*Jurnal Pengurusan 53(2018) 169 – 180*
*https://doi.org/10.17576/pengurusan-2018-53-15*

# Model Kesediaan Pelaksanaan Sistem Kawalan Industri di Persekitaran Awan dari Perspektif Keselamatan Maklumat

*(Readiness Model for the Implementation of Industrial Control System into Cloud Environment Based on Information Security Perspective)*

Asma Zubaida M. Ibrahim
Jamaiah H. Yahaya
(Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia)
Aziz Deraman
(Pusat Pengajian Informatik dan Matematik Gunaan, Universiti Malaysia Terengganu)

*ABSTRAK*

*Persekitaran awan adalah satu bidang yang pesat berkembang dengan keupayaan mengakses perkhidmatan dari mana sahaja dan pada bila-bila masa. Sistem Kawalan Industri atau ICS adalah istilah umum untuk sistem kawalan yang digunakan di dalam infrastruktur kritikal. Apabila ICS dilaksanakan di persekitaran awan, keselamatan maklumat menjadi satu kebimbangan utama bagi organisasi ICS. Sebelum melaksanakan ICS ke awan, penting bagi organisasi ICS untuk bersedia kerana kurang kesediaan boleh membawa kepada kegagalan dalam pelaksanaannya. Oleh itu objektif utama kajian ini adalah untuk mencadangkan Model Kesediaan Pelaksanaan ICS di persekitaran awan (RMfIC) dari perspektif keselamatan maklumat. RMfIC terdiri daripada tiga komponen utama iaitu komponen pertama ialah analisis kesesuaian, komponen kedua, mengukur kesediaan dari perspektif keselamatan maklumat, dan komponen ketiga ialah pengiraan kesediaan organisasi ICS yang juga akan mengenal pasti tahap kesediaan sesebuah organisasi. Sumbangan utama RMfIC adalah organisasi ICS boleh mengenal pasti tahap kesediaan dan menangani cabaran sebelum melaksanakan perkhidamatan ICS di persekitaran awan.*

*Kata kunci: Persekitaran awan; sistem kawalan industri; model kesediaan; analisis kesesuaian; keselamatan maklumat.*

*ABSTRACT*

*Cloud environment is one of the growing areas due to the ability to access "Cloud" anywhere and anytime. Industrial Control System (ICS) is a general term that includes the control systems used in the critical infrastructures. When ICS is implemented into the cloud environment, information security is one of the major concern for the organisation. ICS organisation must attain a high level of readiness because lack of readiness may lead to cloud implementation failure. Therefore, the main objective of this research is to propose a Readiness Model for ICS implementation into Cloud environment (RMfIC) from the information security perspective. RMfIC consists of three main components. The first component is the suitability analysis. Second component is the measurement of readiness for information security perspective. The third component is to identify the readiness level achieved based on the readiness measurements. The contribution of RMfIC is that ICS organisation may know their level of readiness and address the challenges before implementing to cloud environment.*

*Keywords: Cloud environment; industrial control system; readiness model; suitability analysis; information security.*

## PENGENALAN

Persekitaran Awan (PA) merupakan teknologi baharu yang mempunyai permintaan tinggi dalam industri teknologi dan komunikasi pada hari ini. PA menyediakan perkhidmatan dan perkongsian maklumat yang tepat dan fleksibel, kos yang rendah serta sumber PA boleh diakses di mana-mana dan pada bila-bila masa yang diinginkan oleh pengguna (Wang et al. 2010). Terdapat dua pengetahuan asas mengenai PA yang perlu diketahui iaitu perkhidmatan yang disediakan dan juga model yang terdapat dalam PA. Terdapat tiga perkhidmatan asas yang disediakan oleh PA iaitu platform sebagai perkhidmatan (PaaS), perisian sebagai perkhidmatan (SaaS) dan infrastruktur sebagai perkhidmatan (IaaS) (Calero et al. 2010). Di bawah setiap perkhidmatan dalam PA, terdapat beberapa jenis sub perkhidmatan yang ditawarkan. Sub perkhidmatan seperti yang dinyatakan oleh Mohamed (2012) di bawah IaaS adalah seperti pengiraan kapasiti sebagai perkhidmatan (CCaaS) dan pangkalan data sebagai perkhidmatan (DBaaS). Di bawah PaaS pula terdapat sub perkhidmatan seperti simpanan sebagai perkhidmatan (STaaS) dan muka-layar sebagai perkhidmatan (DTaaS). Bagi SaaS pula sub perkhidmatan seperti komunikasi sebagai perkhidmatan (CaaS), pemantauan sebagai perkhidmatan (MaaS) dan keselamatan sebagai perkhidmatan (SECaaS) (Mohamed 2012). Dengan perkhidmatan dan sub perkhidmatan

yang telah disediakan oleh PA, pengguna akan mendapat manfaat melalui teknologi yang terkini berdasarkan keperluan dan hanya membayar perkhidmatan yang digunakan sahaja kepada pihak pembekal PA (Gibson et al. 2012).

Model PA pula boleh dibahagikan kepada empat jenis iaitu model awam, model persendirian, model hibrid dan model komuniti. Dalam PA, model awam ialah model yang ditawarkan oleh pihak ketiga atau dikenali sebagai pembekal PA. Antara manfaat utama penggunaan model awam ialah ia memudahkan pengguna serta harganya yang murah kerana kos perkakasan, aplikasi dan jalur lebar ditanggung oleh pembekal PA. Kelemahan utama dalam model awam adalah akses keselamatannya yang lemah. Ini adalah kerana sumber awan dikongsi bersama beberapa pihak yang tidak dikenali seperti yang dinyatakan oleh Dillon, Wu dan Chang (2010). Model kedua PA adalah model persendirian atau juga dikenali sebagai model swasta, yang biasanya digunakan oleh organisasi yang tertentu sahaja. Pengguna bagi model ini memiliki kuasa sepenuhnya ke atas PA tanpa campur tangan pihak ketiga. Pengguna luar tidak dapat mencapai data dalam PA persendirian ini. Geberslassie & Bitzer (2010) membuktikan kelebihan utama dalam model ini ialah akses sumber dan penggunaan adalah lebih selamat dan dipercayai oleh pengguna. Bagi model hibrid pula, ia merupakan kombinasi antara model persendirian dan model awam yang membolehkan sesebuah organisasi menyimpan maklumat penting di dalam simpanan model persendirian sementara maklumat yang lainnya dikekalkan di dalam model awam. Model komuniti pula merupakan kombinasi antara model awam, model persendirian dan model hibrid.

Sistem Kawalan Industri atau *Industrial Control System* (ICS) merupakan istilah umum yang merangkumi beberapa jenis sistem kawalan yang digunakan dalam bidang pengeluaran bagi sektor perindustrian (McPhillips et al. 2015). Sistem-sistem kawalan yang sering digunakan dalam sektor perindustrian dan infrastruktur kritikal adalah termasuk *Supervisory Control And Data Acquisition* (SCADA), *Distributed Control System* (DCS) dan *Programmable Logic Controller* (PLC). ICS biasanya digunakan dalam industri seperti industri elektrikal, pemprosesan air, minyak, gas dan data. Secara umumnya, sistem kawalan industri terdiri daripada beberapa alatan elektronik, sistem penyimpanan pangkalan maklumat dan sebuah sistem utama yang dikenali sebagai sistem antara muka pengguna (Goldschmidt et al. 2015). Ia berfungsi untuk memastikan kawalan terhadap proses dalam bidang pengeluaran stabil, tepat dan berjalan lancar. Selain daripada mengawal sesebuah proses dalam bidang pengeluaran, ICS juga banyak digunakan untuk merekod dan menyimpan maklumat secara langsung (Shahzad et al. 2013). Fungsi ini menjadi langkah penting bagi memastikan proses tersebut dikawal selia dari semasa ke semasa. Dalam kertas kerja ini, infrastruktur kritikal seperti loji penjanaan elektrik, sistem pengangkutan, kilang penapisan minyak dan kilang-kilang yang menguna dan mengaplikasi sistem ICS akan dirujuk sebagai "Oraganisasi ICS." Operator di organisasi ICS terus memantau dan mengawal bahagian yang berbeza untuk memastikan operasi organisasi ICS berjalan dengan betul dan lancar.

