International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

INTERNATIONAL JOURNAL OF INNOVATION AND INDUSTRIAL REVOLUTION (IJIREV)
www.ijirev.com

CLOUD SECURITY PRE-ASSESSMENT MODEL FOR CLOUD SERVICE PROVIDER BASED ON ISO/IEC 27017:2015 ADDITIONAL CONTROL

Nur Ahada Kamaruddin[1*], Ibrahim Mohamed[2], Ahmad Dahari Jarno[3], Maslina Daud[4]

[1] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Malaysia
Email: ahadakamaruddin@gmail.com
[2] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Malaysia
Email: ibrahim@ukm.edu.my
[3] Malaysian Security Evaluation Facility (MySEF) Department, CyberSecurity (CSM), Malaysia
Email: dahari@cybersecurity.my
[4] CyberSecurity Proactive Services (CSPS), CyberSecurity (CSM), Malaysia
Email: maslina@cybersecurity.my
[*] Corresponding Author

Article Info:

Article History:
Received date: 11.10.2020
Revised date: 20.10.2020
Accepted date: 22.11.2020
Published date: 01.12.2020

To cite this document:

Kamaruddin, N. A., Mohamed, I., Jarno, A. D., & Daud, M. (2020). Cloud Security Pre-Assessment Model For Cloud Service Provider Based On ISO/IEC 27017:2015 Additional Control. International Journal of Innovation and Industrial Revolution, 2 (5), 01-17.

DOI: 10.35631/ IJIREV.25001

Abstract:

Cloud computing technology has succeeded in attracting the interest of both academics and industries because of its ability to provide flexible, cost-effective, and adaptable services in IT solution deployment. The services offered to Cloud Service Subscriber (CSS) are based on the concept of on-demand self-service, scalability, and rapid elasticity, which allows fast deployment of IT solutions, whilst leads to possible misconfiguration, un-patched system, etc. which, allows security threats to compromise the cloud services operations. From the viewpoint of Cloud Service Provider (CSP), incidents such as data loss and information breach, will tarnish their reputations, whilst allow them to conserve the issues internally, in which there is no transparency between CSP and CSS. In the aspects of information security, CSP is encouraged to practice cybersecurity in their cloud services by adopting ISO/IEC27017:2015 inclusive of all additional security controls as mandatory requirements. This study was conducted to identify factors that are influencing the CSP readiness level in the cybersecurity implementation of their cloud services by leveraging the developed pre-assessment model to determine the level of cloud security readiness. Approached the study is based on the combination of qualitative and quantitative assessment method in validating the proposed model through interview and prototype testing. The findings of this study had shown that factors that influence the CSP level of cloud security readiness are based on these domains; technology, organisation, policy, stakeholders, culture, knowledge, and environment. The contribution of the study as a Pre-Assessment Model for CSP which is suitable to be used as a guideline to provide a safer cloud computing environment.

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Keywords:

Cloud Computing, Cloud Security, Pre-Assessment and ISO/IEC 27017:2015

Introduction

Cloud computing is a rapid evolving technology and emerged as one of the technologies paradigm that attracts academics and industry players, in which offers great potential to innovate the IT operations of various organisations that fulfil common IT infrastructure deployment requirements such as scalability, broad network access, resources pooling and cost effectiveness (Abbas & Khan, 2014). However, there are concerns regarding the loss of control over data, managing the cybersecurity aspects of the IT infrastructures, data security implementation and continuous enabling governance compliance, that causes the lack of transparency between Cloud Service Subscriber (CSS) and Cloud Service Provider (CSP). This leads to mistrust of technological growth in cloud computing between these two parties in the cloud computing adoption (Ali et al., 2017; Nur Ilyani, Ibrahim, Maslina, Ahmad Dahari, & Norlaili, 2019).

Information security is one of the crucial elements in organisational operations as part of mandatory requirements by the CSS and the CSP in various aspects of cloud computing adoption. Therefore, issues such as data security, information leakage, access privilege, privacy, governance and other related matters that highlights as the information security concerns by the Cloud Service Subscriber (CSS) (Pauley, 2010). Indulge on the trust of the CSS can only be realised by CSP through the compliance by upholding the information security standards such as ISO/IEC 27001: 2013 (Giulio et al., 2017). To ensure all the security controls defined by ISO/IEC 27001:2013 are comply by the CSP, guidance is been elaborated in the ISO/IEC 27002:2013 in which, equipped with suggestion, general expectation and guideline in implementing the security controls of Information Security Management System (ISMS). Whereas ISO/IEC 27017:2015 is the additional reference added to the ISO/IEC27001:2013, that provides additional explanation and guidance of relevant security controls elaborated in the same format of ISO/IEC 27002:2013, whilst provides the explanations on the additional security controls in the cloud services that requires by the organization that adopts ISMS and cloud computing technology in their organization operations.

