MODEL KESEDIAAN PENYEDIA PERKHIDMATAN AWAN TERHADAP STANDARD PRIVASI AWAN

Noor Asmah binti Halimi
haliminoorasmah@gmail.com

Ibrahim bin Mohamed
ibrahim@ukm.edu.my

ABSTRAK

Internet merupakan teknologi paling popular yang telah menjadi sebahagian besar daripada Industri Teknologi Maklumat (TM) serta memudahkan pengkongsian maklumat dalam masa yang singkat melalui pengkomputeran awam. Pengkomputeran awan menyediakan kaedah penyimpanan yang elakstik, yang fleksibel membolehkan data diakses diuruskan oleh sesiapa yang mempunyai sumber dan mengikut permintaan pelanggan. Sebagai teknologi yang baru mucul, pengkomputeran awan juga menghadapi cabaran keselamatan dan privasi yang luar biasa, menghalang penggunaannya berkembang dengan lebih pesat. Banyak organisasi enggan menggunakan teknologi pengkomputeran awan kerana isu keselamatan, privasi, dan kepercayaan yang wujud serta risiko pengawalseliaan dan implikasi pematuhan. Bagi meningkatkan keyakinan pengguna perkhidmatan awan (CSU) terhadap privasi dan keselamatan penyedia perkhidmatan awan (CSP) hendaklah menggunakan piawaian keselamatan seperti standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001:2013 dan Standard berkaitan keselamatan pengkomputeran awan seperti ISO/IEC 27017:2015 dan Standard berkaitan perlindungan maklumat pengenalan peribadi (PII) ISO/IEC 27018:2015 dalam menguruskan privasi dan keselamatan maklumat pengguna. Kajian ini bertujuan untuk mengenal pasti faktor domain yang mempengaruhi tahap kesediaan CSP terhadap standard privasi dan juga mengesahkan model melalui pengujian keberkesanan dan kecekapan prototaip berdasarkan 39 kawalan standard ISO/IEC 27018:2019 Pemakaian kod amalan perlindungan maklumat pengenalan peribadi (PII).Enam domain utama yang mempengaruhi penilaian tahap kesediaan CSP terhadap standard privasi iaitu Teknologi & Privasi, Organisasi & Privasi, Dasar & Privasi, Pemegang Taruh & Privasi, Budaya & Privasi, Pengetahuan & Privasi Dan Persekitaran & Privasi. Berdasarkan 39 kawalan yang dipetakan kepada enam domain, satu model senarai semak tahap kesediaan CSP terhadap standard privasi berdasarkan ISO/IEC 27018 :2015 berjaya dihasilkan. Model ini dapat membantu organisasi CSP sebagai garis panduan dalam melaksanakan audit privasi awan seterusnya meningkatkan kepercayaan CSU dalam menggunakan perkhidmatan pengkomputeran awam.

Kata kunci—pengkomputeran awan;privasi awan, keselamatan awan; kesediaan awan, ISO/IEC 27017 dan ISO/IEC 27018.

PENGENALAN

Pengkomputeran awam merupakan teknologi paling popular yang telah menjadi sebahagian besar daripada Industri Teknologi Maklumat (TM) serta memudahkan pengkongsian maklumat atau data dalam masa yang singkat (Saeed et al. 2019). Pengkomputeran awan juga digunakan untuk menyimpan, memproses dan bertukar maklumat mengenai permintaan dalam rangkaian atau

organisasi (Tubaishat 2019). Organisasi dengan belanjawan yang rendah kini boleh menggunakan perkhidmatan pengkomputeran awan dan storan tinggi tanpa banyak pelaburan dalam infrastruktur dan penyelenggaraan (Ali et al. 2017).

Pengurusan teknologi dan perkhidmatan juga menjadi lebih mudah apabila pelanggan menyerahkan pengurusan mereka kepada penyedia perkhidmatan (Ali et al. 2017). Walaupun mempunyai kelebihan sebagai teknologi yang baru mucul, pengkomputeran awan juga menghadapi cabaran keselamatan dan privasi yang luar biasa, yang menghalang penggunaannya berkembang dengan lebih pesat (Liu et al. 2012; Ristov & Gusev 2015). Ini disokong oleh kajian lampau Ren et al. (2012) bahawa banyak organisasi enggan menggunakan teknologi pengkomputeran awan kerana isu keselamatan, privasi, dan kepercayaan yang wujud serta risiko pengawalseliaan dan implikasi pematuhan.

Bagi mengurangkan tahap kebimbangan dan meningkatkan keyakinan organisasi dalam keselamatan Penyedia Perkhidmatan Awan (CSP), CSP harus menggunakan standard atau standard keselamatan untuk menangani masalah keselamatan, privasi dan kepercayaan yang membolehkan organisasi menilai CSP terbaik untuk memenuhi keperluan keselamatan mereka (Giulio et al. 2017).

Peraturan dan pengawasan yang efektif serta penguatkuasaan peraturan privasi data adalah aspek penting dalam kesediaan awan ini kerana perkhidmatan pengkomputeran awan memerlukan aliran data yang selamat dan boleh dipercayai untuk melintasi sempadan, rangkaian dan penyedia pihak ketiga bagi menjamin privasi data awan tersebut. Pengguna hanya akan menggunakan perkhidmatan pengkomputeran awan jika maklumat mereka selamat dan disimpan secara peribadi tanpa ada pelanggaran yang tidak dijangka. Peraturan dan pengawasan yang efektif dan penguatkuasaan peraturan privasi data adalah aspek penting dalam kesediaan awan (ACCA 2020).

Salah satu pendekatan yang dicadangkan oleh Nur Ilyani Ahmad et al. (2019) bagi menyelesaikan masalah ini ialah dengan melaksanakan pengauditan keselamatan terhadap CSP. Kenyataan ini turut disokong oleh Pauley (2010) yang menyatakan pengguna awan boleh menilai ketelusan Penyedia Perkhidmatan Awan berdasarkan penggunaan standard, amalan terbaik, dasar dan prosedur yang berkaitan dengan keselamatan, privasi, audit dan tahap perkhidmatan.Di antara standard atau standard keselamatan awan termasuk ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, Cloud Security Alliance (CSA) dan Program Pengurusan Risiko dan Kebenaran Persekutuan (FedRAMP). Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001 memainkan peranan utama dalam pengurusan dan pensijilan keselamatan maklumat dalam sesebuah

organisasi. Meningkatkan standard ISMS dalam persekitaran pengkomputeran awan boleh meningkatkan keyakinan organisasi (Pandey 2016). ISO/IEC 27001 ditakrifkan sebagai keperluan mandatori Sistem Pengurusan Keselamatan Maklumat (ISMS).

Kajian ini mendapati kajian kesusasteraan sedia ada hanya membangunkan model kesediaan untuk sistem pengurusan keselamatan maklumat (ISMS) berdasarkan standard ISO/IEC 27001 dan ISO/IEC 27002 (Susanto et al. 2012) yang tidak meliputi kawalan terhadap awan (Tariq & Santarcangelo 2016) dan hanya meliputi kesediaan dari segi teknologi (Oliveira et al. 2014). Manakala kajian yang berkaitan dengan tahap kesediaan CSP terhadap pematuhan keselamatan awan hanya dibangunkan untuk memfokuskan 37 kawalan yang terdapat di dalam standard ISO/IEC 27017 (Nur Ilyani Ahmad et al. 2019).

Di antara standard atau standard keselamatan awan termasuk ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017, Cloud Security Alliance (CSA) dan Program Pengurusan Risiko dan Kebenaran Persekutuan (FedRAMP). Standard Sistem Pengurusan Keselamatan Maklumat (ISMS) ISO/IEC 27001 memainkan peranan utama dalam pengurusan dan pensijilan keselamatan maklumat dalam sesebuah organisasi. Meningkatkan standard ISMS dalam persekitaran pengkomputeran awan boleh meningkatkan keyakinan organisasi (Pandey 2016). ISO/IEC 27001 ditakrifkan sebagai keperluan mandatori Sistem Pengurusan Keselamatan Maklumat (ISMS).