Sejak ICS mula diperkenalkan pada tahun 2000, ia telah melalui transformasi yang ketara iaitu daripada sebuah sistem kawalan yang terpencil kepada sebuah sistem kawalan dengan seni bina dan teknologi piawaian yang besar dan berhubung rapat dengan rangkaian jalur lebar (Shahzad et al. 2013). Hari ini, produk ICS secara komersialnya dibekalkan secara berasingan daripada infrastruktur oleh pembekal ICS. Pembekal ICS merujuk kepada syarikat perisian yang mencipta dan menjual sistem ICS kepada organisasi ICS. Ia digunakan berdasarkan piawaian platform dengan pelbagai peranti seperti penghala, modem data dan sistem antara muka pengguna yang diperlukan oleh organisasi ICS. Dengan ini, organisasi ICS dapat mengurangkan kos serta penggunaan sistem ICS juga menjadi lebih mudah (Misra & Mondal 2011). Pengawalan sistem ICS secara jauh serta pemantauan dari pelbagai lokasi dan pada bila-bila masa boleh dilakukan dengan hanya melaksanakan sistem ICS ke PA. Walau bagaimanapun, dengan pelaksanaan sistem ICS di dalam PA, keselamatan maklumat menjadi satu kebimbangan dan cabaran. Ini adalah kerana melalui pendekatan ini, pengguna ICS berisiko untuk mendapat serangan keselamatan berasaskan rangkaian komputer.

## LATAR BELAKANG KAJIAN

ICS seperti sistem SCADA dan DCS mempunyai banyak komponen autonomi dan dikenali sebagai sistem yang menelan belanja yang tinggi untuk dilaksana (Urias, Van Leeuwen & Richardson 2012). Pelaksanaan ICS perlu menitik beratkan semua aspek seperti keselamatan dan juga penyelenggaraan (Dumont 2010). Terdapat juga sistem ICS yang dilaksanakan oleh organisasi kecil pada skala data yang kecil seperti kilang pengeluaran yang kecil.

PA telah menjadi salah satu model baharu dalam perkhidmatan teknologi maklumat (Rahimli 2013). PA mempunyai faedah yang besar dan menjadi pilihan kerana ianya sangat kos-efektif bagi sesebuah organisasi yang berkongsi maklumat dengan pengguna mereka. Sistem PA adalah kumpulan sistem pelayan jauh yang dikendalikan oleh rangkaian yang membolehkan penyimpanan maklumat berpusat, dan akses dalam talian untuk perkhidmatan atau sumber dari mana-mana lokasi.

Namun begitu PA adalah satu teknologi yang agak baharu dalam bidang ICS (Birman, Ganesh & Van Renesse 2011). PA menyediakan akses ke ICS dengan lebih mudah dan efisyen kepada pengguna ICS dengan berkongsi sumber pengkomputeran. Teknologi ini merangkumi rangkaian, pelayan, penyimpanan, aplikasi dan perkhidmatan. Sumber-sumber ini dengan pantas boleh dibekal dan diguna dengan usaha pengurusan yang

minimum serta interaksi antara pembekal PA dengan pengguna menjadi lebih mudah. Setelah beralih ke PA, pembekal dan pengguna ICS boleh mengurangkan kos, mencapai kebolehpercayaan yang lebih tinggi, seterusnya mampu meningkatkan fungsi kegunaan ICS seperti yang dinyatakan oleh Wilhoit (2013). Selain mengurangkan kos perbelanjaan dan memudahkan pengurusan sesebuah ICS, penggunaan PA membolehkan pengguna ICS untuk mencapai maklumat dari semasa ke semasa dengan hanya menggunakan peranti seperti telefon pintar, komputer, tablet juga melalui mesej teks SMS dan E-mel.

Sejak penggunaan PA diperluaskan dalam pelbagai bidang, pelaksanaan ICS di dalam PA telah dicadang dan diimplemen oleh beberapa organisasi. Pembekal ICS yang mempunyai sistem ICS juga telah menjual pakej ICS mereka bersama dengan perkhidmatan PA awam atau swasta (Consulting 2012).

Beberapa kajian terdahulu telah dilakukan terhadap manfaat dan faedah PA ke atas ICS dan telah dikenalpasti iaitu kebolehpercayaan, prestasi dan penggurangan kos (Akande & Van Belle 2014). Terdapat juga perbincangan mengenai beberapa risiko PA yang menjadi faktor yang perlu diambil kira seperti keselamatan maklumat, isu perundangan, privasi dan cabaran migrasi (Wilhoit 2013). Antara faktor risiko yang dibimbangi apabila mengaplikasi ICS di PA dan perlu diberi lebih perhatian adalah faktor keselamatan maklumat (Carroll, Kotze & Merwe 2012; Kayali et al. 2016; Meri et al. 2017). Merujuk kepada kajian oleh Rao dan Selvamani (2015), keselamatan maklumat mempunyai lebih tujuh puluh peratus (70%) tahap kritikal dalam melaksanakan PA berbanding faktor lain seperti cabaran migrasi dengan sebelas peratus (11%) tahap kritikal dan isu perundangan dengan tiga puluh sembilan peratus (39%). Keselamatan maklumat merangkumi pengawalan terhadap kebocoran maklumat yang boleh memberi implikasi yang besar terhadap organisasi dan kepercayaan organisasi ICS kepada PA (Rao & Selvamani 2015). Selain isu kebocoran maklumat, isu seperti kehilangan data, *phishing* dan *botnet* (Kuyoro 2011) juga dikenalpasti sebagai isu keselamatan maklumat yang kritikal (Raisian & Yahaya 2015)

Menurut Keegan (2001), pengurusan ialah satu proses sosial dibentuk untuk mendapatkan kerjasama, penyertaan dan penglibatan ahli-ahli dalam sesebuah organisasi bagi mencapai sesuatu maklumat atau objektif yang paling berkesan. Definisi pengurusan yang lain adalah proses merancang, mengorganisasi, memimpin dan mengawal daya usaha anggota organisasi dan menggunakan sumber-sumber lain dalam organisasi bagi mencapai matlamat organisasi yang ditetapkan (Stoner, James & Wankel 1986).

## METODOLOGI KAJIAN

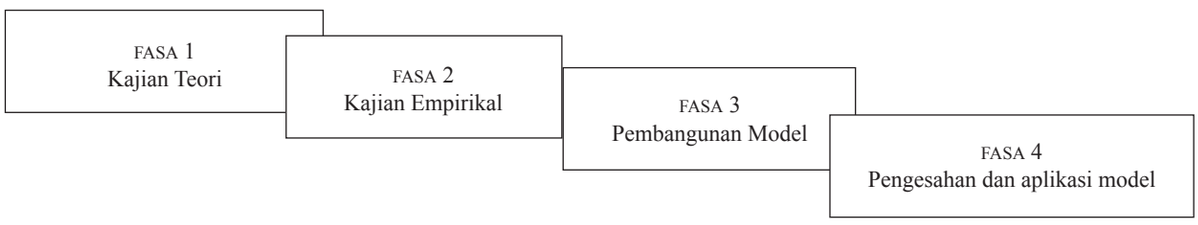
Metodologi yang digunakan dalam kajian ini dibahagikan kepada empat fasa utama seperti Rajah 1.