In all the existing research and studies were focusing on the development of maturity or readiness models based on ISO/IEC 27001:2013 (also known as ISMS) by defining the generic compliance in the model and did not consider the cloud security requirements through the cloud-specific controls as part of the requirements in ISMS implementation (Susanto & Almunawar, 2012). A study conducted by Nur Ilyani et al. (2019) on security readiness model for cloud computing had covered the 37 cloud-specific security controls stated in ISO/IEC 27017: 2015. However, additional controls defined in the Annex A of ISO/IEC 27017:2015 were not discussed, which are; (i) shared roles and responsibilities within a cloud computing environment; (ii) removal of CSS assets; (iii) segregation in virtual computing environments; (iv) virtual machine hardening; (v) administrator's operational security; (vi) monitoring of cloud services; and (vii) alignment of security management for virtual and physical networks.

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Therefore, the objective of this study is to enhance the existing models of cloud readiness assessment and cloud maturity model based on ISMS and cloud security by incorporating the seven (7) additional controls defined in the ISO/IEC 27017:2015 through the development of pre-assessment model of cloud security readiness assessment for CSP in providing CSP with a method to evaluate their level of readiness on cloud security controls implemented in their cloud services operations that shall conformance to the standards. Additionally, this study shall be able to guide the CSP in identifying any gap in the cloud security implementation of their cloud services operations that will be overcome before facing the actual audit process by the relevant certification body.

Literature Review

As one of the greatest technology innovations, cloud computing has become a part of technology that put evolution on the traditional IT infrastructure and its ecosystem. This innovation came through as an emerging phenomenon and has been a major agenda in the field of computing for the past decade. In Malaysia, the cloud computing initiative began in 2010 through an implementation of Government Cloud (G-Cloud) by the Government sector led by the Malaysian Administrative Modernisation and Management Planning Unit (MAMPU). The intention of Malaysia Government is to enable the adoption of cloud computing technology, with the objective of reducing the capital expenditure (CapEx) on the IT infrastructure by moving the budget allocation to operation expenditure (OpEx). Additionally, the adoption was being boost by Malaysia Prime Minister in 2017 through the Cloud First Strategy, that has given a great insight of the cloud computing acceptance in Malaysia IT industry and government sector by allowing flexibility in managing IT infrastructure by putting focus on investment on innovation and encouragement of new technology adoptions.

Through the use of cloud computing technology, resources were used comprehensively and in return, government sector were able to increase productivity and achieved better cost savings in IT operations (Jasmin & Hasan, 2018). There are many benefits that can be gain by using cloud computing services apart from cost savings and increased productivity. Among those benefits are self-service; supported varieties of IT equipment; fast elasticity; extensive network access as well as the ability to adjust resources as needed (Shahzad, 2014; Tweneboah-Koduah, Endicott-Popovsky, & Tsetse, 2014). Through these benefits, organizations inclusive of government entities able to utilize the cloud computing technology in many forms as per required or as per needed in the varieties of IT requirements. Aside of CapEx and OpEx perspectives, cloud computing comes with several aspects that able to mitigate limitation of on-premise IT infrastructures, in which allow the growth of organization and government entities to explore new technology such as big data, performance computing, artificial intelligence and other emergence that fall under Industry Revolution 4.0 (IR4.0).

Nonetheless, despite of the encouragement and support on cloud computing technology, challenges have been a technology growth demotivator for all types of IT innovations. Cloud computing is one of the technologies are slowly growth on acceptance and adoption due to its characteristics that has a root as a subscription based platform, in which leads to curiosity on the ownership values. Subscription based product introduced by the CSP has been a long prudent discussion among IT practitioner in the aspects of trust, cybersecurity and privacy. The increase of acceptance on cloud computing technology, the curiosity of the transparency of cloud services by CSP are being questions prudently by community and government sector. Upon the increase of cloud computing adoptions in from of subscription, high risk of data

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

breach are seems to be co-exist to each other. And, needless to say, this matter has been raised as a major issue by the industries and government on the concerns in the cybersecurity viewpoints. As the growth of cloud computing, this technology has been exposed to security risks such as data breach, hacking, denial of service attack etc. and these matters have raise many concerns from the CSS and CSP (Latif, Abbas, Assar, & Ali, 2014).