Berdasarkan kajian kesusasteraan yang dibincangkan di atas, penerapan penyelesaian berdasarkan standard ISO/IEC 27001, ISO/IEC 27002 dan ISO/IEC 27017 kepada persekitaran pengkomputeraan awan tidak dapat dinafikan, tetapi tidak mencukupi untuk sepenuhnya melindungi semua privasi dan keselamatan maklumat CSU. Penilaian kesediaan privasi dan keselamatan CSP belum diteliti secara mendalam dalam kajian kepustakaan sedia ada. Justeru itu, satu model kesediaan yang komprehensif dan konsisten meliputi aspek Organisasi, Teknologi, Polisi, Privasi, Budaya, Pemegang Taruh, Pengetahuan dan Persekitaran perlu dibangunkan bagi menilai tahap kesediaan CSP terhadap pematuhan privasi awan yang boleh dijadikan sebagai panduan dalam menghadapi persediaan audit privasi dan keselamatan awan serta menyediakan asas praktikal untuk menggalakkan keyakinan terhadap perkhidmatan awan. Pada masa yang sama, CSP awam akan mempunyai panduan yang jelas untuk memenuhi beberapa kebimbangan undang-undang dan kawal selia pelanggannya.

KAJIAN LAMPAU YANG BERKAITAN

A. Pengkomputeran Awan

Pengkomputeran awan menawarkan tiga jenis model perkhidmatan iaitu Perisian sebagai Service (SaaS), Platform sebagai Perkhidmatan (PaaS) dan Prasarana sebagai Perkhidmatan (IaaS). SaaS adalah yang tertinggi tahap pengkomputeran awan di mana semua perkhidmatan ditawarkan oleh penyedia pengkomputeran awan. Pengguna yang menggunakan PaaS sahaja menguruskan aplikasi dan data mereka dan yang lain menggunakan IaaS akan mempunyai infrastruktur mereka seperti pelayan, penyimpanan dan rangkaian yang dijalankan oleh penyedia (Ryoo et al. 2013).

Terdapat tiga (3) model pengkomputeran awan iaitu Pengkomputeran Awan Awam (Public Cloud), Pengkomputeran Awan Persendirian (Private Cloud) dan Pengkomputeran Awan Hibrid (Hybrid Cloud). Di Pengkomputeran Awan Awam (Public Cloud), semua perkhidmatan yang ditawarkan oleh penyedia adalah dikongsi bersama dengan semua pengguna awan. Manakan Pengkomputeran Awan Persendirian (Private Cloud) digunakan apabila pengguna perlu meningkatkannya keselamatan data di mana pengkomputeran awan disediakan secara eksklusif untuk mereka. Pengkomputeran Awan Hibrid (Hybrid Cloud) adalah gabungan kedua-duanya Pengkomputeran Awan (Public Cloud) dan Pengkomputeran Awan Persendirian (Private Cloud). Penerimaan penggunaan dan perkhidmatan pengkomputeran awan yang ditawarkan bergantung pada keperluan dan kehendak organisasi (Hanifah Abdul Hamida & Mokhtar Mohd Yusofa 2015).

B. Isu Pengkomputeran Awan

Privasi adalah isu dan cabaran utama dalam pengkomputeran awan termasuk perlu melindungi identiti dengan teratur, strategi komponen semasa integrasi dan transaksi sejarah. Eksploitasi pencurian identiti yang berjaya dapat mengakibatkan kehilangan privasi yang mempengaruhi organisasi kerana kehilangan kredibiliti dengan keyakinan dan negatif publisiti. Mekanisme perlindungan privasi mestilah tertanam dalam semua penyelesaian keselamatan awan (Singh & Singh 2018; Upadhyay & Jain 2015)

C. Risiko Teratas Keselamatan Pengkomputeran Awam

Penggunaan pengkomputeran awan menjadi semakin lazim dalam industri masa kini, menjadikan persekitaran pengkomputeran mempunyai risiko dan cabaran keselamatan. Rajah 1 menunjukkan sepuluh (10) risiko keselamatan pengkomputeran awan OWASP bertujuan untuk membantu industri dan organisasi melaksanakan amalan terbaik dan selamat ketika ingin menggunakan penyelesaian berasaskan awan sambil memanfaatkan faedah penjimatan kos yang disediakan oleh model SaaS.

Rajah 1 Sepuluh (10) risiko keselamatan pengkomputeran awan OWASP

Sumber: Zaydi & Nasserddine (2016)

D. Ancaman Teratas Pengkomputeran Awan

Computer Security Alliance (CSA) telah melancarkan penyelidikan baru ancaman teratas untuk pengkomputeran awan pada tahun 2020 (CSA 2020). Jadual 1 menunjukan untuk sebelas (11) ancaman teratas pengkomputeran awan pada tahun 2020 menurut susunan.

Jadual 1 Ancaman teratas pengkomputeran awan pada tahun 2020

No	Ancaman Keselamatan Pengkomputeran Awan
1	Pelanggaran Data
2	Salah Konfigurasi Dan Kawalan Perubahan Yang Tidak Mencukupi.
3	Kekurangan Seni Bina Dan Strategi Keselamatan Awan
4	Identiti, Kelayakkan, Akses Dan Pengurusan Utama Yang Tidak Cukup
5	Rampasan Akaun
6	Antaramuka Dan Api Yang Tidak Selamat
7	Ancaman Orang Dalam
8	Kawalan yang lemah
9	Kegagalan Metastruktur dan Pentadbiran
10	Terhad Keterlihatan Penggunaan Awan
11	Penyalahgunaan dan Penggunaan Perkhidmatan Pengkomputeran Awan yang Tidak Betul

Sumber: CSA (2020)

E. Cadangan Model Pematuhan Keselamatan Berdasarkan Ancaman Keselamatan

Daripada sebelas (11) ancaman teratas pengkomputeran awan pada tahun 2020 mendapati pelanggaran data berada pada tangga pertama, pelanggaran data adalah kejadian keselamatan siber di mana maklumat sensitif, dilindungi atau sulit dilepaskan, dilihat, dicuri atau digunakan oleh individu yang tidak dibenarkan. Pelanggaran data mungkin merupakan tujuan utama serangan yang disasarkan atau hanya akibat kesalahan manusia, kerentanan aplikasi atau amalan keselamatan yang

tidak mencukupi. Pelanggaran data melibatkan apa-apa jenis maklumat yang tidak dimaksudkan untuk dikeluarkan oleh orang ramai, termasuk tetapi tidak terbatas pada maklumat kesihatan diri, maklumat kewangan, maklumat peribadi (PII), rahsia perdagangan dan harta intelek (CSA, 2020). Penyelidik Hendre & Joshi (2015) telah menganalisis ancaman keselamatan dan dokumen awam lain dari badan standard, untuk menentukan ancaman yang dihadapi oleh pengguna awan, penyelidik telah mengaitkannya dengan cadangan model kawalan keselamatan dan kepatuhan yang melindungi dari ancaman ini. Daripada penyelidikan Hendre & Joshi (2015) dapat dirumuskan cadangan model pematuhan keselamatan bagi pelanggaran data adalah menggunakan standard ISO/IEC 27001. Standard ISO/IEC 27001: 2013 Information Security Management Systems – Requirements. merupakan panduan utama bagi pelaksanaan ISMS yang menitikberatkan aspek dan prinsip keselamatan maklumat melalui pemeliharaan kerahsiaan, integriti dan kebolehsediaan (I.S.O./I.E.C. 2013).

F. ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO/IEC 27017:2015 dan ISO/IEC 27018:2019

ISO/IEC27001:2013 merupakan panduan utama bagi keselamatan teknologi maklumat dan ISO/IEC 27002:2013 merupakan pelengkap kepada ISO/IEC 27001:2013 dalam melaksanakan kawalan keselamatan alternatif yang sesuai dengan organisasi. Manakala bagi standard pengkomputeran awan ISO/IEC 27017:2015 merupakan kod amalan untuk kawalan keselamatan maklumat berasaskan daripada ISO/IEC 27002:2013 dengan memfokuskan kepada kawalan keselamatan pengkomputeran awan. ISO/IEC 27018:2019 merupakan standard di pengkomputeran awan umum yang boleh digunakan sebagai "amalan terbaik" standard panduan untuk melindungi PII. Sehingga tahun 2019 sebanyak 36,362 sijil yang sah bagi 68,930 lokasi ISO/IEC 27001:2013 diguna pakai secara meluas di seluruh dunia (I.S.O./I.E.C. 2019). Oleh itu, standard ini merupakan instrumen yang sesuai untuk kajian pematuhan kerana merangkumi skop yang lebih luas dan sesuai untuk organisasi dari pelbagai sektor dan saiz.

