan berdasarkan model yang telah disahkan pakar.

C. Pengesahan Model Akhir

Proses pengesahan model akhir dilaksanakan melalui prototaip sebagai pembuktian konsep (Proof of Concept (POC)) dan melalui soal selidik bagi menilai keberkesanan dan kecekapan model. Pemilihan responden dalam fasa pengesahan ini dilaksanakan dengan menggunakan teknik pensampelan rawak. Sampel yang terlibat dalam proses pengujian prototaip ini melibatkan 10 orang pengamal dalam bidang keselamatan maklumat dan pengkomputeran awan yang dipilih berdasarkan agensi yang telah mendapatkan pensijilan ISMS dan dalam proses mendapatkan pensijilan ISMS khusus bagi perkhidmatan awan.

Model prototaip bagi kajian ini dibangunkan menggunakan perisian Microsoft Excel Home and Student 2016. Prototaip ini dibina dengan instrumen kajian yang terdiri daripada 37 kawalan dan 116 senarai semak yang dipetakan kepada lima (5) domain kajian. Responden dikehendaki menguji prototaip ini dan seterusnya melengkapkan borang soal selidik yang diedarkan secara bersama untuk mengesahkan keberkesanan dan kecekapan model prototaip kajian.

Borang soal selidik dibangunkan menggunakan aplikasi Google Form. Pemilihan soalan dan pengukuran bagi mengkaji tahap keberkesanan dan kecekapan prototaip dibuat berdasarkan dari matriks keberkesanan dan kecekapan [32] seperti di Rajah 2.

Cekap	7	Pembaziran	Berjaya
	0	Gagal	Tidak Cekap
		Berkesan	
		0	7

RAJAH 2 MATRIKS KEBERKESANAN DAN KECEKAPAN

Pengukuran keberkesanan dan kecekapan prototaip diukur menggunakan min. Disebabkan soal selidik adalah menggunakan skala likert dari 1 – Sangat Tidak Setuju hingga 7- Sangat Setuju, maka bagi pengiraan min, skor 4 dijadikan null bagi mengelakkan skor 4 (yang membawa maksud “Berkecuali”) mempengaruhi nilai min. Selain itu, ujian kebolehppercayaan menggunakan

Chronbach's Alpha juga dilaksanakan bagi mengukur kebolehppercayaan soal selidik yang digunakan dalam kajian ini seperti di Jadual 2 [33].

JADUAL 2: NILAI CHRONBACH'S ALPHA

Chronbach's Alpha	Interpretasi
$\alpha \geq 0.9$	Cemerlang
$0.9 \geq \alpha \geq 0.8$	Baik
$0.8 \geq \alpha \geq 0.7$	Boleh diterima
$0.7 \geq \alpha \geq 0.6$	Diragui
$0.6 \geq \alpha \geq 0.5$	Lemah
$0.5 \geq \alpha$	Tidak boleh diterima

HASIL PENGUJIAN

A. Analisis Penentusahan Pakar

Penentusahan oleh pakar melibatkan proses mendapatkan penentusahan model awal yang dibangunkan. Hasil penentusahan ini mendapati bahawa pakar bersetuju dengan lima (5) domain yang dicadangkan beserta 37 kawalan keselamatan awan dan instrumen senarai semak yang dibangunkan. Walau bagaimanapun, pakar mencadangkan penambahbaikan dibuat ke atas senarai semak sedia ada di subsekyen kawalan 7.2.2, 11.2.7 dan 12.1.2.

B. Analisa Pengesahan Model Akhir

Model akhir disahkan dengan menggunakan prototaip dan soal selidik kajian keberkesanan model kepada responden yang terdiri daripada pengamal yang berpengalaman dalam bidang pengkomputeran awan dan pengurusan keselamatan maklumat. Seramai sepuluh (10) orang responden yang terdiri daripada empat (4) orang juruaudit dan enam (6) orang pihak yang diaudit (auditee) terlibat dalam pengesahan prototaip. Proses pengesahan dilaksanakan dengan menguji keberkesanan dan kecekapan penggunaan prototaip oleh agensi terhadap kesemua 116 senarai semak yang dibentuk daripada 37 kawalan yang dipetakan ke atas lima (5) domain yang terdiri daripada domain teknologi, organisasi dan proses, budaya, undang-undang dan persekitaran.

Nilai skor yang diperolehi hasil daripada penggunaan prototaip oleh responden adalah tidak penting bagi tujuan statistik tetapi adalah untuk menggambarkan bahawa responden yang merupakan pengamal dalam bidang keselamatan awan telah menggunakan prototaip yang dibangunkan sebagai POC dan bagi mengesahkan model akhir.