Security concerns raised as a crucial matters by CSS and CSP were defined in many forms and factors as such: (i) the requirements of data security, privacy, access control; (ii) diversity of frameworks, guidelines, legislation, compliance and audits; virtual environment risk; (iii) identity management, authentication and access control; (iv) data availability and business continuity; (v) application development; (vi) the availability of cloud services and data locations and data centres; (vii) vulnerability attacks; limited user access; (viii) as well as unclear service level agreements (Abolfazli et al., 2015; Benslimane, Yang, & Bahli, 2015; Hashizume, Rosado, Fernández-Medina, & Fernandez, 2013; Latif et al., 2014; Xiang, Shahpasand, & Jarno, 2019).

As these security concerns arise from the continuous usage and acceptance of cloud computing technology, there were several studies and research has been conducted to acknowledge these security concerns in ensuring the cloud computing technology are not been push aside as non-reliable technology, but to embrace its co-exitance with the security requirements. ISMS is a comprehensive assessment of information security that is not limited to provide accurate indications related to the level of information security but also able to assist in identifying aspects of information security that need improvement involves directly with the vision, mission and direction of the organisation (C.N.I.I., 2020). Through ISMS, security concerns on cloud computing technology implemented by CSP can be assessed through proper assessment process that indicated the security implementation in the cloud services by validating the CSP organization process, people and security implementation to uphold information security management.

Aside of process, people and security controls, ISMS covers various types of laws and regulations related to security and privacy, in which the assessment coverage have a wider view of security controls defined by ISMS, indeed covers the cloud computing security implementation of the CSP, as well as from the CSS perspectives (Jansen & Grance, 2011). Meanwhile, ISMS auditing is to provide the CSP and CSS organisation on the aspects of IT security assurance related to information security by adopting several standards (Rasheed, 2014). ISMS auditing standards covers ISO/IEC 27001:2013 and supported by guidance defined by ISO/IEC27002. Local laws and regulations are being covered as part of ISMS auditing process as per defined by the organization. The auditing process would be able to increase the integrity and confidence of CSS towards the CSP as well as be a benchmark for the level of information security system management of an organisation (C.S.M., 2013).

Nonetheless, the limitation of existing requirements of ISMS audit and certification, the cloud computing security aspects are reviewed from the surface points, in which, there was no technicality audit or assessment been performed on the cloud computing technology technical aspects and its security implementation through technical viewpoints. Example features are not been covered by common ISMS audit such as: hypervisor configurations, virtual machines management, multi-tenant access control, data protection on multi-tenant mode operations etc.

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Those limitations of audit coverage are eventuality been addressed by ISMS by the introduction of ISO/IEC 27017:2015. The creation of the ISO/IEC27017:2013 are to elaborate in detail the security controls and requirements defined by the ISMS in ISO/IEC27001:2013 by defining the specification cloud security requirements for CSP and CSS. ISO/IEC 27017:2015 of cloud computing standard is a code of practice for information security control based on ISO/IEC 27002: 2013, is focusing on cloud computing security control. Under the umbrella of ISMS audit and certification program, organization such as CSS and CSP able to console and leverage this method in assessing the security control implementation in the cloud services operations as well as giving assurance confidence to both CSS and CSP. As of 2018, there were 31,910 certificates ISMS produced for 59,934 locations worldwide (I.S.O./I.E.C., 2018). Therefore, this standard is an appropriate instrument to be use for cloud security compliance audit.

Even though ISMS audit and certification has put an effort to provide great assurance on the security controls implemented in the cloud services operations by CSP and through acceptance of CSS, limitations of the ISO/IEC27017:2015 are meant as guidance to the CSP and CSS, whilst are not meant to covers all types of security implementation of cloud security controls. This due to the ISO/IEC27001:2013 security controls are defined quite long ago. On that aspects of limitation, Cloud Security Alliance (CSA) has put a great initiative to promote Open Certification Framework (OCF) and Security, Trust and Security Registration Program (STAR) that meant specifically for cloud computing practitioner that includes CSP and CSS.