KERANGKA DAN MODEL BERKAITAN TEKNOLOGI MAKLUMAT

A. Kerangka Teknologi Organisasi Persekitaran (TOE)

Hasimi Sallehudin et al. (2018) menyatakan Kerangka Teknologi Organisasi Persekitaran (TOE) yang dibangunkan oleh Tornatzky dan Fleischer pada tahun 1990 merupakan satu model penerapan teknologi yang menjadi asas bagi banyak penyiasatan sistem maklumat (IS) bagi sesebuah organisasi. Berdasarkan kerangka ini, keputusan yang dibuat dalam organisasi dipengaruhi oleh tiga (3) elemen yang terdiri daripada teknologi, organisasi dan persekitaran.

B. Kerangka Penilaian Kesediaan Awan

Kerangka ini dibina berasaskan gabungan kerangka TOE dan DOI serta model TAM (Alemeye & Taddesse 2015). Hasil gabungan ini menghasilkan 12 faktor kesediaan untuk menentukan kesediaan awan organisasi iaitu Perceived Usefulness (PU), Perceived Ease of Use (PE), dan Relative Advantage (RA) dari model TAM; Trial- Ability Observable Result (TO) dan Compatibility with Existing Values and Practices (CE) dari kerangka DOI; serta Executive Support (ES), Business Case and Budget (BB), Technological Readiness Number of Servers (TRNS), Technological Readiness Server Age (TRSA), Technological Readiness Virtualization (TRVI), Network Connectivity (CO) dan Competitive Edge (CA) dari kerangka TOE.

C. Kerangka Enam Lapis

Kerangka Enam Lapis terdiri dari enam (6) domain iaitu Organisasi (Organisation, O), Pemegang Taruh (Stakeholders, S), Alat dan Teknologi (Technology, T), Dasar (Policy, P), Budaya (Culture, C) dan Pengetahuan (Knowledge, K) digunakan sebagai elemen asas dalam penilaian tahap kesediaan organisasi dalam pelaksanaan pensijilan ISMS (Susanto et al. 2012) Kerangka ini menggunakan 21 kawalan keselamatan penting di ambil dari standard pengurusan keselamatan maklumat dalam ISO27001.

D. Rangka Kerja Pelaksanaan RMfIC

Rangka kerja ini terdiri daripada empat (4) peringkat bermula dari penerangan dan tujuan RMfIC; pelaksanaan komponen 1 iaitu menganalisis kesesuaian ke atas organisasi; komponen 2 untuk menguji instrumen nilai kesediaan organisasi (INKO); serta komponen 3 bagi pengiraan INKO dan menentukan tahap kesediaan organisasi (SPKO) (Asma Zubaida M. Ibrahim et al. 2018).

E. Model Keselamatan Awan Hexagonal

Model ini terdiri enam (6) elemen asas dan dua (2) elemen tambahan ketahanan, ketersediaan, kesahihan, kerahsiaan, utiliti, pemilikan, integriti dan keselamatan (Bhatia & Malhotra 2018). Model ini membantu CSP untuk membuat penilaian risiko berdasarkan kepada kemungkinan ancaman yang berlaku.

F. Model Kesediaan Keselamatan Awan

Model ini juga dibangunkan berdasarkan gabungan satu (1) asas teori yang popular mengenai Kerangka Teknologi Organisasi Persekitaran (TOE) (Tornatzky & Fleischer 1990) dan Kerangka Enam Lapis (Susanto et al. 2012). Kerangka TOE ini terdiri daripada domain Teknologi, Organisasi dan Persekitaran. Manakala Kerangka Enam Lapis ini terdiri dari enam (6) domain iaitu Organisasi (Organisation, O), Pemegang Taruh (Stakeholders, S), Alat & Teknologi (Technology, T), Dasar

(Policy, P), Budaya (Culture, C) dan Pengetahuan (Knowledge, K). Nur Ilyani Ahmad (2019) telah menambahbaik Kerangka Enam Lapis dengan mengintegrasikan dengan kerangka TOE untuk menghasilkan Model Kesediaan Keselamatan Awan. Model Kesediaan Keselamatan Awan adalah terdiri daripada 37 kawalan yang dinyatakan dalam standard ISO/IEC 27017 dan dikumpulkan ke dalam 7 domain iaitu Organisasi (Organisation, O), Pemegang Taruh (Stakeholders, S), Alat & Teknologi (Technology, T), Dasar (Policy, P), Budaya (Culture, C) dan Pengetahuan (Knowledge, K) dan Persekitaran (Environment, E)

KRITERIA PEMILIHAN DOMAIN MENYUMBANG PRIVASI AWAN

Berdasarkan kajian kesusasteraan yang dilaksanakan ke atas kerangka dan model dalam kajian lepas, sebanyak tujuh (7) domain telah dipilih bagi cadangan pembangunan model awal kajian ini. Pemilihan domain-domain ini berdasarkan kepada kajian terdahulu iaitu model CSR yang dibangunkan oleh Nur Ilyani Ahmad et al. (2019) setiap domain pada model CSR perlu digabungkan dengan eleman privasi untuk membentuk cadangan model awal Model Kesediaan Penyedia Perkhidmatan Awan Terhadap Privasi Awan (Mather et al. 2009). Dengan memetakan 39 kawalan dalam ISO/IEC 27018:2019 dengan tujuh (7) domain ini, ia berupaya membantu CSP bagi memahami kawalan privasi dengan cara yang lebih tersusun mengikut domain-domain tersebut seperti di Jadual 2.

Jadual 2 Perincian domain kesediaan dari kajian lepas

Domain	Perincian dari Kajian Lepas
Teknologi	Teknologi ditakrif sebagai industri berasaskan perkhidmatan, atau teknologi. Penggunaan perisian adalah berfokuskan reka bentuk, pengeluaran, penggunaan barangan dan perkhidmatan. Ia dibahagikan kepada dua(2) dalam pengurusan aktiviti manusia, iaitu: Penjelasan: rancangan pembangunan, model, manual operasi dan prototaip Tidak ketara: nasihat, penyelesaian masalah dan latihan (Susanto & Al Munawar, 2018; Nur Ilyani Ahmad, 2019).
Organisasi	Organisasi ditakrif sebagaii Unit sosial manusia yang teratur dan dinamik yang berjaya memenuhi objektif atau keperluan berkaitan industri atau perkhidmatan (Susanto & Al Munawar, 2018; Nur Ilyani Ahmad, 2019).
Dasar	Dasar ditakrif sebagai prinsip atau peraturan untuk membuat keputusan untuk mendapatkan dasar nasional yang rasional mengenai pertumbuhan perindustrian atau perkhidmatan masa depan (Susanto & Al Munawar, 2018; Nur Ilyani Ahmad, 2019).
Pemegang Taruh	Pemegang Taruh ditakrif sebagai Individu, Kumpulan atau Persatuan yang mempunyai kepentingan langsung atau tidak langsung dalam organisasi kerana ia boleh mempengaruhi atau mempengaruhi tindakan, matlamat dan dasar organisasi (Susanto & Al Munawar, 2018; NurIlyani Ahmad, 2019) Menurut NIST, pemegang taruh itu terdiri daripada penyedia awan, pemilik awan, broker awan, audit awan dan pelanggan awan (Liu et al. 2012; Nur Ilyani Ahmad, 2019).
Budaya	Budaya adalah ditakrifkan menentukan apa yang boleh diterima atau tidak boleh diterima, sama ada perlu atau tidak, sama ada betul atau salah, sama ada layak atau tidak praktikal. Budaya organisasi: kepercayaan dan sikap yang membawa kepada