### FASA KAJIAN TEORI

Fasa pertama adalah fasa kajian teori. Fasa kajian teori dijalankan secara tiga peringkat. Peringkat pertama adalah untuk menetapkan fokus kajian ini dengan membentuk soalan mengenai keadaan atau masalah yang dikaji dan menentukan tujuan kajian. Peringkat pertama kajian teori merangkumi latar belakang kajian, objektif kajian, persoalan kajian, skop kajian dan kepentingan kajian. Peringkat kedua pula adalah kajian susastera yang dijalankan bagi mengenal pasti faktor-faktor keselamatan maklumat dalam ICS dan PA. Kajian terhadap model yang terdahulu bagi aspek kesediaan juga dikaji secara teori dan mendalami jurang yang wujud pada masa sekarang dan apa yang sepatutnya dicapai. Kajian susastera dibuat ke atas dokumen yang diterbitkan dan tidak diterbitkan. Dokumen yang diterbitkan adalah jurnal dan prosiding yang diperolehi berdasarkan carian pangkalan data seperti *IEEE, Elsevier, Springer* dan *Google Scholar*. Manakala dokumen yang tidak diterbitkan adalah merupakan kertas putih dari sesebuah organisasi, kertas pembentangan dan buku rujukan. Teknik bola salji (*snow ball*) digunakan iaitu membuat carian lanjut ke atas bahan penerbitan berdasarkan senarai rujukan jurnal atau prosiding yang dibaca (Sekaran & Roger 2010; Dragan & Isaic-Maniu 2013). Fasa ini dirumuskan dengan pembangunan sebuah model konsep berdasarkan hasil kajian susastera yg dijalankan. Model ini akan dikenali sebagai *Readiness Model for ICS and Cloud* (RMfIC).

### FASA KAJIAN EMPIRIKAL

Fasa kedua pula ialah fasa kajian empirikal. Fasa ini merupakan fasa pengesahan faktor-faktor keselamatan maklumat dan model konsep yang dibangunkan. Pensampelan adalah salah satu cara untuk mendapatkan maklumat daripada setiap individu dalam satu populasi yang dikaji. Pemilihan sampel dibuat secara berterusan sehingga tiada lagi maklumat baharu diperolehi. Peringkat




RAJAH 1. Metodologi kajian

ini dinamakan peringkat ketepuan, ia dicapai apabila tiada lagi maklumat baharu yang dapat diperhalusi daripada jawapan informan (Othman 2006). Peringkat ketepuan dapat dicapai berdasarkan jawapan berulang dan sama diberikan oleh informan dan tiada lagi data baharu ditemui. Oleh itu sampel kajian ini ditentukan dengan mengadaptasi kaedah persampelan bertujuan (*purposive sampling*) dan bilangan sampel adalah kecil. Kaedah pensampelan bertujuan ini membolehkan penyelidik menetapkan individu yang boleh membantu dan bersedia memberikan maklumat menurut pengetahuan dan pengalaman mereka (Tongco 2007). Teknik pensampelan ini dipilih kerana sasaran sampel memerlukan informan yang berhubung kait dengan kajian. Kaedah ini juga bersesuaian kerana kerjasama dan kesediaan informan yang dikenal pasti dapat membantu dalam melancarkan proses temu bual dan pengumpulan data. Kajian ini mencapai tahap ketepuan setelah melibatkan seramai tujuh orang informan.

Para informan terdiri daripada kakitangan atau staf dalam organisasi ICS iaitu seorang pengarah, seorang eksekutif IT, seorang pembantu teknikal, seorang pembangun perisian dan tiga orang eksekutif projek. Informan ini dipilih berdasarkan pengalaman mereka bekerja yang melibatkan ICS dan juga PA. Fasa ini dimulakan dengan menyediakan soalan temu bual, mengenal pasti informan, menjalankan sesi temu bual, dan merakam audio temu bual serta mentranskrip ke dalam bentuk teks. Kemudian, aktiviti menganalisis dan mengkod data hasil temu bual dijalankan. Langkah terakhir adalah dengan menjalankan pembaikan terhadap model konsep.

Dapatan daripada kajian empirikal ini adalah senarai faktor keselamatan yang telah disahkan dan model konsep yang telah ditambah baik berdasarkan pandangan pakar. Senarai faktor keselamatan maklumat ini boleh dirujuk pada bahagian Pembangunan Model RMfIC, komponen kedua pada Jadual 1. Faktor keselamatan maklumat yang telah disahkan pada fasa ini juga boleh dirujuk dalam Mohamad Ibrahim dan Yahaya (2018).

## FASA PEMBANGUNAN MODEL

Fasa ini bermula dengan membangunkan model sebenar berdasarkan model konsep yang telah dibangunkan dalam fasa 1. Model ini dikenali sebagai RMfIC sepanjang kajian ini. Model RMfIC ini terdiri daripada tiga komponen iaitu komponen-1 pra-implementasi, komponen-2 implementasi dan komponen-3 pasca-implementasi. Komponen-1 atau pra-implementasi dimulakan dengan menganalisis kesesuaian organisasi ICS sebelum melaksanakan PA. Jika sesebuah organisasi ICS memperolehi skor yang menunjukkan kesesuaian yang tinggi maka organisasi ICS boleh terus ke komponen-2 dalam model RMfIC. Komponen-2 atau dikenali sebagai implementasi merupakan komponen utama bagi model ini. Komponen-2 berfungsi menilai kesediaan faktor-faktor keselamatan maklumat yang telah dikenal pasti. Bagi menilai faktor-faktor ini, sebuah instrumen untuk menilai kesediaan organisasi ICS yang dikenali sebagai "Instrumen Nilai Kesediaan Organisasi" (INKO) dibangunkan. Kemudian kredit bagi setiap faktor dalam INKO ditentukan berdasarkan kredit bagi faktor yang hampir sama daripada kajian sebelum ini. Komponen-3 atau pasca-implementasi pula ialah komponen pengiraan dan penentuan kesediaan yang perlu dilakukan. Sebuah rumus bagi mengira skor yang diperolehi dalam INKO yang dikenali sebagai "Nilai Kesediaan Organisasi" (NKO) juga telah dibangunkan dalam fasa ini. Dalam komponen ini juga, sebuah skala dibina bagi menilai tahap kesediaan organisasi berdasarkan peratusan NKO yang diperoleh. Skala ini dikenali sebagai "Skala Penilaian Kesediaan Organisasi" (SKPO).

## FASA PENGESAHAN MODEL

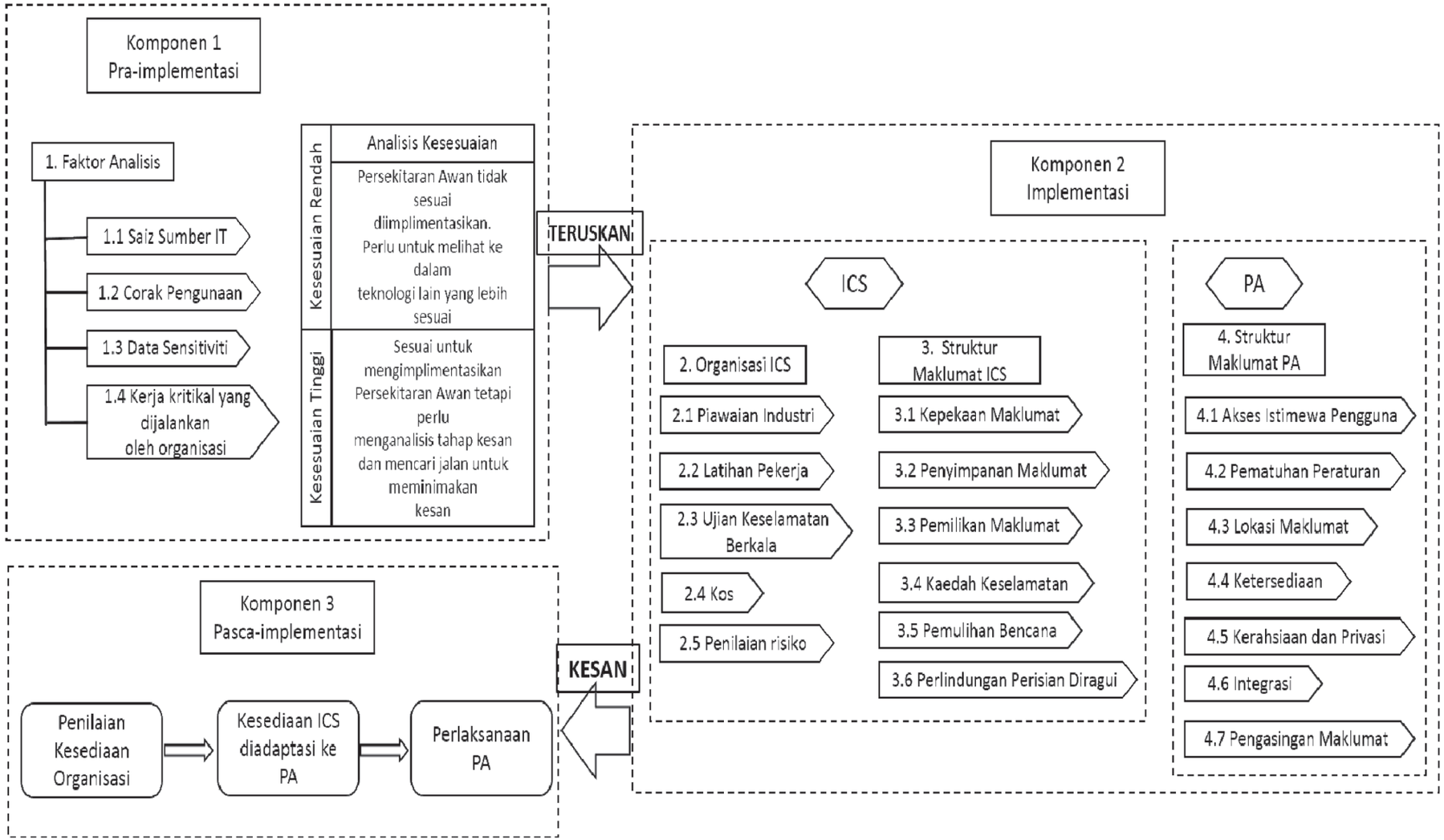
Fasa pengesahan melibatkan dua aktiviti utama iaitu mengaplikasi model dan mengesah model oleh pakar. Model disahkan terlebih dahulu dan dilaksanakan dalam kajian kes yang melibatkan kolaborasi bersama organisasi ICS. Dalam fasa ini instrumen penilaian diaplikasi dalam persekitaran sebenar yang melibatkan pakar ICS untuk menilai kesediaan organisasi mengikut model RMfIC. Langkah ini merupakan satu kaedah bagi menganalisis hasil kajian kes yang dijalankan dan menyediakan maklum balas bagi hasil kajian kes tersebut. Pada akhir kajian kes, pakar ICS dari organisasi dapat mengetahui status kesesuaian organisasi mereka dari perspektif keselamatan maklumat.