STAR program defined by the CSA are to accommodate the evaluation and certification requirements under the purview of OCF scheme. The STAR is an independent third-party evaluation process on the security controls implemented in the cloud services offers by CSP. This certification assessed the security control of the ISO/IEC 27001:2013 and evaluate together with the CSA Cloud Control Matrix (CCM) (Catteddu et al., 2018). However, the STAR certification are self-executed assessments performed by CSP and these introduce a gap on the certification process in which, there will be a tendency by the CSP to perform the assessment non-transparently. In regard to this, there is a crucial need for special method and approaches to ensure that the assessments performed are reliable and promote confidence in assurance by the CSS.

Aside of ISMS and CSA OCF, cloud computing is embedded in the IT managed services culture as part of datacentre providers. CSP deploys several datacentres to accommodate the needs of cloud computing services such as IaaS, PaaS and SaaS around the selected countries, regional and worldwide. In ensuring these cloud datacentres, which also known as software defined datacentres are also required to be evaluated and endorsed by entity such as Service Organization Control (SOC). SOC is an assessment program that introduced an assessment process and produce a report that been administered by a third parties consist of several certified public accountant (CPA) bodies. Through the SOC reports, organisations are able to gain consumer trust and confidence in the process and control of service delivery offered (Shackleford, 2012). The SOC report contains assessment findings that are do mentioned on cybersecurity elements that are beneficial to datacentre service providers inclusive of cloud datacentre managed by CSP. However, the overall contents of the report elaborate on the financial criteria related datacentre provider services and less focus on cybersecurity criteria.

Additionally, financial sector also has defined criteria of cybersecurity in their certification program, which is the Payment Card Industry, Data Security Standard (PCI DSS). PCI DSS is

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

a defined control that focuses on data security in payment cards processing system and is widely used in financial sector in business transactions. Security threats associated with payment card such as information leakage, lead to the need of standardization of data protection on financial information (P.C.I Security Standards Council, 2018). However, these controls are meant for financial sector requirements in managing financial transaction under payment industry, in which cybersecurity requirements are mostly defined to meet the financial industry expectations with generic focus.

By doing further comparison and gap analysis through all the mentioned standards, certification programs and cybersecurity requirements, it been decided that the security controls and criteria specifically defined for the cloud computing are been covered by ISO/IEC27017:2015, inclusive of its Annex A, security controls. Thus, in this study shall focus on the ISO/IEC27017:2015 standard inclusive of Annex A, as baseline criteria to develop the pre-assessment model for cloud security readiness level assessment approach through the methodology defined in this study.

Methodology

Existing Cloud Security Readiness Models Comparison Assessment

The initial stage of this study was to identify the existing studies covers on cloud security criteria that were assessing the level of cloud security implementations in the cloud services and operations within the CSP. There were several studies that shown the method and approaches made into models or framework that was leverage information security standards and cloud security criteria in assessing the cloud readiness or maturity level of cloud security implementations.

This study has took four (4) model and framework that defined the architecture assessment on the cloud security readiness that defined as baselines of this study. The following is the existing cloud security readiness assessment models, as stated below:

a) Framework 1: Six (6) Domain Framework;
b) Framework 2: Cloud Readiness Assessment Framework;
c) Model 1: Readiness Model for ICS and Cloud (***RMflC***); and
d) Model 2: Hexagonal Cloud Security Model.

Study 1 defined the model of security criteria based on these six (6) domains in understanding the level of readiness of information security implementation in the organization. These domains namely are Organisation (O), Stakeholders (S), Tools and Technology (T), Policy (P), Culture (C) and Knowledge (K) is used as a basic element in assessing the level of organisational readiness in the implementation of ISMS certification (Susanto, Almunawar, & Tuan, 2012). This framework elaborates the 21 important security controls taken from the information security management standard in ISO/IEC 27001:2013.

Framework 2 is built based on these combination of 3 perspectives: (i) Technology-Organisation-Environment (TOE), (ii) Diffusion on Innovation (DOI) and (iii) Technology Acceptance Model (TAM) (Alemeye & Getahun, 2015). From these uniquely defined criteria, the combination had produced twelve (12) readiness factors in determining the cloud readiness namely Perceived Usefulness (PU), Perceived Ease of Use (PE), Relative Advantage (RA), Trial- Ability Observable Result (TO), Compatibility with Existing Values and Practices (CE),

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

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) and Competitive Edge (CA).