Domain	Perincian dari Kajian Lepas
	iklim sosial dan psikologi tertentu dalam organisasi, budaya juga merupakan jumlah keseluruhan sejarah dan jangkaan organisasi (Susanto & Al Munawar, 2018; Nur Ilyani Ahmad, 2019).
Pengetahuan	Pengetahuan ditakrif dalam pengertian organisasi adalah tahap kecekapan dan kecerdasan dan jumlah pengetahuan yang ada pada manusia.Pengetahuan baru-baru ini telah diiktiraf sebagai faktor dalam pembangunan (Susanto & Al Munawar, 2018; NurIlyani Ahmad, 2019).
Persekitaran	Persekitaran adalah ditakrifkan merangkumi segala-galanya di sekeliling syarikat, dari struktur ekonomi dan daya saing kepada persekitaran kawal selia. Rangka ini melibatkan pengawalan persekitaran fizikal dan logik, berdasarkan pandangan sistem keselamatan maklumat (Susanto & Al Munawar, 2018; NurIlyani Ahmad, 2019).
Privasi	Privasi adalah ditakrifkan hak atau kewajiban privasi berkaitan dengan pengumpulan, penggunaan, pengungkapan, penyimpanan, dan pemusnahan data peribadi (atau maklumat yang dapat dikenal pasti secara peribadi — *Personally Identifiable Information* (PII)). Atau dalam kata lain privasi adalah mengenai kebertanggungjawaban organisasi kepada subjek data, dan juga ketelusan terhadap amalan organisasi mengenai maklumat peribadi (Mather et al. 2009; Yee, 2017) Definisi yang diterima pakai oleh *Organization for Economic Cooperation* and Development (OECD): : sebarang maklumat yang berkaitan dengan individu yang dikenali atau dikenali (subjek data). Definisi lain yang diterima secara umum oleh Canadian Institute of Chartered Accountants (CICA) : "Hak dan tanggungjawab individu dan organisasi dengan berkenaan dengan pengumpulan, penggunaan, penyimpanan, dan pendedahan maklumat peribadi. "

A. Pemetaan Domain terhadap Kawalan Standard Privasi Awan

Domain yang telah dikenal pasti, dipetakan ke atas kawalan dalam standard ISO/IEC 27018:2019. Ini kerana kawalan ini merupakan panduan perlindungan maklumat pengenalan peribadi (PII) pada pengkomputeran awan dan digunakan sebagai instrumen kajian. Sebanyak 39 kawalan yang akan dipetakan ke atas tujuh (7) domain dalam cadangan model awal kajian ini.

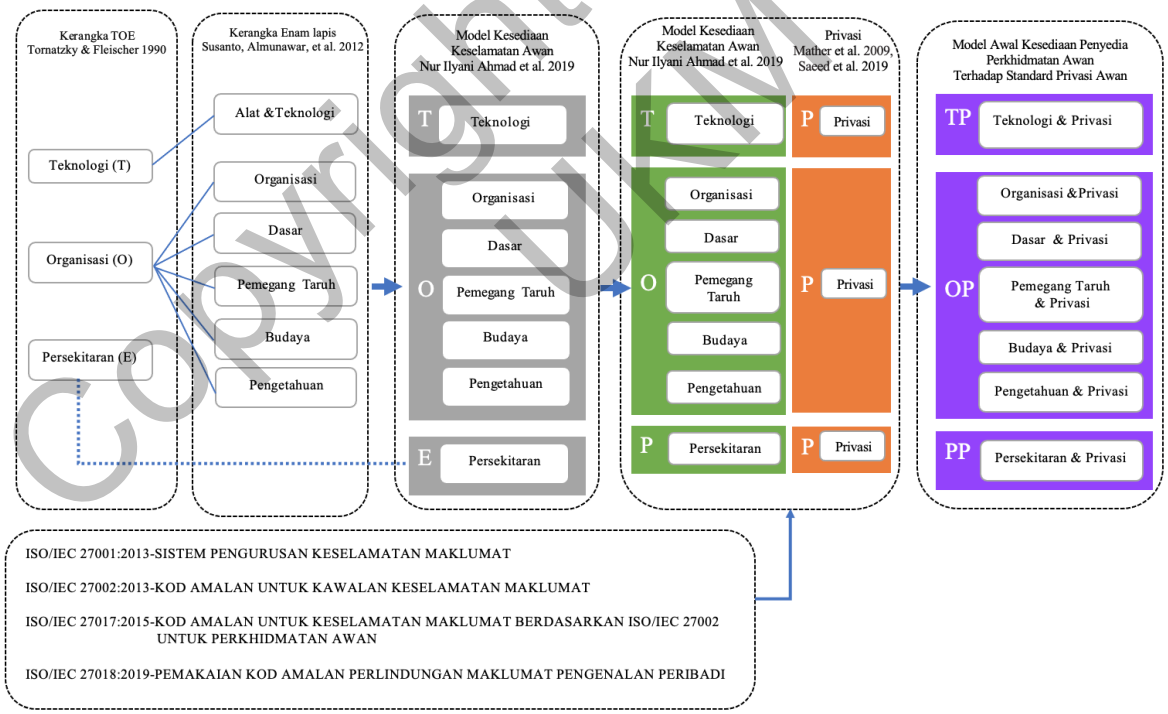
B. Cadangan Model Awal

Pembangunan cadangan model awal dalam kajian ini diadaptasikan daripada Model Kesediaan Keselamatan Awan (CSR) yang dibangunkan oleh Nur Ilyani Ahmad et al. (2019) berdasarkan gabungan Kerangka Teknologi Organisasi Persekitaran (TOE) (Tornatzky & Fleischer 1990) dan model sedia ada Kerangka Enam Lapis (Six Layer Framework) (Susanto et al. 2012). Untuk mengisi jurang Kerangka enam Lapis ini, elemen persekitaran telah ditambahbaik oleh Nur Ilyani Ahmad (2019) dengan menghasilkan model CSR. Model ini terdiri daripada tujuh (7) domain dengan menambahbaik Kerangka Enam Lapis dan menambah domain persekitaran (P) dari kerangka TOE.

Menurut Tariq & Santarcangelo (2016), standard ISO 27001 yang digunakan oleh rangka kerja ini hanyalah standard generik yang merangkumi semua aspek pengurusan, operasi, teknikal untuk menangani ancaman dan kelemahan. Oleh kerana sifat generiknya, ia tidak meliputi semua cabaran sistem keselamatan dan privasi maklumat awan. Untuk mengisi jurang kajian ini, setiap

domain pada Model Kesediaan Keselamatan Awan perlu digabungkan dengan eleman privasi untuk membentuk cadangan model awal Model Kesediaan Penyedia Perkhidmatan Awan Terhadap Privasi Awan. Mather et al. (2009) menyatakan bahawa "Anda dapat memiliki keselamatan dan tidak memiliki privasi, tetapi Anda tidak dapat privasi tanpa keselamatan".

Ini turut di sokong oleh Saeed et al. (2019) bahawa CSP perlu berusaha untuk memperkuat kepercayaan pengguna mereka dengan menawarkan perkhidmatan dengan keselamatan dan privasi terjamin dalam untuk menjaga integriti, kerahsiaan dan ketersediaan data. Integriti bermaksud pengguna ingin memastikan bahawa data tidak akan diubah semasa transit atau penyimpanan. Kerahsiaan bermaksud pengguna ingin memastikan bahawa data tidak dapat diakses oleh orang yang tidak dibenarkan. Ketersediaan bermaksud pengguna ingin mengakses data dan aplikasi di pengkomputeran awan dengan cara yang dapat diramalkan dan tanpa berhenti atau kehilangan data. Kerahsiaan, integriti dan ketersediaan adalah kebimbangan keselamatan terbesar yang dihadapi oleh pengguna di pengkomputeran awan awam (Harauz et al. 2009; Hirlei A. De Chaves et al. 2011; Jensen et al. 2009). Rajah 2 merupakan cadangan model awal Model Kesediaan Penyediaan Perhidmatan Awan Terhadap Standard Privasi Awan.



Rajah 2 Pembangunan cadangan model awal

PENDEKATAN KAJIAN

Kajian ini dilaksanakan secara kaedah pensampelan dengan melibatkan responden yang terdiri daripada pengamal pengkomputeran awan dan juruaudit. Pendekatan kajian dilaksanakan merupakan gabungan kaedah kualitatif dan kuantitatif. Pendekatan kajian terbahagi kepada tiga (3) fasa iaitu pembangunan model awal, penentusahan model awal dan pengesahan model akhir.