## PEMBANGUNAN MODEL RMFIC

Seperti yang telah dijelaskan sebelum ini, model RMfIC terdiri daripada tiga komponen utama iaitu komponen pra-implementasi, komponen implementasi dan komponen pasca-implementasi. Komponen pra-implementasi merupakan komponen yang berfungsi untuk menganalisis kesesuaian organisasi ICS sebelum melaksanakan di dalam persekitaran awan. Komponen kedua iaitu implementasi berfungsi untuk mengukur kesediaan untuk tiga kategori yang dikenal pasti dari perspektif keselamatan maklumat iaitu organisasi ICS, maklumat ICS dan maklumat PA. Komponen ini mengandungi faktor-faktor yang boleh mengukur kesediaan organisasi ICS dalam faktor keselamatan maklumat. Komponen ketiga iaitu pasca-implementasi adalah komponen pengiraan kesediaan yang mengenal pasti tahap kesediaan yang dicapai oleh sesebuah organisasi. Model lengkap RMfIC boleh dirujuk pada Rajah 2.

## KOMPONEN-1 PRA-IMPLEMENTASI

Komponen ini bertujuan membantu organisasi ICS bagi menentu dan menilai tahap kesesuaian sebelum melaksanakan ICS di persekitaran awan (PA). Berdasarkan peringkat pertama ini, sekiranya tahap kesesuaian adalah




RAJAH 2. Model RMfIC

rendah maka organisasi ICS harus mempertimbangkan kembali cadangan atau hasrat untuk meneruskan pelaksanaan ICS di persekitaran awan. Keadaan ini menimbulkan kerisauan dan cabaran bagi memastikan faedah utama perpindahan ke PA iaitu kos-efektif dapat dicapai.

Langkah pertama ke arah penilaian kesesuaian ialah sesebuah organisasi ICS perlu memahami sebab-sebab untuk melaksanakan ICS di PA. Organisasi ICS perlu menilai kehendak serta keperluan yang dikehendaki bermula dari faedah, risiko dan cabaran di dalam PA. Kemudian, organisasi ICS itu perlu mengambil kira kesan-kesan penggunaan PA dan membuat perbandingan antara kesesuaian dan impak. Sebagai contoh, jika sesebuah organisasi ICS mempunyai impak yang rendah dan kesesuaian yang tinggi maka PA adalah sesuai untuk digunakan oleh organisasi tersebut. Namun jika keputusan organisasi tersebut mempunyai impak yang tinggi dan kesesuaian yang rendah, maka organisasi ICS boleh meneruskan penilaian terhadap kesediaan PA seperti yang ditakrif dalam model ini. Analisis kesesuaian ini diadpatasi berdasarkan penyelidikan oleh Misra dan Mondal (2011) yang kemudiannya disokong oleh Saedi dan Iahad (2013), dan Sen, Chan dan Wenxue (2016).

Sebuah instrumen yang diberi nama Instrumen Penilaian Komponen-1 RMfIC diambil berdasarkan model *Return On Inverstement* (ROI). Instrumen ini digunakan sebagai langkah pertama pelaksanaan model RMfIC. Instrumen ini dijawab oleh pakar rujuk organisasi ICS yang terlibat untuk melaksanakan model RMfIC. Selepas organisasi ICS menanda jawapan yang sesuai bagi setiap soalan dalam instrumen, jawapan hendaklah dirujuk pada jadual kredit dan dirumuskan mengikut rumus pengiraan nilai kesediaan model ROI. Hasil pengiraan kredit ke dalam rumus pengiraan ROI dikenali sebagai skor kesesuaian. Skor kesesuaian ini digunakan dalam komponen-1 bagi memastikan terlebih dahulu bahawa organisasi ICS berkenaan melepasi tahap kesesuaian sebelum memasuki komponen-2.

Skor kesesuaian dinilai menggunakan skala penilaian kesesuaian model ROI. Dalam model RMfIC, jika organisasi memperolehi tahap 3 dari skala penilaian kesesuaian model ROI, adalah dicadangkan agar organisasi untuk tidak meneruskan pelaksanaan model RMfIC ke komponen-2. Ini adalah kerana organisasi dipercayai akan mengalami kerugian dan tidak mendapat faedah sepenuhnya jika pelaksanaan PA dijalankan. Jika organisasi ICS mendapat skor kesesuaian di antara 3760 dan 4600 atau tahap 2, organisasi ICS masih boleh meneruskan ke komponen-2 RMfIC kerana siasatan lanjutan diperlukan dari faktor-faktor lain seperti yang dicadangkan oleh model ROI. Justeru itu, dalam model ini siasatan lanjutan dijalankan adalah dari segi faktor keselamatan maklumat. Bagi organisasi ICS yang memperolehi skor lebih dari 4600 atau tahap 1 adalah sangat sesuai melaksanakan ICS di dalam PA dan boleh meneruskan komponen-2 model RMfIC untuk meneliti kesediaan dari perspektif keselamatan maklumat organisasi.

KOMPONEN-2 IMPLEMENTASI

Komponen kedua RMfIC ialah komponen implementasi atau pelaksanaan. Peringkat ini menilai kesediaan organisasi dalam melaksanakan ICS di PA dari perspektif dan faktor keselamatan maklumat. Faktor keselamatan maklumat ini boleh dirujuk dengan lebih terperinci dalam Mohamad Ibrahim dan Yahaya (2018). Dalam komponen-2 ini terdapat 3 kategori utama iaitu Organisasi ICS, Struktur Maklumat ICS dan Struktur Maklumat PA seperti dalam Rajah 1. Setiap kategori ini diikuti dengan faktor-faktor keselamatan maklumat yang diukur untuk mengetahui tahap kesediaan organisasi tersebut. Setiap faktor bagi kategori ini adalah seperti Jadual 1. Kategori dan faktor-faktor ini disahkan melalui kajian empirik yang dijalankan dalam fasa 1 kajian ini.