Model 1 is a model consists of four (4) stages that assess the information security in the ICS components and cloud computing deployment as IT infrastructure. The stages are defined to feed the requirements of information security implementation of ICS system towards the usage of cloud computing as one of the ICS infrastructures in its ecosystem. These stages are defined as in: (i) implementation of component 1 through the method of analysing the suitability of the organisation; (ii) implementation of component 2 for testing organisational readiness of the value instruments (INKO); (iii) implementation of component 3 for the calculation of INKO; and (iv) determining the level of readiness of the organisation (SPKO) (Asma Zubaida M Ibrahim, Jamaiah H Yahaya, & Aziz Deraman, 2018).

Model 2 follows the aspects of cloud security by defining the importance of six (6) basic elements in information security for cloud computing, in which are: durability, availability, validity, confidentiality, utility, ownership, integrity and security (Bhatia & Malhotra, 2018). In the surface views of this model, helps the CSP to understand the security requirements as part of cloud security implementations from the operational views of cloud services.

Selection Criteria of Domains in Pre-Assessment Model for Cloud Security Readiness Development

Based on the two (2) frameworks and two (2) models mentioned as per discussed, added with supported facts on the literature reviews, there are seven (7) domains were selected for the proposed development of this study. In the process of domain selection from the defined frameworks and models, a baseline criteria of the domains selected was made based on the reference of cloud security readiness model study on the ISO/IEC 27017:2015 security controls excluding the Annex A (Nur Ilyani et al., 2019). With the mentioned study (Nur Ilyani et al., 2019) used as the foundation built-up of this study, domain selection criteria for the cloud readiness model persist on the pre-assessment stage were defined and helps in supporting this study in assessing the level of maturity or readiness of CSP in implementing cloud security controls on their cloud services operations.

The following is the definitions of the domains selected from the models and frameworks that shall be used as reference in this study specifically during the analysis and findings. These definitions are taken from all the previous study models and framework supporting with the facts found under literature review process.

Table 1: Domain Definition

Domain	Definition
Technology	Consist of IT infrastructure deployment adopted or implement by the industry organisation as in services for internal usage or in services for organization external. The purpose of this domain is in the application of information in the design, production, utilisation of goods and services, and in the organisation of human activities, which are divided into two categories: (1) Tangible: blueprints, models, operating manuals, prototypes. (2) Intangible: consultancy, problem-

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Domain	Definition
	solving, and training methods.
Organisation	Consist of community or an entity establishment, operates in form of systematically structured and managed to pursue collective goals on a continual basis, as in related to the industry or service concerned.
Policy	Described as a principle or rule to guide in decision making and achieve rational outcome(s), and reflective towards the implementation or enforcement in the regional aspects that shall be a consideration to the future development of the industry, or the relevant service concerned.
Stakeholder	A person, group, or organization that has direct or indirect influence in the organisation operations in forms that can affect or be affected by the organisation's actions, objectives, and process.
Culture	Determine the aspects to be consider in adaption as acceptable or unacceptable, important or unimportant, right or wrong, workable or unworkable. Consideration are based on the values and behaviours that contribute to the unique social and psychological environment of an organisation, inclusive of the experience of the organisation's past and current assumptions.
Knowledge	Consist of the sum of information in form of what is known, resides in the intelligence and value of the competency in people or individual. This domain as has been recognised as a factor of production and continuous improvement affecting the organization goals and future.
Environment	This domain covers everything that established around the organisation, from the market structures, competitive pressures and towards regulatory requirements in the perspective of information security systems.

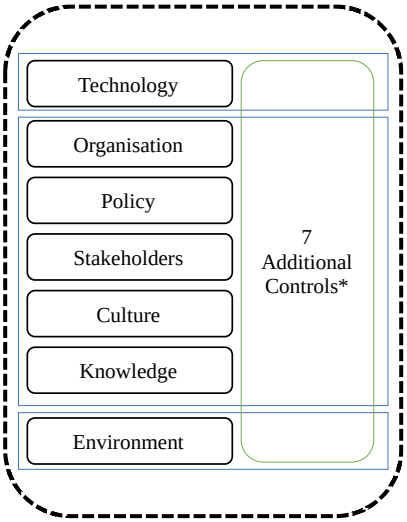
Development of the Pre-Assessment Model for Cloud Security Readiness

Based on the findings through the frameworks and models comparison, the domains selected as per defined in the definition, are based on the existing thirty-seven (37) security controls elaborated in the domain format from Nur Ilyani et al. (2019). There are used as the foundation in the creation of mapping between the domains towards the existed thirty-seven (37) security controls with added controls defined in Annex A controls of ISO/IEC27017:2015. The combination of thirty-seven (37) security controls and seven (7) security controls in Annex Aare used as the research instrument are been consolidate in domains structure in the process of developing the model for this study. The following Figure 1 described the pre-assessment model in form of high level view of the domains mapped towards the thirty-seven (37) security controls plus seven (7) security controls of ISO/IEC27017:2015 inclusive of Annex A.