A. Pembangunan Model Awal

Model awal dihasilkan adalah melalui kajian kesusasteraan ke atas bagi jurnal, artikel dan buku berkenaan dengan pengkomputeran awan yang terdiri daripada standard berkaitan sistem keselamatan maklumat, privasi dan keselamatan awan serta model kesediaan keselamatan awan. Model awal dihasilkan dari adaptasi Model Kesediaan Keselamatan Awan (CSR).

Model awal ini telah dibangunkan selaras dengan standard ISO/IEC 27018:2019 serta merujuk standard ISO/IEC 27017:2015, ISO/IEC 27002:2013 dan ISO/IEC 27001:2013 yang mengkhusus kepada 39 kawalan pemakaian kod amalan perlindungan maklumat pengenalan peribadi (PII). Pembangunan model awal dalam bentuk instrumen ini adalah berdasarkan 39 kawalan yang dinyatakan di dalam standard ISO/IEC 27018 dan dipetakan ke atas tujuh (7) domain Model Kesediaan Keselamatan Awan (CSR). Gambaran model awal kajian adalah seperti di Rajah 2.

B. Penentusahkan Model Awal

Penentusahan model awal melibatkan dua (2) proses iaitu pengumpulan dan penentusahan maklumat serta penganalisaan. Kaedah kajian adalah secara kualitatif melalui temubual untuk mendapatkan penentusahan terhadap model awal yang dibina. Dalam ini, penentusahan model awal dilaksanakan oleh tiga (3) pakar dalam bidang pengurusan keselamatan maklumat (ISMS), pengkomputeran awan dan privasi awam. Model awal tersebut akan diperbaiki mengikut cadangan penambahbaikan pakar dan seterusnya terhasil model yang telah ditambah baik.

C. Pengesahan Model Akhir

Proses pengesahan model akhir dibuat melalui pengesahan menggunakan prototaip model dan soal selidik borang penilaian. Prototaip kajian ini dibina menggunakan Microsoft Excel 365 manakala borang soal selidik dibangunkan menggunakan aplikasi atas talian, Google Form. Pengesahan akan dilaksanakan oleh responden yang terdiri daripada pengamal yang berpengalaman luas dalam bidang pengurusan keselamatan maklumat (ISMS), pengkomputeran awan dan privasi awam. Seramai lapan (8) orang responden yang mewakili syarikat CSP terlibat dalam kajian ini, responden ini terdiri daripada enam (6) orang CSP dan dua (2) orang Juruaudit (JA) yang mewakili syarikat CSP yang

berbeza.Pengamal-pengamal ini dipilih berdasarkan agensi yang telah mendapatkan pensijilan ISMS dan dalam proses mendapatkan pensijilan ISMS khusus bagi perkhidmatan awan.

Prototaip kajian yang dibina dengan instrumen kajian terdiri daripada 39 kawalan pemakaian kod amalan perlindungan maklumat pengenalan peribadi (PII) dan 206 senarai semak yang dipetakan kepada tujuh (7) domain kajian. Tahap kesediaan diukur dengan skala Yes dengan nilai 1 atau No dengan nilai 0. Jumlah markah yang diperolehi bagi ketujuh-tujuh domain dikira dengan menggunakan formula adalah seperti berikut:

$$\boldsymbol{m = \frac{y}{v} \times 5} \quad \textbf{(1)}$$

Di mana,

$\boldsymbol{m}$ = Jumlah markah

$\boldsymbol{y}$ = Jumlah jawapan "Yes"

$\boldsymbol{v}$ = Jumlah soalan di dalam domain

$\boldsymbol{5}$ = Lima (5) tahap kesediaan ((*Not ready/ Vigilant/ Partial Readiness/Primary Readines/ Complete Readines*)

Purata keseluruhan bagi ketujuh-tujuh domain akan dikira dengan menggunakan formula seperti berikut:

$$\boldsymbol{a = \sum_{i=1}^{7} \frac{s}{7}} \quad \textbf{(2)}$$

Di mana,

$\boldsymbol{a}$ = Jumlah markah keseluruhan

$\boldsymbol{s}$ = Jumlah markah setiap domain

$\boldsymbol{7}$ = Jumlah domain

Markah keseluruhan yang telah diperolehi iaitu, $\boldsymbol{a}$, akan menunjukkan tahap kesediaan sesebuah agensi dengan skala penilaian tahap kesediaan seperti di Jadual 3. Skala ini telah di adaptasi dari jadual tahap pengukuran untuk keselamatan, privasi, kesediaan pematuhan pengkomputeran awan oleh Bhatia & Malhotra (2018).

Jadual 3 Skala penilaian tahap kesediaan

Markah keseluruhan, *p*	**Tahap Kesediaan**
0 ≤ a ≤ 1	Tidak bersedia
1 < a ≤ 2	Kesediaan berjaga-jaga
2 < a ≤ 3	Kesediaan separa

3 < a ≤ 4	Kesediaan utama
4 < a ≤ 5	Kesediaan lengkap

Sumber : Bhatia & Malhotra (2018)

PENDEKATAN KAJIAN

A. Analisis Penentusahan Pakar

Penentusahan oleh pakar melibatkan proses mendapatkan penentusahan model awal yang dibangunkan. Hasil penentusahan ini mendapati bahawa pakar bersetuju dengan tujuh (7) domain yang dicadangkan beserta 39 kawalan privasi awan. Walau bagaimanapun, pakar mencadangkan penambahbaikan dibuat ke atas cadangan pemetaan domain dan senarai semak berdasarkan kawalan standard ISO/IEC 27018:2019 boleh dirujuk di Jadual 4.

Jadual 4 Rumusan penentusahan pakar

Bahagian	**Pekara**	**Cadangan Pakar**	**Penilaian Pakar**
Cadangan Pemetaan Domain dan Senarai Semak	Semua Kawalan	Dicadangankan kawalan ISO/IEC 27018:2014 dikemaskini kepada versi standard terkini iaitu ISO/IEC 27018:2019	Pakar 1
	Semua Kawalan Pemetaan	Dicadangkan semua kawalan pemetaan ISO/IEC 27001:2013 dipetakan berdasarkan standard ISO/IEC 27017:2015 *Implementation Guidance*	Pakar 2, 3
	Subseksyen Kawalan A.10.2	Dicadang senarai semak sub kawalan A.10.2 dari Domain Organisasi & Privasi di letakan dibawah Domain Dasar & Privasi	Pakar 1
	Subseksyen Kawalan A.10.2	Dicadang senarai semak sub kawalan A.10.2 di petakan kepada sub kawalan 5.1.2 *Review of the policies for information security*	Pakar 1
	Subseksyen Kawalan A.3.1	Dicadang senarai semak sub kawalan A.3.1 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1
	Subseksyen Kawalan A.3.2	Dicadang senarai semak sub kawalan A.3.2 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1
	Subseksyen Kawalan A.6.1	Dicadang senarai semak sub kawalan A.6.1 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1
	Subseksyen Kawalan A.11.11	Dicadang senarai semak sub kawalan A.11.11 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1
	Subseksyen Kawalan A.11.12	Dicadang senarai semak sub kawalan A.11.12 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1
	Subseksyen Kawalan A.8.1	Dicadang senarai semak sub kawalan A.8.1 Domain Dasar & Privasi di letakan dibawah Domain Organisasi & Privasi	Pakar 1

A. Analisa Pengesahan Model Akhir

Pengesahan model akhir menggunakan prototaip model dan soal selidik oleh responden yang terdiri daripada pengamal-pengamal berpengalaman luas dalam bidang pengurusan keselamatan maklumat pengkomputeran awan dan privasi awan. Proses pengesahan dilaksanakan dengan menguji keberkesanan dan kecekapan penggunaan prototaip oleh agensi terhadap kesemua tujuh (7) domain terdiri daripada Teknologi & Privasi, Organisasi & Privasi, Dasar & Privasi, Pemegang Taruh & Privasi, Budaya & Privasi, Pengetahuan & Privasi Dan Persekitaran & Privasi. Skor keseluruhan mengikut domain-domain yang diperolehi adalah seperti di Jadual 5.