JADUAL 1. Faktor dan kategori Komponen 2 – Implementasi RMfIC

| Kategori | Faktor |
|---|---|
| Organisasi ICS | ■ Piawaian Industri<br>■ Latihan Pekerja<br>■ Ujian Keselamatan Berkala<br>■ Kos<br>■ Penilaian Risiko<br>■ Maklumat ICS<br>■ Sensitiviti Maklumat<br>■ Penyimpanan |
| Maklumat | ■ Pemilikan Maklumat<br>■ Kaedah Keselamatan<br>■ Pemulihan Bencana<br>■ Perlindungan Perisian Diragui |
| Maklumat PA | ■ Akses Istimewa Pengguna<br>■ Pematuhan Peraturan<br>■ Lokasi Data<br>■ Ketersediaan<br>■ Kerahsiaan dan Privasi<br>■ Integriti<br>■ Pengasingan Maklumat |

Setiap faktor yang dikenal pasti akan dinilai tahap kesediaannya ke atas sesebuah organisasi. Sebuah intrumen yang dikenali Intrumen Nilai Kesediaan Organisasi (INKO) dibangunkan dan menpunyai lapan belas (18) soalan berdasarkan lapan belas faktor tersebut. Nilai atau skor bagi INKO ini akan digunakan di komponen-3 RMfIC bagi mendapatkan tahap kesediaan organisasi ICS. Setiap soalan menyediakan empat kemungkinan jawapan yang merupakan tahap implemantasi organisasi tersebut. Semua jawapan kepada soalan dalam INKO ini diberikan kredit mengikut kepentingan relatif jawapan tersebut kepada faktor dalam model RMfIC. Kredit yang diberikan mengikut kepentingan relatif faktor bagi menilai kesediaan yang dirujuk kepada kajian yang dijalankan oleh Misra dan Mondal (2011).

KOMPONEN-3 PASCA-IMPLEMENTASI

Komponen ketiga dalam RMfIC merupakan komponen pasca implementasi yang mengira dan menentu kesediaan bagi sesebuah organisasi ICS. Komponen ini memerlukan instrumen yang telah diisi atau dijawab oleh organisasi ICS iaitu INKO seperti yang terdapat dalam komponen-2.

Berdasarkan empat jawapan yang disediakan dalam INKO, kredit yang diberikan adalah mengikut tahap pelaksanaan sesebuah organisasi ICS. Kredit pertama ialah tahap pelaksanaan pada aras permulaan dengan kredit 1. Kredit kedua pula ialah pelaksanaan yang masih dalam kemajuan dengan kredit 2. Kredit ketiga merujuk kepada pelaksanaan yang hampir mencapai matlamat dengan kredit 3. Akhir sekali ialah pelaksanaan yang telah mencapai matlamatnya dan usaha yang patut diteruskan dengan kredit 4. Pengiraan kredit yang diperolehi oleh organisasi bagi mendapatkan peratusan kesediaan pelaksanaan organisasi di dalam persekitaran awan ini dikenali sebagai Skor NKO (rujuk Rajah 3). Keterangan rumus ini adalah seperti berikut:-

- "NKO" mewakili Nilai Kesediaan Organisasi iaitu peratusan tahap kesediaan organisasi.
- "a" mewakili kredit jawapan yang telah dipilih oleh organisasi di dalam instrumen.
- "a1" bagi soalan pertama, "a2" bagi soalan kedua dan seterusnya.

$$\text{NKO} = \left(\sum \frac{(a1 + a2 + a3 + \cdots \ldots \ldots + a18)}{(18 \, x \, 4)}\right) \text{x } 100$$

RAJAH 3. Rumus pengiraan nilai NKO

Berdasarkan skor NKO yang diperolehi oleh organisasi, Jadual 2 menunjukkan Skala Penilaian Nilai Kesediaan (SPKO) yang bertindak sebagai panduan dalam membuat keputusan sama ada ICS akan dilaksanakan atau tidak di dalam PA. SPKO ini dibina merujuk kepada skala kesediaan yang ditakrif dalam model kesediaan oleh Aydin dan Tasci (2005). Dalam skala penilaian oleh Aydin dan Tasci (2005), jawapan bagi soalan penilaian dikodkan sebagai 1, 2, 3, 4, dan 5, seperti dalam *Likert scale* iaitu jenis skala lima-titik. Kemudian 4 selang kesediaan / 5 kategori kod = 0.8. Yakni skor dalam kesediaan bermula dari 1, 1.8, 2.6, 3.4, 4.2 dan 5.0. Oleh itu, skor min 3.4 dikenalpasti sebagai tahap kesediaan yang berada di tengah-tengah skala.

Dalam model RMfIC, jawapan bagi soalan INKO dikodkan kepada empat pilihan jawapan iaitu 1, 2, 3 dan 4 yang setara dengan status permulaan, kemajuan, mencapai matlamat dan usaha dikekalkan. Nilai peratusan digunakan dalam pengiraan NKO bagi memudahkan pengiraan dan bacaan hasil. Oleh itu, skor min 50 boleh dikenalpasti sebagai tahap jangkaan sedia selepas mengenal pasti tahap kritikal: 4 selang kesediaan / 4 kategori kod = 1.0, nilai 1.0 dari 5.0 digandakan kepada 20 bagi mendapatkan skala per 100 seperti Rajah 4. Hasil analisis ini, skala kesediaan ditentukan seperti yang ditunjukkan dalam Rajah 4.

Selain daripada mendapat tahap jangkaan 'Sedia' pada skor 50, SPKO bagi model RMfIC juga telah dipersetujui dan disahkan oleh pakar yang juga telah mengesahkan INKO. Pakar berpendapat bahawa tahap 'Sangat Bersedia' perlulah berada pada skor NKO yang tinggi bagi mendapatkan keadaan organisasi yg benar-benar bersedia. Organisasi ICS dalam kajian kes bersetuju dengan tahap kesediaan yang mereka dapati hasil daripada pelaksanaan model RMfIC dan SPKO dengan keadaan sebenar dan semasa organisasi ICS berkenaan.

Dalam Jadual 2, SPKO menyediakan skor NKO bermula 0 hingga 24 peratus iaitu nilai terendah atau sangat tidak bersedia, 25 hingga 49 peratus adalah sebagai tidak sedia, 50 hingga 89 adalah sedia, dan 90 hingga 100 adalah nilai tertinggi atau sangat bersedia bagi sesebuah organisasi yang dinilai tahap kesediaan pelaksanaan awan mengikut perspektif keselamatan maklumat. SPKO ini juga menyediakan huraian bagi empat tahap kesediaan tersebut bagi membantu organisasi untuk memahami setiap tahap dengan lebih baik dan tindakan susulan yang boleh dilakukan untuk penambahbaikan (rujuk Jadual 2).

APLIKASI MODEL MELALUI KAJIAN KES

Model RMfIC diaplikasi dalam kajian kes ke atas sebuah organisasi yang menggunakan ICS. Kajian kes A adalah organisasi ICS yang beroperasi di Malaysia. Bagi memudahkan perlaksanaan kajian kes, sebuah rangka kerja pelaksanaan dan pengujian RMfIC dibina


RAJAH 4. Tahap jangkaan "Sedia" SPKO bagi Model RmfIC

JADUAL 2. Skala penilaian kesediaan organisasi (SPKO) bagi RMfIC

| Nilai NKO ($N_{nko}$) | Tahap/Status | Huraian |
|---|---|---|
| 90>=$N_{nko}$ <100 | 4/Sangat Bersedia | Organisasi sangat bersedia dengan memenuhi faktor-faktor keselamatan maklumat untuk melaksanakan ICS ke PA. Usaha berterusan boleh dilakukan untuk memastikan keselamatan maklumat ICS dilaksanakan dalam PA terus dipertingkatkan. |
| 50>=$N_{nko}$ <89 | 3/Sedia | Organisasi dalam keadaan bersedia untuk melaksanakan ICS ke PA dan terdapat kelemahan yang yang dikenal pasti. Keselamatan maklumat berada tahap yang tidak merbahayakan organisasi serta boleh dipertingkatkan dan diberi perhatian. |
| 24>=$N_{nko}$ <49 | 2/Tidak Sedia | Organisasi masih berada pada tahap tidak bersedia untuk melaksanakan ICS ke PA serta terdapat beberapa faktor keselama tan maklumat yang masih lemah. Ianya boleh dipertingkatkan supaya boleh memasuki skala 3. |
| 0>=$N_{nko}$ <24 | 1/Sangat Tidak Sedia | Organisasi berada dalam keadaan sangat tidak bersedia untuk melaksanakan ICS ke PA. Dibimbangi jika mengalikasi ICS ke PA dengan skala yang lemah ini keselamatan maklumat, dicerobohi dan implikasi lain yang merug ikan organisasi. |

seperti Rajah 5. Rangka kerja ini adalah berdasarkan 3 komponen RMfIC beserta langkah-langkah yang perlu dijalankan bagi setiap komponen.