C. Pengesahan Model melalui Prototaip

Sesi pengesahan dilaksanakan untuk menilai tahap keberkesanan dan kecekapan prototaip yang telah dibangunkan melalui soal selidik ke atas responden. Soal selidik tersebut mempunyai empat (4) bahagian utama yang wajib dijawab oleh setiap responden. Perincian borang adalah seperti di dalam Jadual 3.

JADUAL 3 PERINCIAN BORANG PENILAIAN PROTOTAIP MODEL

Bahagian	Jumlah Soalan	Skala Jawapan
A: Maklumat Responden	5	-
B: Keberkesanan Prototaip	8	Skala 1 – 7
C: Kecekapan Prototaip	7	Skala 1 – 7
D: Penilaian Keseluruhan Prototaip	6	Skala 1 – 7

Hasil bagi ujian kebolehpercayaan dengan menggunakan Chronbach's Alpha pada item di setiap bahagian adalah seperti di Jadual 4.

JADUAL 4 KEPUTUSAN UJIAN CHRONBACH'S ALPHA PADA SETIAP BAHAGIAN

Bahagian	Chronbach's Alpha	Bilangan Item
B: Keberkesanan Prototaip	0.902	8
C: Kecekapan Prototaip	0.944	7
D: Penilaian Keseluruhan Prototaip	0.966	4

Hasil analisis kebolehpercayaan berdasarkan keputusan ujian Chronbach's Alpha yang dilaksanakan mendapati ketiga-tiga bahagian soal selidik iaitu bahagian keberkesanan prototaip, kecekapan prototaip dan penilaian keseluruhan prototaip mencatatkan nilai $\alpha \geq 0.9$ iaitu berada dalam kategori cemerlang. Ini menunjukkan setiap item di dalam soal selidik pada setiap bahagian mempunyai keseragaman dan saling berkaitan antara satu sama lain. Ujian keberkesanan juga turut dibuat ke atas keseluruhan 19 item yang terlibat di dalam soal selidik dan nilai Chronbach's Alpha yang dihasilkan adalah 0.965 iaitu cemerlang seperti ditunjukkan di Jadual 5.

JADUAL 5 KEPUTUSAN UJIAN CHRONBACH'S ALPHA PADA KESELURUHAN ITEM

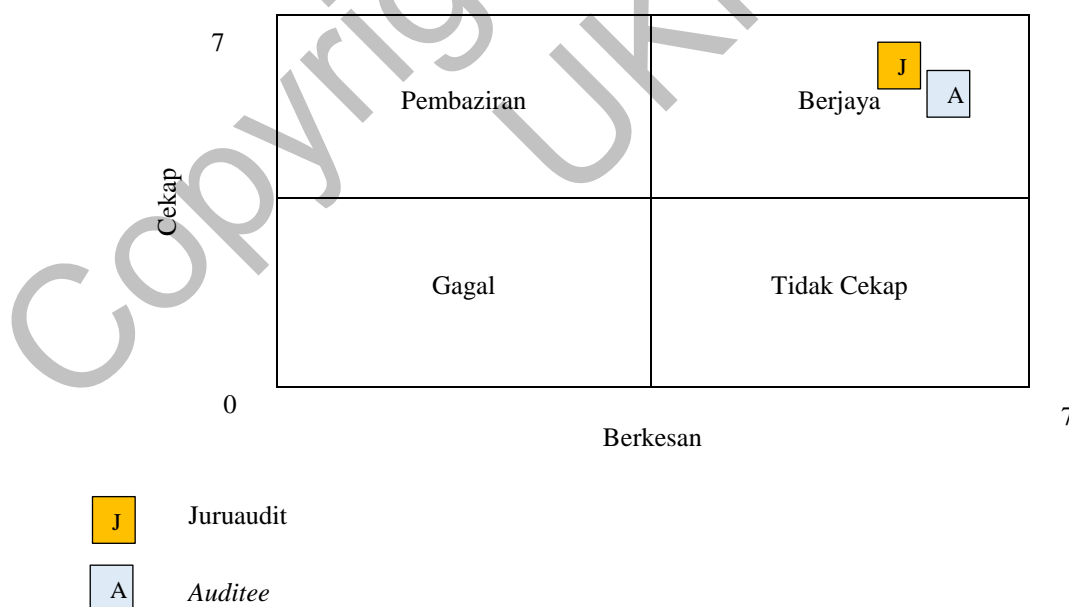
Chronbach's Alpha	Bilangan Item
0.965	19

Hasil soal selidik juga mendapati bahawa kesemua responden bersetuju bahawa prototaip tahap pematuhan keselamatan awan berdasarkan standard ISO/IEC 27017:2015 sesuai digunakan oleh Agensi sebagai panduan bagi tujuan audit keselamatan perkhidmatan awan. Berdasarkan maklumbalas responden ke atas soal selidik, pengiraan min keseluruhan bagi keberkesanan dan kecekapan prototaip dilaksanakan seperti di dalam Jadual 6.