Jadual 5 Skor Keseluruhan Mengikut Responden

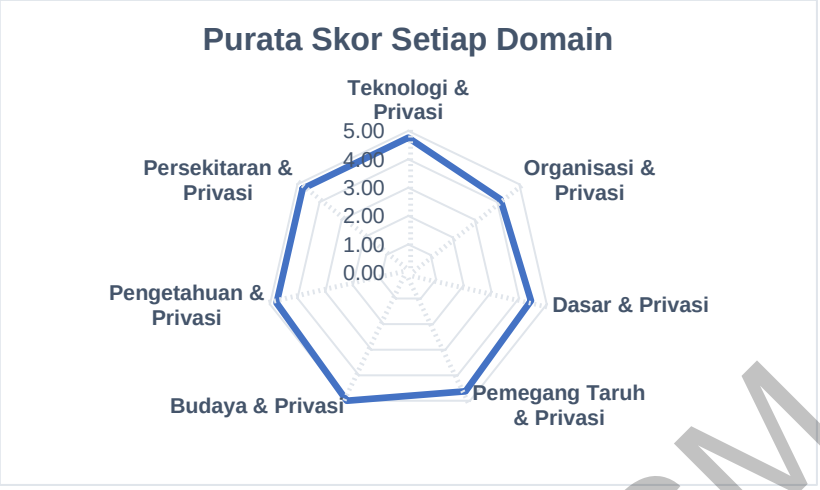
Kod Responden	Skor Keseluruhan	Tahap Kesediaan
CSP1	4.89	Kesediaan Lengkap
CSP2	4.57	Kesediaan Lengkap
CSP3	4.56	Kesediaan Lengkap
CSP4	4.63	Kesediaan Lengkap
CSP5	4.88	Kesediaan Lengkap
CSP6	4.95	Kesediaan Lengkap
JA1	3.66	Kesediaan Utama
JA2	4.96	Kesediaan Lengkap

Berdasarkan analisa keputusan ini, pada peringkat pra penilaian sebanyak tujuh (7) pengamal iaitu CSP 1, CSP 2, CSP 3, CSP 4, CSP 5, CSP6 dan CSP 8 (JA 2) telah mencapai tahap kesediaan lengkap manakala satu (1) lagi pengamal iaitu JA1 menunjukkan tahap kesediaan utama yang mempunyai skor tahap kesediaan adalah 3.66.

Jadual 6 Purata Skor Mengikut Domain

Domain	Purata Skor	Tahap Kesediaan
Teknologi	**4.64**	Kesediaan Lengkap
Organisasi	**4.15**	Kesediaan Lengkap
Dasar	**4.43**	Kesediaan Lengkap
Pemegang Taruh	**4.63**	Kesediaan Lengkap
Budaya	**5.00**	Kesediaan Lengkap
Pengetahuan	**4.79**	Kesediaan Lengkap
Persekitaran	**4.72**	Kesediaan Lengkap

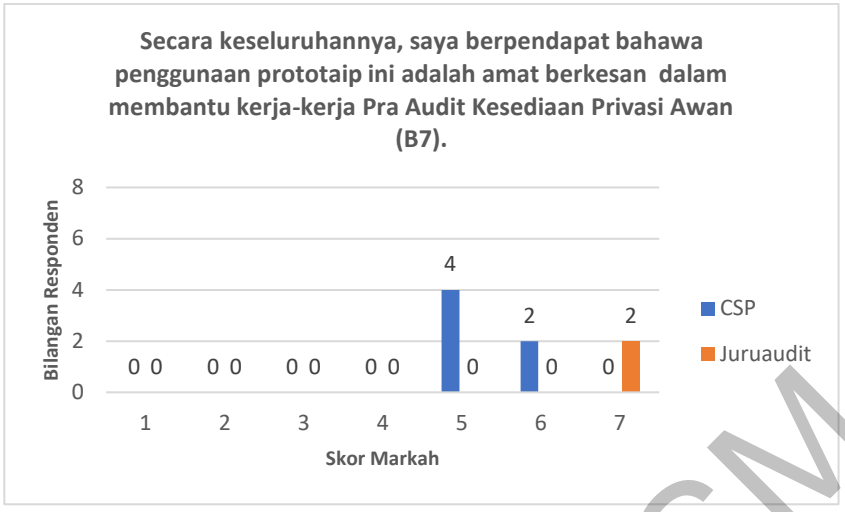
Melalui graf radar Rajah 3 dan Jadual 6 mendapati domain Organisasi & Privasi berada di kedudukan radar yang paling minimum di antara domain-domain tersebut. Domain Organisasi & Privasi berada pada tahap kesediaan yang lengkap tetapi mempunyai nilai markah tahap kesediaan adalah 4.15 dan terendah di antara domain-domain lain.



Rajah 3 Graf radar skor bagi setiap domain

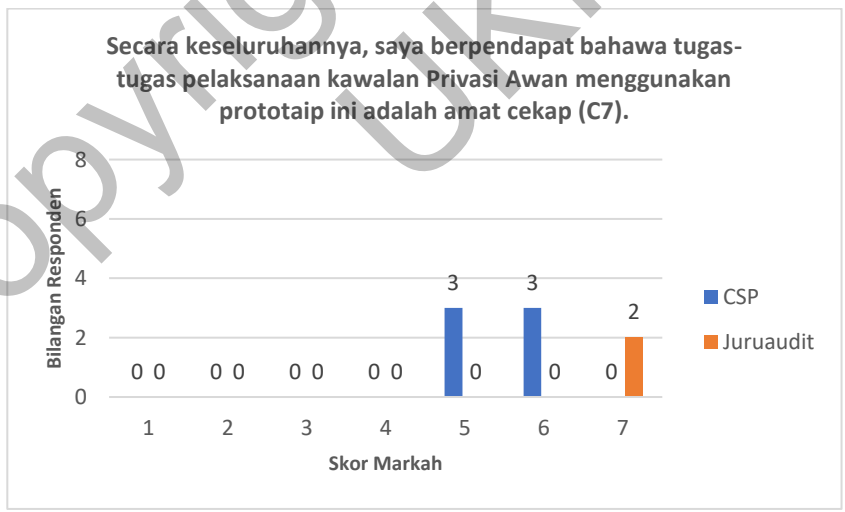
PENGESAHAN MODEL MELALUI PROTOTAIP

Sesi pengesahan yang dilaksanakan bertujuan untuk menilai tahap keberkesanan dan kecekapan prototaip model yang telah dibangunkan. Sejurus sesi pengesahan melalui prototaip selesai, responden mengesahkan tahap keberkesanan dan kecekapan prototaip model dan model akhir kajian dengan menjawab Borang Penilaian Prototaip Model Kesediaan Penyedia Perkhidmatan Awan Terhadap Standard Privasi Awan. Hasil yang diperolehi melalui soalan-soalan pengesahan prototaip model, mendapati bahawa melalui prototaip yang dibangunkan telah berjaya menjawab persoalan kajian. Sebanyak 25 % (2 orang) pengamal Juruaudit Amat Setuju dengan tahap keberkesanannya prototaip model ini. Manakala 25 % (2 orang) pengamal CSP Bersetuju dan baki 50% (4 orang) pengamal CSP Agak Setuju dengan tahap keberkesanannya prototaip model ini.Pencapaian tahap keberkesanan boleh dirujuk di Rajah 3.