KAJIAN KES A

Kajian kes A atau RSA adalah sebuah organisasi swasta yang telah ditubuhkan pada tahun 2002. Bidang perniagaan RSA adalah mengeluar dan menghasilkan mesin ujian yang digunakan untuk menguji bahan-bahan yang dihantar oleh pengguna atau menyediakan mesin ujian khas mengikut kehendak pengguna. Bagi mengawal mesin-mesin ujian ini, RSA menggunakan salah satu jenis ICS yang dikenali sebagai Supervisory Control and Data Acquisition (SCADA). RSA masih mempertimbangkan keputusan untuk melaksana sepenuhnya di dalam PA. Beberapa faktor masih dibincangkan dan dikaji oleh jurutera RSA sebelum keputusan tersebut dibuat. Antara faktor-faktor ini adalah pakej-pakej yang disediakan oleh pihak penyedia PA dan faktor keselamatan. Berdasarkan keadaan ini RSA dipilih untuk mengaplikasikan model RMfIC bagi membantu RSA untuk membuat keputusan pelaksanaan ICS di PA.

Berdasarkan rangka kerja pelaksanaan kajian kes bagi model RMfIC, langkah pertama adalah penerangan tujuan model RMfIC kepada RSA. Langkah kedua iaitu pelaksanaan komponen-1 dimulakan dengan penerangan mengenai tujuan komponen-1 dijalankan ke atas RSA, dan juga instrumen penilaian komponen-1 bagi model RMfIC. Seperti diterangkan dalam seksyen-seksyen sebelum ini, komponen-1 bertujuan untuk mengira kesesuaian RSA sebelum melangkah ke PA.

Jurutera RSA kemudiannya menjalankan pengujian analisis kesesuaian dengan menjawab instrumen penilaian komponen-1. Setelah selesai menjawab, jurutera RSA diterangkan mengenai kredit bagi setiap jawapan yang dipilih oleh jurutera RSA dan rumus pengiraan kesediaan juga diterangkan. Skala kesediaan juga ditunjukkan kepada jurutera RSA.

Langkah terakhir bagi komponen-1 adalah validasi skor dan penentuan skala penilaian bagi RSA adalah seperti Jadual 3.


RAJAH 5. Rangka kerja pelaksanaan RMfIC

JADUAL 3. Kredit kesesuaian yang diperoleh dalam kajian kes A

| Kategori (Kod) | Kredit |
|---|---|
| Saiz Sumber IT (L) | 7 |
| Kredit Bilangan Pelayan (CNoS) | 8 |
| Bilangan Pelayan (NoS) | 4 |
| Kredit Bilangan Negara IT Tersebar (CNoC) | 4 |
| Bilangan Negara IT Tersebar (NoC) | 4 |
| Kredit Pendapatan Tahunan (CAR) | 4 |
| Pendapatan Tahunan (AR) | 3 |
| Kredit Waktu Penggunaan Puncak (CDoP) | 6 |
| Waktu Penggunaan Puncak (DoP) | 3 |
| Kredit Purata Penggunaan Puncak (CPbA) | 9 |
| Purata Penggunaan Puncak (PbA) | 4 |
| Kredit Jenis Perkhidmatan (CToS) | 5 |
| Jenis Perkhidmatan (ToS) | 3 |
| Kredit Jenis Pojek Di (CToP) | 5 |
| Jenis Pojek Di (ToP) | 3 |
| Kredit Saiz Asas Pengguna (CSCB) | 7 |
| Saiz Asas Pengguna (SCB) | 3 |
| Kredit Jumlah Data yang Dikendalikan (CADH) | 5 |
| Jumlah Data yang Dikendalikan (ADH) | 4 |
| Data Sensitiviti (DS) | 3 |
| Kredit Kerja Kritikal yang Dijalankan (CC) | 4 |
| Kerja Kritikal yang Dijalankan (C) | 3 |

Berdasarkan kredit-kredit yang diperoleh dan yang dikumpulkan oleh RSA, contoh pengiraan skor kesesuaian bagi organisasi RSA adalah seperti Rajah 6.

Dalam kajian kes ini skor kesesuaian yang diperolehi oleh RSA adalah 4264. Berdasarkan skala penilaian kesesuaian model ROI, RSA berada di dalam tahap 2 dan siasatan lanjutan diperlukan untuk melaksana PA. Justeru itu, RSA masih boleh meneruskan ke komponen-2 bagi model RMfIC untuk menjalankan siasatan lanjutan dalam faktor keselamatan maklumat.

Langkah ketiga adalah pelaksanaan komponen-2 dalam model RMfIC iaitu peringkat di mana RSA menilai kesediaan di dalam melaksanakan ICS ke PA dari faktor keselamatan maklumat. Setiap daripada lapan belas faktor tersebut diperjelaskan kepada RSA. Langkah seterusnya adalah penerangan terhadap instrumen INKO yang digunakan oleh jurutera RSA bagi menilai tahap kesediaan bagi peringkat kedua di dalam Model RMfIC. Jurutera RSA kemudian diminta untuk menjawab instrumen bagi komponen-2 model RMfIC ini. Jurutera RSA mengambil kira-kira 20 minit untuk menjawab kesemua lapan belas soalan di dalam INKO.

Langkah terakhir adalah pelaksanaan komponen-3 bagi model RMfIC. Skor yang diperolehi oleh RSA adalah seperti Jadual 4. Seterusnya pengiraan Nilai Kesediaan Organisasi (NKO) bagi RSA adalah seperti Rajah 7.

Dalam kajian kes ini seterusnya, jurutera RSA telah mengira NKO dan memperolehi nilai NKO sebanyak 63.9%. Nilai NKO ini dipetakan kepada skala penilaian kesediaan organisasi atau SPKO seperti ditunjuk dalam Jadual 2. Hasil pemetaan ini mendapati skala SPKO bagi RSA adalah di skala 3 iaitu dengan status "Sedia."

## RUMUSAN KAJIAN KES

Kajian kes yang dilaksanakan ini dapat meyimpulkan bahawa model RMfIC adalah suatu model yang praktikal dan sesuai digunakan dalam organisasi untuk menilai kesesuaian pelaksanaan ICS organisasi atau syarikat di PA. Memandangkan isu keselamatan maklumat adalah isu yang penting dan perlu dipertimbangkan sebelum melaksanakan PA, model RMfIC dapat membantu organisasi menilai tahap keselamatan maklumat di

Nilai (L) = NoS × CNoS + NoC × CNoC + AR × CAR
= (4 x 8) + (4 x 4) + (4 x 3)
= 60
Nilai (AU) = ToS × CToS (or) ToP × CToP + (4 − SCB) × CSCB.
= ( 15 x 3 )
= 15
Nilai (PU) = DoP × CDoP + PbA × CPbA
= ( 6 x 3 ) + ( 4 x 9 )
= 54
Nilai (WV) = PU × CPU + AU × CAU + ADH × CADH.
= (54 x 6 ) + ( 15 x 8 ) + ( 4 x 5 )
= 464
Nilai (DS) = SoD.
= 3
Nilai (C) = CWD.
= 3
Skor Kesesuaian = L × CL + WV × CWV + DS × CDS × ADH + C × CC × (65 − L).
= ( 60 x 7 ) + (464 x 8 ) + (3 x 6 x 4 ) + ( 3 x 4 x ( 65-60))
= 420 + 3712 + 72 + 60
= 4264 #