JADUAL 6 PENGUKURAN MIN BAGI RESPONDEN

	Min Juruaudit	Min Auditee
Keberkesanan	5.59	5.77
Kecekapan	5.93	5.86

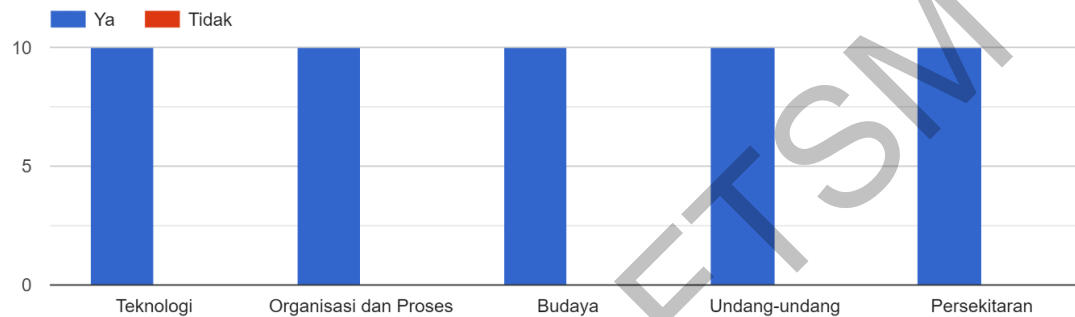
Hasil daripada pengiraan min bagi responden yang terdiri daripada juruaudit dan auditee tersebut diplotkan kepada matriks keberkesanan dan kecekapan seperti di dalam Rajah 3. Keputusan daripada pengiraan min berdasarkan soal selidik terhadap prototaip mendapati ianya berada pada tahap berjaya.



RAJAH 3 PENGUKURAN TAHAP KEBERKESANAN DAN KECEKAPAN PROTOTAIP

Bagi penilaian keseluruhan prototaip, 100% responden bersetuju bahawa kelima-lima domain yang disenaraikan membantu Agensi dalam penilaian audit pematuhan tahap keselamatan perkhidmatan awan seperti yang ditunjukkan di dalam Rajah 5.

1. Adakah domain-domain yang disenaraikan membantu Agensi dalam penilaian audit pematuhan tahap keselamatan perkhidmatan awan?



RAJAH 5 HASIL PENILAIAN DOMAIN

KESIMPULAN

A. Rumusan dan penemuan

Kajian yang dijalankan telah berjaya menjawab persoalan kajian yang telah digariskan seterusnya membolehkan objektif kajian dipenuhi.

1) *Objektif pertama kajian adalah mengenal pasti domain utama dalam menilai tahap pematuhan penyedia perkhidmatan awan terhadap keselamatan awan berdasarkan standard kawalan keselamatan awan ISO/IEC 27017:2015 melalui kajian kesusasteraan yang dilaksanakan yang berjaya mengenalpasti lima (5) domain bagi menghasilkan model awal. Model awal yang terhasil terdiri daripada lima domain iaitu teknologi, organisasi dan proses, undang-undang, budaya dan persekitaran. Seterusnya, domain-domain ini dipetakan ke atas standard kawalan ISO/IEC 27017:2015 untuk membentuk instrumen kajian.*

2) *Objektif kedua kajian adalah membangunkan model senarai semak pematuhan audit keselamatan awan bagi CSP berdasarkan standard ISO/IEC 27017:2015 dicapai melalui penentuan model awal oleh pakar dengan menghubungkan domain yang telah dikenalpasti dengan kawalan ISO/IEC 27017:2015. Pakar-pakar yang terlibat adalah daripada bidang keselamatan pengurusan maklumat dan pengkomputeran awan.*