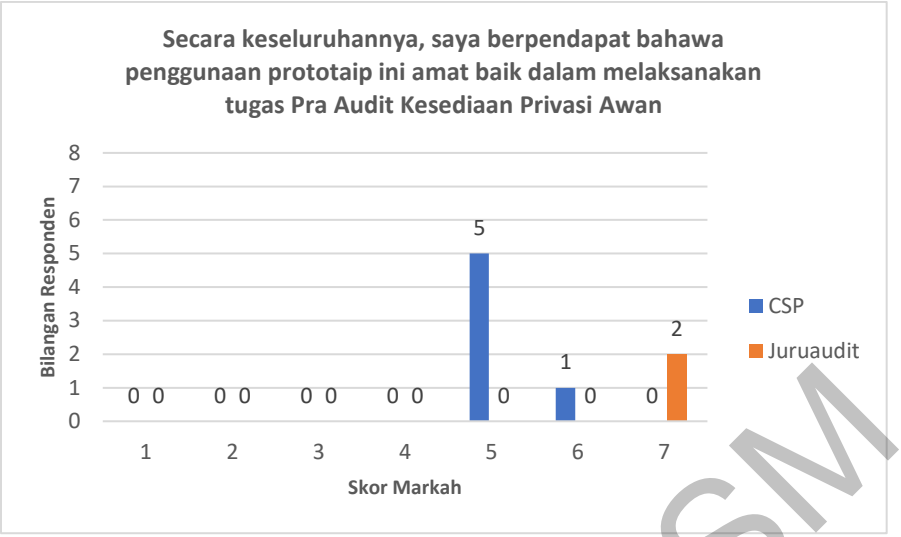
Rajah 4 Pencapaian tahap keberkesanan

Bagi tahap kecekapan prototaip model, terdapat 25 % (2 orang) pengamal Juruaudit amat setuju dengan tahap kecekapan model ini. Manakala 37.5 % (3 orang) pengamal CSP bersetuju dengan tahap kecekapan prototaip model dan baki 37.5 % (3 orang) pengamal CSP agak bersetuju dengan tahap kecekapan prototaip model yang dibangunkan. Pencapaian tahap kecekapan boleh dirujuk di Rajah 4.



Rajah 5 Pencapaian tahap kecekapan

Secara keseluruhan, melalui pembangunan prototaip model ini ia membantu agensi dalam menilai tahap kesediaan keselamatan perkhidmatan awan secara efektif dengan mudah tanpa sebarang pembaziran sumber. Pencapaian ini boleh di lihat di Rajah 6.



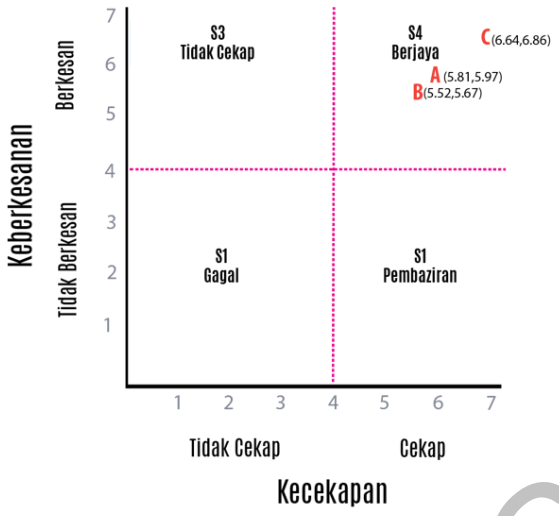
Rajah 6 Pencapaian secara keseluruhan prototaip model

Jadual 7 menunjuk nilai purata tahap Keberkesanan dan Kecekapan berdasarkan perbandingan Keseluruhan, Pengamal CSP dan Pengamal Juruaudit. Tahap Keberkesanan dan Kecekapan Model ini dibangunkan berdasarkan matrik pengukuran yang diadaptasikan dari matriks keberkesanan dan kecekapan oleh Ibrahim Mohamed (2013).

Jadual 7 Perbandingan nilai purata tahap kerberkesanan dan kecekapan keseluruhan, pengamal CSP dan pengamal Juruaudit

Kategori	Purata Keberkesanan	Purata Kecekapan
Keseluruhan (A)	5.81	5.97
Pengamal CSP (B)	5.52	5.67
Pengamal Juruaudit (C)	6.64	6.86

Rajah 7 menunjukkan dengan lebih jelas perbandingan tahap keberkesanan dan kecekapan berdasarkan perbandingan Keseluruhan (A), Pengamal CSP (B) dan Pengamal Juruaudit (C). Nilai plot A, B dan C berada di S4 yang membawa maksud tahap Keberkesanan dan Kecekapan adalah berjaya. Justeru itu model yang dibangunkan adalah berjaya sekaligus menjawab persoalan kajian



Rajah 7 Tahap keberkesanan dan kecekapan berdasarkan perbandingan Keseluruhan, pengamal CSP dan pengamal Juruaudit

RUMUSAN DAN PENEMUAN

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

A. **Objektif 1: Mengenal Pasti Faktor Domain Berdasarkan Kawalan Privasi Awan Dalam Menilai Tahap Kesediaan Penyedia Perkhidmatan Awan Terhadap Standard Privasi Awan**.

Model awal menghasilkan tujuh (7) domain iaitu teknologi & privasi, organisasi& privasi, dasar & privasi, pemegang taruh & privasi, budaya & privasi, pengetahuan & privasi dan persekitaran & privasi. Model awal ini seterusnya dipetakan ke atas kawalan standard ISO/IEC 27017:2015 dan kawalan standard ISO/IEC 27018:2019 yang membentuk instrumen kajian ini.

B. **Objektif 2: Membangunkan Model Kesediaan Penyedia Perkhidmatan Awan (CSP) Terhadap Privasi Awan Berdasarkan Pematuhan Terhadap Standard ISO/IEC 27018:2019-Pemakaian Kod Amalan Perlindungan Maklumat Pengenalan Peribadi (PII) Dengan Merujuk Standard ISO/IEC 27017, ISO/IEC 27001 dan ISO/IEC 27002**

Objektif kedua ini juga merupakan gabungan peringkat Fasa 1 dan peringkat Fasa 2. Pada peringkat Fasa 1, hasil kajian kesusasteraan akan menghasilkan cadangan model awal kajian. Manakala pada peringkat Fasa 2 cadangan model awal kajian akan di hantar kepada tiga (3) orang pakar yang berpengalaman dalam bidang pengurusan keselamatan maklumat (ISMS), pengkomputeran awan dan privasi awam untuk ditentusahkan. Hasil proses penentusahan ini berjaya membangunkan Model Kesediaan Penyedia Perkhidmatan Awan (CSP) Terhadap Standard Privasi Awan yang

memberi tumpuan berdasarkan kepada 39 kawalan pemakaian kod amalan perlindungan maklumat pengenalan peribadi (PII) yang terdapat di dalam standard ISO/IEC 27018:2019.

C. **Objektif 3: Mengesahkan Model Melalui Pengujian Kecekapan Dan Keberkesanan Prototaip.**

Objektif ketiga kajian ini adalah untuk mengesahkan model melalui pengujian kecekapan dan keberkesanan prototaip. Proses pengesahan model ini dilaksanakan melalui prototaip (*proof of concept*) dimana ianya berada di peringkat Fasa 3. Pada fasa ini, model awal yang telah ditentusah atas cadangan dan komen dari pakar telah menghasilkan kepada prototaip model. Prototaip model ini di uji oleh sekumpulan pengamal yang berpengalaman dalam bidang pengurusan keselamatan maklumat, privasi pengkomputeran awan dan pengkomputeran awan.

Pengamal yang telah selesai menggunakan prototaip ini, kemudiannya diminta untuk mengisi borang soal selidik bagi pengesahan model untuk mengkaji keberkesanan dan kecekapan prototaip secara atas talian dengan menggunakan *Google Form*. Hasil analisa terhadap proses pengesahan mendapati secara keseluruhan pengamal yang terdiri dari lapan (8) responden iaitu enam (6) orang CSP dan dua (2) orang Juruaudit bersetuju prototaip model kajian ini boleh digunakan oleh agensi sebagai panduan dalam menilai tahap kesediaan privasi perkhidmatan awan dan membantu agensi membuat pemantauan secara dalaman bagi memastikan privasi perkhidmatan awan terpelihara. Selain itu juga dapat membantu agensi dalam membuat pra-penilaian audit privasi pengkomputeran awan secara efektif dan produktif.