RAJAH 6. Rumus pengiraan nilai kesesuaiaan kajian kes A

JADUAL 4. Kredit faktor keselamatan maklumat bagi kajian kes A

| Kategori | Faktor | Kredit |
|---|---|---|
| Organisasi ICS | Pawaian Industri | 3 |
| | Latihan Pekerja | 3 |
| | Ujian Keselamatan Berkala | 3 |
| | Kos | 4 |
| | Penilaian Risiko | 2 |
| Maklumat ICS | Sensitiviti Maklumat | 3 |
| | Penyimpanan Maklumat | 3 |
| | Pemilikan Maklumat | 2 |
| | Kaedah Keselamatan | 3 |
| | Pemulihan Bencana | 2 |
| | Perlindungan Perisian Diragui | 2 |
| Maklumat PA | Akses Istimewa Pengguna | 2 |
| | Pematuhan Peraturan | 1 |
| | Lokasi Data | 3 |
| | Ketersediaan | 2 |
| | Kerahsiaan dan Privasi | 3 |
| | Integriti | 3 |
| | Pengasingan Maklumat | 2 |

organisasi mereka dengan menilai komponen-komponen dari aspek ICS dan PA. Syarikat RSA yang merupakan kajian kes dalam penyelidikan ini telah melaksana komponen-1, komponen-2 dan komponen-3 dalam model RMfIC dengan mudah dan mereka memahami tujuan kajian ini dijalankan. Seperti dijelaskan dalam seksyen sebelum ini, syarikat RSA telah memperoleh skala kesediaan tahap 3 iaitu "Sedia". Setelah melaksana proses penilaian ini, RSA mengetahui kelemahan mengenai sistem keselamatan maklumat organisasi mereka dan perkara yang harus organisasi mereka pertimbangkan dan perbaiki sebelum ICS berpindah ke PA. Ini berdasarkan instrumen yang telah dijawab oleh jurutera syarikat berdasarkan faktor-faktor yang terdapat di komponen-2 dalam model RMfIC.

Model RMfIC boleh digunakan untuk menguji semua tahap kesediaan keselamatan organisasi selepas pembaikan terhadap penilaian pertama dilakukan. Organisasi lebih bersedia jika mendapat nilai NKO yang lebih tinggi berbanding penilaian pertama. Penambahbaikan seterusnya boleh dibuat berulang kali berdasarkan kelemahan yang dikenalpasti dalam penilaian kedua dan seterusnya.

Berdasarkan kelancaran semasa mengaplikasi model RMfIC ke dalam kajian kes sebenar, model RMfIC ini boleh dibuktikan sebagai sebuah model yang telah berjaya diaplikasi dan hasilnya difahami dan berguna kepada pengguna. Maklum balas daripada syarikat RSA juga mengatakan bahawa model RMfIC mudah difahami dan praktikal untuk digunakan dalam mana-mana syarikat atau organisasi. Syarikat RSA memberikan pengesahan bersetuju dengan keputusan dan pelaksanaan model RMfIC ini ke atas skor kesesuaian dan skor kesediaan yang telah mereka peroleh. Tujuan pelaksanaan model RMfIC juga berjaya dicapai iaitu untuk mengenal pasti tahap kesediaan sesebuah organisasi ICS di samping mengenal pasti faktor-faktor keselamatan yang perlu diperbaiki sekiranya organisasi ingin memindah pengoperasian ICS ke PA.

## IMPLIKASI PENGURUSAN

Bagi kajian ini, implikasi pengurusan yang diterokai adalah pengurusan maklumat dalam sesebuah organisasi dari aspek keselamatan. Pengurusan keselamatan maklumat adalah penting dan masih perlu diterokai dengan lebih terperinci kerana masih terdapat masalah-masalah dan isu-isu keselamatan yang timbul dalam organisasi sehingga hari ini seperti ancaman, kelemahan dan risiko keselamatan (Zammani & Razali 2016). Model RMfIC digunakan bagi mengukur dan menilai tahap kesediaan sesebuah organisasi ICS dari segi keselamatan maklumat sebelum melaksanakan perpindahan perkhidmatan ICS ke persekitaran awan. Organisasi ICS dapat mengenal pasti kekuatan dan kelemahan syarikat mereka berdasarkan penilaian yang dijalankan mengunakan model RMfIC. Langkah seterusnya pula di mana organisasi ICS boleh memperbaiki atau mengawal kelemahan pengurusan keselamatan maklumat mereka selepas penilaian menggunakan model ini dilakukan.

Oleh itu, pengurusan keselamatan maklumat digunakan untuk melindungi semua harta maklumat yang bernilai dan risiko perpindahan dalam pelbagai aspek persekitaran organisasi dengan menggunakan teknologi keselamatan dan proses pengurusan yang baik (Chang & Lin 2007; Zammani & Razali 2016). Dalam kajian ini, organisasi ICS yang mengaplikasi model RMfIC berupaya merancang dan mengawal pengurusan maklumat dari aspek keselamatan maklumat bagi mencapai matlamat dan objektif yang ditetapkan oleh organisasi.

$$NKO = \left(\frac{3+3+3+4+2+3+3+2+3+2+2+2+1+3+2+3+3+2}{18x4}\right) X\ 100$$

$$= \frac{46}{72} X\ 100$$

$$= 63.9\ \%$$

RAJAH 7. Rumus pengiraan NKO bagi kajian kes A

## KESIMPULAN

Persekitaran awan atau PA merupakan bidang yang semakin berkembang pesat dengan penggunaanya dalam pelbagai sektor seperti dibincang dalam kertas kerja ini. Sistem Kawalan Industri atau ICS adalah istilah umum untuk sistem kawalan dalam infrastruktur kritikal dan merupakan antara bidang baharu yang mengamalkan PA bagi mendapatkan faedah PA yang nyata lebih mudah diurus dan mengurangkan kos. Di samping faedah yang diperolehi dalam pelaksanaan PA terdapat juga beberapa faktor yang dibimbangi atau cabaran membawa masalah kepada pengguna PA sekiranya tidak dibuat kajian persediaan yang lebih teliti. Sehubungan dengan itu, kajian ini menerokai salah satu faktor penting dalam pelaksanaan PA ini iaitu faktor keselamatan maklumat.

Kajian ini dijalankan bagi menjawab persoalan mengenai faktor-faktor keselamatan maklumat yang perlu diambilkira dalam pelaksanaan ICS dan PA, dan juga membentuk sebuah model kesediaan yang mengukur kesediaan sesebuah organisasi ICS sebelum melaksanakan ICS di dalam PA. Hasil daripada kajian emperik yang dijalankan ke atas tujuh informan, sebuah model kesediaan bagi pelaksanaan ICS di persekitaran awan dari perspektif keselamatan maklumat atau *Readiness Model for ICS and Cloud* (RMfIC) telah dibangunkan. Model ini bertindak sebagai mekanisma untuk mengukur tahap kesediaan sesebuah organisasi ICS sebelum melaksanakan PA dan menjurus kepada faktor keselamatan maklumat.

Kajian ini berjaya mengumpul dan memperolehi maklumat dan pengetahuan mengenai perkembangan terkini ICS dan PA melalui kajian emperik dan juga kajian kes yang dijalankan yang melibatkan penglibatan pakar dari industri. Hasil kajian ini juga mendapati majoriti organisasi ICS masih dalam proses melaksanakan PA. Kajian ini juga mengenal pasti faktor dan cabaran keselamatan maklumat yang wujud dan sekali gus membantu pengamal perisian dan pihak pengurusan dalam mengenal pasti tindakan yang perlu diambil sebelum melaksanakan ICS di PA dalam organisasi masing-masing.

## RUJUKAN


Akande, A.O. & Van Belle, J.P. 2014. A proposed framework to assess and increase the cloud computing readiness of financial institutions in South Africa. *2014 5th International Conference-Confluence The Next Generation Information Technology Summit (Confluence)*, 46-52.

Aydin, C.H., & Tasci, D. 2005. Measuring readiness for e-Learning: Reflections from an emerging country. *Educational Technology & Society* 8(4): 244-257.