3) *Objektif ketiga kajian adalah mengesahkan model yang dibangunkan dengan pakar bidang bagi memastikan keberkesanan model dengan melaksanakan proses pengesahan model akhir menggunakan prototaip yang dibangunkan sebagai pembuktian konsep (POC). Bagi mengesahkan model dan memastikan keberkesanan dan kecekapan prototaip, para pengamal tersebut diminta untuk menjawab dan melengkapkan borang soal selidik yang berkaitan. Hasil analisis mendapati semua pengamal yang terlibat dalam kajian bersetuju bahawa model yang dihasilkan adalah berkesan dan cekap. Kesemua pengamal atau responden juga bersetuju bahawa model yang dihasilkan dapat membantu mengukur tahap pematuhan audit keselamatan awan di agensi berdasarkan standard kawalan ISO/IEC 27017:2015.*

B. Sumbangan

Kajian ini diharap dapat memberi sumbangan kepada persediaan agensi CSP semasa pelaksanaan audit keselamatan pengkomputeran awan seperti berikut:

- i) Model dijadikan sebagai garis panduan dalam memastikan perkhidmatan pengkomputeran awan yang disediakan sentiasa dalam keadaan selamat dan terjamin;
- ii) Penggunaan prototaip yang dibangunkan berupaya memberikan maklumat yang relevan ketika melaksanakan audit keselamatan awan di agensi berdasarkan senarai semak yang terhasil dari standard kawalan ISO/IEC 27017:2015; dan
- iii) Prototaip dapat membantu pelaksanaan audit keselamatan perkhidmatan pengkomputeran awan berdasarkan domain-domain yang telah dikenal pasti iaitu teknologi, organisasi dan proses, undang-undang, budaya dan persekitaran.

C. Cadangan dan Kajian Masa Depan

Satu model bagi menilai tahap pematuhan penyedia perkhidmatan awan terhadap keselamatan awan berdasarkan standard kawalan keselamatan awan ISO/IEC 27017:2015 telah dihasilkan berdasarkan pemetaan kawalan dengan lima domain iaitu teknologi, organisasi dan proses, undang-undang, budaya dan persekitaran. Walau bagaimanapun, untuk penyelidikan masa hadapan, kajian lanjutan dicadangkan untuk dilaksanakan dengan penekanan kepada isu privasi dan juga tujuh kawalan keselamatan baru yang terdapat dalam standard kawalan ISO/IEC 27017:2015 dalam mengukur tahap pematuhan keselamatan awan bagi CSP.

RUJUKAN

- [1] Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology. *NIST Spec. Publ* 145(1-7).
- [2] Salasiah, A. & Khairul Azmi, A. B. 2018. Security and Privacy Challenges in Cloud Computing. *2018 Cyber Resilience Conference (CRC)*, hlm. 1-3.
- [3] Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y. & Vasilakos, A. V. 2014. Security and Privacy for Storage and Computation in Cloud Computing. *Information Sciences* 258(371-386).
- [4] Khan, N. & Al-Yasiri, A. 2016. Identifying Cloud Security Threats to Strengthen Cloud Computing Adoption Framework. *Procedia Computer Science* 94(485-490).
- [5] Giulio, C. D., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R. H. & Bashir, M. N. 2017. Cloud Standards in Comparison: Are New Security Frameworks Improving Cloud Security? *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, hlm. 50-57.
- [6] Moravcik, M., Segec, P. & Kontsek, M. 2018. Overview of Cloud Computing Standards. *2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, hlm. 395-402.
- [7] Schmidt-Wesche, B., Bleizeffer, T., Calcaterra, J., Nair, D., Rendahl, R. & Sohn, P. 2011. Cloud User Roles: Establishing Standards for Describing Core Tasks of Cloud Creators, Providers, and Consumers. *2011 IEEE 4th International Conference on Cloud Computing*, hlm. 764-765.
- [8] Iankoulova, I. & Daneva, M. 2012. Cloud Computing Security Requirements: A Systematic Review. *2012 Sixth International Conference on Research Challenges in Information Science (RCIS)*, hlm. 1-7.
- [9] Narang, A. & Gupta, D. 2019. A Review on Different Security Issues and Challenges in Cloud Computing. *2018 International Conference on Computing, Power and Communication Technologies, GUCON 2018*, hlm. 121-125.
- [10] Rizvi, S., Ryoo, J., Kissell, J., Aiken, W. & Liu, Y. H. 2018. A Security Evaluation Framework for Cloud Security Auditing. *Journal of Supercomputing* 74(11): 5774-5796.
- [11] Tajammul, M. & Parveen, R. 2017. Comparative Analysis of Big Ten Isms Standards and Their Effect on Cloud Computing. *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, hlm. 362-367.
- [12] Al-Anzi, F. S., Yadav, S. K. & Soni, J. 2014. Cloud Computing: Security Model Comprising Governance, Risk Management and Compliance. *2014 International Conference on Data Mining and Intelligent Computing (ICDMIC)*, hlm. 1-6.
- [13] Kandira, M., Mtsweni, J. & Padayachee, K. 2013. Cloud Security and Compliance Concerns: Demystifying Stakeholders' Roles and Responsibilities. *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*, hlm. 653-658.
- [14] Al-Ruithe, M., Benkhelifa, E. & Hameed, K. 2019. A Systematic Literature Review of Data Governance and Cloud Data Governance. *Personal and Ubiquitous Computing* 23(5-6): 839-859.
- [15] Narang, A. & Gupta, D. 2019. A Review on Different Security Issues and Challenges in Cloud Computing. *2018 International Conference on Computing, Power and Communication Technologies, GUCON 2018*, hlm. 121-125.