SUMBANGAN

Kajian ini telah berjaya menghasilkan dua (2) sumbangan utama iaitu model dan prototaip kesediaan yang telah dihasilkan. Melalui sumbangan ini, sesebuah agensi dapat menilai tahap kesediaan penyedia perkhimatan awan terhadap standard privasi awan dengan berkesan dan cekap. Model yang dihasilkan boleh menjadi garis panduan kepada agensi awam atau swasta dalam usaha menyediakan perkhidmatan pengkomputeran awan yang selamat dan terjamin serta dapat diakreditasi oleh badan pensijilan yang diiktiraf seluruh dunia. Prototaip yang dihasilkan membantu agensi dalam memahami senarai semak dari kawalan standard ISO/IEC 27018:2019 serta meningkatkan tahap kesedaran dan kesediaan sesebuah agensi terhadap privasi perkhidmatan pengkomputeran awan berdasarkan domain-domain yang telah dikenal pasti iaitu Teknologi & Privasi, Organisasi& Privasi, Dasar & Privasi, Pemegang Taruh & Privasi, Budaya & Privasi, Pengetahuan & Privasi Dan Persekitaran & Privasi

CADANGAN DAN KAJIAN MASA DEPAN

Kajian ini hanya memberi tumpuan berdasarkan kepada 39 kawalan pemakaian kod amalan perlindungan maklumat pengenalan peribadi (PII) yang terdapat di dalam standard ISO/IEC 27018:2019. Dicadangkan kajian masa depan dikembangkan kepada standard ISO/IEC 27701:2019 Security Technique-Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management-Requirement and guidelines. Selain itu, kajian ini juga mempunyai batasan kajian yang boleh dipertingkatkan melalui kajian susulan. Batasan yang terdapat dalam kajian ini ialah ia tertumpu kepada agensi yang telah diakreditasi dan mempraktikkan ISO/IEC 27001:2013. Lantaran dalam aspek keselamatan siber yang saban hari dihujani dengan pelbagai isu-isu keselamatan penting untuk dikaji tahap kesediaan terhadap agensi yang belum diakreditasi dan mempraktikkan ISO/IEC 27001:2013.

KESIMPULAN

Secara keseluruhannya kajian ini telah berjaya membangunkan Model Kesediaan Penyedia Perkhidmatan Awan (CSP) Terhadap Standard Privasi Awan yang dibangunkan berdasarkan kepada standard ISO/IEC 27018:2019 dengan merujuk standard ISO/IEC 27017:2015, ISO/IEC 27002:2013 dan ISO/IEC 27001:2013. Kajian ini juga telah berjaya mengenal pasti faktor domain yang mempengaruhi tahap penilaian kesediaan Penyedia Perkhidmatan Awan terhadap standard privasi awan. Model ini telah membuktikan keberkesanan dan kecekapan dalam menilai tahap kesediaan CSP dalam mematuhi kawalan privasi pengkomputeran awan melalui prototaip model yang dihasilkan dalam kajian ini. Hasil soal selidik pengesahan oleh pengamal yang terdiri daripada enam (6) orang CSP dan dua (2) orang Juruaudit menunjukkan model ini senang digunakan dan mempunyai keboleharapan dalam menilai tahap kesediaan sesebuah agensi khasnya CSP. Selain itu juga model ini menambahkan produktiviti pengamal dengan lebih cekap dan berkesan. Melalui prototaip model yang dihasilkan juga dapat membantu agensi membuat persediaan menghadapi proses audit ISMS mengkhusus pada kawalan privasi pengkomputeran awan.

RUJUKAN

Alemeye, F. & Taddesse, F. G. 2015. Cloud Readiness Assessment Framework and Recommendation System. 1-5.
Ali, M., Dhamotharan, R., Khan, E., Khan, S. U., V, A., Vasilakos, Li, K. & Zomaya, A. Y. 2017. Sedasc: Secure Data Sharing in Clouds. *IEEE SYSTEMS JOURNAL* 11(2):
Asma Zubaida M. Ibrahim, Jamaiah H Yahaya & Aziz Deraman. 2018. Model Kesediaan Pelaksanaan Sistem Kawalan Industri Di Persekitaran Awan Dari Perspektif Keselamatan Maklumat. *Jurnal Pengurusan UKM* 53(15): 169-180.
Bhatia, S. & Malhotra, J. 2018. Cspcr: Cloud Security, Privacy and Compliance Readiness - a Trustworthy Framework. *International Journal of Electrical and Computer Engineering (IJECE)* 8(3756-3766.

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). Anjuran

Hanifah Abdul Hamida & Mokhtar Mohd Yusofa. 2015. State-of-the-Art of Cloud Computing Adoption in Malaysia: A Review. *Jurnal Teknologi* 2015): 131-136.

Harauz, J., Kaufman, L. M. & Potter, B. 2009. "Data Security in the World of Cloud Computing," *Security Privacy, IEEE* 7(4):

Hasimi Sallehudin, Razli Che Razak, Mohammad Ismail, Ahmad Firdause Md Fadzil & Rogis Baker. 2018. Cloud Computing Implementation in the Public Sector: Factors and Impact. *Jurnal Teknologi Maklumat dan Multimedia Asia-Pasifik* 7(2-2): 27 - 42.

Hendre, A. & Joshi, K. P. 2015. A Semantic Approach to Cloud Security and Compliance. *2015 IEEE 8th International Conference on Cloud Computing*, hlm.

Hirlei A. De Chaves, Westphall, C. B., Westphall, C. M. & Gerônimo, G. A. 2011. "Customer Security Concerns in Cloud Computing,". *Proceedings of the 10-th Int. Conf. on Networks, ser. ICN 2011. IARIA, 2011*, hlm. 7-11.

I.S.O./I.E.C. 2013. Iso/Iec 27001:2013 Information Security Management Systems – Requirements.

I.S.O./I.E.C. 2019. The Iso Survey of Management System Standard Certifications 2019.

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.

Jensen, M., Schwenk, J., Gruschka, N. & Iacono, L. L. 2009. "On Technical Security Issues in Cloud Computing,". *Cloud Computing, 2009. CLOUD '09. IEEE International Conference* 109 –116.

Liu, F., Tong, J., Mao, J., Bohn, R. B., Messina, J. V., Badger, M. L. & Leaf, D. M. 2012. Nist Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). *NIST Special Publication 500-292 292* 1–28.

Mather, T., Kumaraswamy, S. & Latif, S. 2009. *Cloud Security and Privacy* O'Reilly Media, Inc.

Nur Ilyani Ahmad. 2019. Model Kesediaan Penyedia Perkhidmatan Awan Terhadap Keselamatan Awan Berdasarkan Standard Khusus Awan. Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia.

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.

Oliveira, T., Thomas, M. & Espadanal, M. 2014. Assessing the Determinants of Cloud Computing Adoption: An Analysis of the Manufacturing and Services Sectors. *Information & Management* 51(5):

Pandey, M. K. 2016. Standards in Cloud Computing-a Critical Review

Pauley, W. 2010. Cloud Provider Transparency: An Empirical Evaluation. *IEEE Security & Privacy* 8(6):

Ren, K., Wang, C. & Wang, Q. 2012. Security Challenges for the Public Cloud. *IEEE INTERNET COMPUTING*

Ristov, S. & Gusev, M. 2015. A Methodology to Evaluate the Trustworthiness of Cloud Service Providers' Availability. *IEEE EUROCON 2015 - International Conference on Computer as a Tool (EUROCON)*

Ryoo, J., Rizvi, S., Aiken, W. & Kissell, J. 2013. Cloud Security Auditing: Challenges and Emerging Approaches. *IEEE Security & Privacy* 12(6): 68 - 74.

Saeed, I., Baras, S. & Hajjdiab, H. 2019. Security and Privacy of Aws S3 and Azure Blob Storage Services. *2019 IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*, hlm.

Singh, N. & Singh, A. K. 2018. Data Privacy Protection Mechanisms in Cloud. *Data Sci. Eng.*

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):

Tariq, M. I. & Santarcangelo, V. 2016. Controls Effectiveness for Cloud Computing. *Proceedings of the 2nd International Conference on Information Systems Security and Privacy* hlm. 201-208.

Tornatzky, L. & Fleischer, M. 1990. *The Process of Technology Innovation.* Lexington, Ma: Lexington Books.

Tubaishat, A. 2019. Security in Cloud Computing: State-of-the-Art, Key Features, Challenges, and Opportunities. *IEEE 4th International Conference on Computer and Communication Systems (ICCCS)*

Upadhyay, V. & Jain, D. A. 2015. An Introduction of Cloud Computing Security and Privacy Issues in It Industries. *International Journal Of Engineering And Computer Science I* 4(6): 12728-12730.

Zaydi, M. & Nasserddine, B. 2016. Information System Security Governance: Technology Intelligence Perspective. *2016 International Conference on Advanced Communication Systems and Information Security (ACOSIS)*, hlm. 1-6.