Birman, K.P., Ganesh, L. & Van Renesse, R. 2011. *Computational needs for the Next Generation electric grid.* White paper running smart grid control software on cloud computing architectures.

Calero, J.M.A., Edwards, N., Kirschnick, J., Wilcock, L. & Wray, M. 2010. Towards a Multi-tenancy Authorization System for Cloud Services. *IEEE Security & Privacy* 8(6): 1-7.

Carroll, M., Kotzé, P. & Van Der Merwe, A. 2012. Securing virtual and cloud environments. *In Cloud Computing and Services Science*. New York: Springer.

Centre, C. 2010. *Cloud Computing for SCADA Moving all or part of SCADA applications to the cloud can cut costs significantly while dramatically increasing reliability and scalability*. A White Paper from InduSoft.

Chang, S.E. & Lin, C.S. 2007. Exploring organizational culture for information security management. *Industrial Management & Data Systems* 107(3):438-458.

Consulting, P. 2012. *SCADA: Risks and rewards of moving to a cloud environment rewards of such environments*. Report for Paladin Consulting.

Control, I. 2010. Distributed power system automation with IEC 61850, IEC 61499, and intelligent control. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)* 41(1): 81-92.

Controllers, P.L. 2013. *Cloud and ICS*. A White Paper from InduSoft.

Dillon, T., Wu, C. & Chang, E. 2010. Cloud computing: Issues and challenges. *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on IEEE*, 27-33.

Dragan, I.M. & Isaic-Maniu, A. 2013. Snowball sampling completion. *Journal of Studies in Social Sciences* 5(2):160-177.

Dumont, D. 2010. Cyber security concerns of supervisory control and data acquisition (SCADA) systems. *Technologies for Homeland Security (HST), 2010 IEEE International Conference*, 473-475.

Geberslassie, M. & Bitzer, B. 2010. Future SCADA systems for decentralized distribution systems. *Universities Power Engineering Conference (UPEC) 2010 45th International IEEE*, 1-4.

Gibson, J., Rondeau, R., Eveleigh, D. & Tan, Q. 2012. Benefits and challenges of three cloud computing service models. *Computational Aspects of Social Networks (CASoN), 2012 Fourth International Conference on IEEE*, 198-205.

Goldschmidt, T., Murugaiah, M.K., Sonntag, C., Schlich, B., Biallas, S. & Weber, P. 2015. Cloud-based control: A multi-tenant, horizontally scalable soft-PLC. *Cloud Computing (CLOUD), 2015 IEEE 8th International Conference on IEEE,* 909-916.

Jadeja, Y. & Modi, K. 2012. Cloud computing-concepts, architecture and challenges. Computing. *Electronics and Electrical Technologies (ICCEET), 2012 International Conference IEEE*, 877-880.

Kayali, M. H., Safie, N. & Mukhtar, M. 2016. Adoption of cloud based elearning: A systematic literature review of adoption factors and theories. *Journal of Engineering and Applied Sciences* 11(8): 1839-1845.

Kilman, D. & Stamp, J. 2005. *Framework for SCADA security policy*. Sandia National Laboratories report SAND2005-1002C.

Kuyoro, S. O. 2011. Cloud computing security issues and challenges. *International Journal of Computer Networks (IJCN)* 3(5): 247-255.

McPhillips, T.M., McPhillips, S.E., Chiu, H.J., Cohen, A.E., Deacon, A.M., Ellis, P.J., Garman, E., Gonzalez, A., Sauter, N.K., Phizackerley, R.P. & Soltis, S.M. 2002. Blu-Ice and the distributed control system: Software for data acquisition and instrument control at macromolecular crystallography beamlines. *Journal of Synchrotron Radiation* 9(6):401-406.

Meri, A., Hasan, M.K. & Mohd Satar, N.S. 2017. Success factors affecting the healthcare professionals to utilize cloud computing services. *Asia-Pasific Journal of Information Technology and Multimedia* 6(2): 31-42.

Misra, S.C. & Mondal, A. 2011. Identification of a company's suitability for the adoption of cloud computing and modelling its corresponding Return on Investment. *Mathematical and Computer Modelling* 53(3-4): 504-521.

Mohamed, E. 2012. Enhanced data security model for cloud computing. *Informatics and Systems (INFOS), 2012 8th International Conference*, 12-17.

Mohamad Ibrahim, A.Z. & Yahaya, J.H. 2018. Information security factors in the implementation of industrial control system into cloud environment. *Advanced Science Letters* 24(7): 5239-5242.

Othman, L. 2006. *Penyelidikan Kualitatif: Pengenalan Kepada Teori dan Method*. Tanjung Malim: UPSI.

Piggin, R.S.H. 2014. Securing SCADA in the cloud: managing the risks to avoid the perfect storm. *IET & ISA 60th International Instrumentation Symposium 2014* (10)1049:1.2-1.2.

Popovic, K. & Hocenski, Z. 2010. Cloud computing security issues and challenges. *MIPRO, Proceedings of the 33rd International Convention 2010*, 344-349.

Rahimli, A. 2013. Factors influencing organization adoption decision on cloud computing. *International Journal of Cloud Computing and Services Science* 2(2): 141.

Raisian, K. & Yahaya, J. 2015. Security issues model on cloud computing: A case of Malaysia. *International Journal of Advanced Computer Science and Applications* 6(8): 216-223.

Rao, R.V. & Selvamani, K. 2015. Data security challenges and its solutions in cloud computing. *Procedia Computer Science* 48(2015): 204-209.

Saedi, A. & Iahad, N.A. 2013. An integrated theoretical framework for cloud computing adoption by small and medium-sized enterprises. *PACIS 2013 Proceedings*, Paper 48. Available at http://aisel.aisnet.org/pacis2013/48.

Sekaran, U. & Roger, B. 2010. *Research Method For Business: A Skill Building Approach*. New York: John Wiley @ Sons.

Sen L., Chan, F.T.S. & Wenxue R. 2016. Decision making for the selection of cloud vendor: An improved approach under group decision-making with integrated weights and objective/subjective attributes. *Expert Systems with Applications* 55: 37-47.

Shahzad, A., Musa, S., Aborujilah, A. & Irfan, M. 2013. A performance approach: SCADA system implementation within cloud computing environment. *Advanced Computer Science Applications and Technologies (ACSAT), 2013 International Conference IEEE*, 274-277.

Stoner, F., James A. & Wankel, C. 1986. *Management*. 3rd ed. Englewood Cliffs, New Jersey: Prentice Hall Inc.

Tongco, M.D.C. 2007. Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications* 5: 147-158.

Turc, T. & Gligor, A. 2014. SCADA virtual instruments management. *Procedia Economics and Finance* 15: 1259-1264.

Urias, V., Van Leeuwen, B. & Richardson, B. 2012. Supervisory command and data acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed. *Proceedings - IEEE Military Communications Conference MILCOM*, (Lvc), 1-8.

Wang, L., Von Laszewski, G., Younge, A., He, X., Kunze, M., Tao, J. & Fu, C. 2010. Cloud computing: A perspective study. *New Generation Computing* 28(2): 137-146.

Wilhoit, K. 2013. *SCADA in the Cloud*. A report from Trend Micro.

Zammani, M. & Razali, R. 2016. An empirical study of information security management success factors. *International Journal on Advanced Science, Engineering and Information Technology* 6(6): 904-913.

Zammani, M. & Razali, R. 2016. Information security management success factors. *Advanced Science Letters* 22(8): 1924-1929.

Zissis, D. & Lekkas, D. 2012. Addressing cloud computing security issues. *Future Generation Computer Systems* 28(3): 583-592.

Asma Zubaida M. Ibrahim
Research Center for Software Technology and Management
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor, MALAYSIA.
E-Mel: asmaamri2012@gmail.com

Jamaiah H. Yahaya (penulis koresponden)
Research Center for Software Technology and Management
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM Bangi, Selangor, MALAYSIA.
E-Mel: jhy@ukm.edu.my

Aziz Deraman
Pusat Pengajian Informatik dan Matematik Gunaan
Universiti Malaysia Terengganu
21030 Kuala Nerus, Terengganu, MALAYSIA.
E-Mel: a.d@umt.edu.my