- [16] Grispos, G., Glisson, W. B. & Storer, T. 2013. Cloud Security Challenges: Investigating Policies, Standards, and Guidelines in a Fortune 500 Organization. *ECIS 2013 - Proceedings of the 21st European Conference on Information Systems*, hlm.
- [17] Diver, S. 2007. Information Security Policy a Development Guide for Large and Small Companies. SANS Institute.
- [18] SKMM. 2018. Technical Code Information & Network Security- Cloud Service Provider Selection.
- [19] Bryce, C. 2018. Security Governance as a Service on the Cloud. *2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion)*, hlm. 30-35.
- [20] Lins, S., Schneider, S. & Sunyaev, A. 2018. Trust Is Good, Control Is Better: Creating Secure Clouds by Continuous Auditing. *IEEE Transactions on Cloud Computing* 6(3): 890-903.
- [21] Brandis, K., Dzombeta, S., Colomo-Palacios, R. & Stantchev, V. 2019. Governance, Risk, and Compliance in Cloud Scenarios. *Applied Sciences (Switzerland)* 9(2):
- [22] Ryoo, J., Rizvi, S., Aiken, W. & Kissell, J. 2014. Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Security & Privacy* 12(6): 68-74.
- [23] Cybersecurity Malaysia 2013. ISMS Implementation Guideline: A Practical Approach.
- [24] Cybersecurity Malaysia. 2020. CNII Portal. [18 Julai 2020].
- [25] De Hert, P., Papakonstantinou, V. & Kamara, I. 2016. The Cloud Computing Standard Iso/Iec 27018 through the Lens of the Eu Legislation on Data Protection. *Computer Law & Security Review* 32(1): 16-30.
- [26] Weil, T. 2018. Taking Compliance to the Cloud—Using ISO Standards (Tools and Techniques). *IT Professional* 20(6): 20-30.
- [27] Chemerkin, Y. 2013. Security Compliance Challenges on Clouds. *Proceedings of the 5th International Conference on Internet Technologies and Applications, ITA 2013*, hlm. 131-145
- [28] Susanto, H., Almunawar, M. N. & Tuan, Y. C. 2012. A Novel Method on Iso 27001 Reviews: Isms Compliance Readiness Level Measurement. *Computer Science Journal* 2(1):
- [29] Nur Ilyani Ahmad, Ibrahim Mohamed, Maslina Daud, Ahmad Dahari Jarno & Norlaili Abdul Hamid. 2019. Cloud Service Provider Security Readiness Model: The Malaysian Perspective. *2019 International Conference on Electrical Engineering and Informatics (ICEEI)*, hlm. 75-80.
- [30] Dewan Bahasa Dan Pustaka 2005. Kamus Dewan. Kuala Lumpur, Dewan Bahasa dan Pustaka. Edisi Keempat.
- [31] Borgman, H. P., Bahli, B., Heier, H. & Schewski, F. 2013. Cloudrise: Exploring Cloud Computing Adoption and Governance with the Toe Framework. *2013 46th Hawaii international conference on system sciences*, hlm. 4425-4435.
- [32] Ibrahim Mohamed. 2013. Business Process Modelling with the Source-Transaction-Agent (S.T.A.) Data Modelling. Kulliyah of Information and Communication Technology, International Islamic University Malaysia.
- [33] George, D. & Mallery, P. 2003. Spss for Windows Step-by-Step: A Simple Guide and Reference, 14.0 Update (7th Edition). [http://lst-iiiep.iiep-unesco.org/cgi-bin/wwwi32.exe/\[in=epidoc1.in\]/?t2000=026564/\(100\)](http://lst-iiiep.iiep-unesco.org/cgi-bin/wwwi32.exe/[in=epidoc1.in]/?t2000=026564/(100))