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Cloud Service Readiness (CSR) Model
Source: Nur Ilyani Ahmad (2019)

Cloud Service Readiness (CSR) Model & Additional Controls ISO/IEC 27017:2015
Source: Nur Ilyani Ahmad (2019)



Pre Assessment Model for Cloud Security

Legend:
* Additional Controls from Annex A in ISO/IEC 27001:2013
6.3.1 Shared roles and responsibilities within a cloud computing environment
8.1.5 Removal of cloud service customer assets
9.5.1 Segregation in virtual computing environments
9.5.2 Virtual machine hardening
12.1.5 Administrator's operational security
12.4.5 Monitoring of cloud services
13.1.4 Alignment of security management for virtual and physical networks

Figure 1: Pre-Assessment Model for Cloud Security Readiness Assessment

The approach of the model development is through a combination both qualitative and quantitative methods, which are being divided into three (3) phases: (i) development preliminary model; (ii) verification of preliminary model; and (iii) validation of final model.

During the initial stage of the pre-assessment model development, study has been performed to map the defined domains towards the thirty-seven (37) security controls plus seven (7) security controls, which are in total of forty-four (44) security controls bounded to specific domains. And then, moving to the second phase of the development which is involved the verification process of the pre-assessment model. During the second phase, the activities covers two (2) processes, which are data collection and analysis. The method used in these two (2) processes are based on qualitative approach through interviews with the technical experts in the field of information security management and cloud computing. Upon the expert's feedback, the preliminary model will be improved towards constructing the agreed model.

The final stage of the pre-assessment model development is the process of validation on the agreed model through the prototype testing and questionnaire in the format of evaluation form. The prototype was built using Microsoft Excel, meanwhile the questionnaire was developed using Google Form. The validation will be carried out by respondents consisting of practitioners in the field of information security and cloud computing accumulated among ten (10) representatives. These representatives are selected based on organization that have obtained ISMS certification and in the process of obtaining ISMS certification for their cloud services. The prototype built with instrument consists of forty-four (44) security controls elaborated in form of ninety-four (94) checklists mapped towards the seven (7) defined

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

domains. The level of readiness is measured by a scale of Yes with a value of 1 or No with a value of 0. The total marks obtained for the domains are calculated using the formula as follows:

$$m = \frac{y}{d} \times 4 \quad (1)$$

Where; m = total score of domains; y = total answer of "Yes"; d = total question in each domain; and 4 = consists of 4 types assessment level (Not ready/ Low/ Intermediate/ High).

The overall average, p, each domain will be calculated using the following formula:

$$p = \sum_{i=1}^{7} \frac{mi}{7} \quad (2)$$

Where; m = total score each domain

The overall score obtained, p, will show the level of readiness of an agency with the scale of readiness level assessment as in Table 2. The defined level of readiness in Table 2 are referring to the study performed by Nur Ilyani et al. (2019).

Table 2: Level of Readiness

Total score, p	Level of Readiness
$0 \leq p \leq 1$	Not Ready
$1 < p \leq 2$	Low
$2 < p \leq 3$	Intermediate
$3 < p \leq 4$	High

Analysis

Experts Verification Analysis on the Pre-Assessment Model Prototype

Verification by experts involves the process of obtaining verification of the pre-assessment model. The experts are labelled into Expert A and Expert B. The experts had agreed on development of pre-assessment model that consists of the seven (7) domains (Nur Ilyani et al., 2019) along with forty-four (44) security controls relevant to the cloud security perspectives (I.S.O./I.E.C., 2015). However, the experts did provide recommendation for improvements on the several selected from the ninety-four (94) checklists in the control subsections as stated in Table 3.

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Table 3: Level of Readiness

Control in ISO/IEC27017	Recommendation	Expert
8.1.1	Proposed to include media handling methods, especially in data sanitation handling and media removal management.	Expert B
8.2.2	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance with reference to ISO/IEC 27002:2013.	Expert A
10.1.1	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance with reference to ISO/IEC 27002:2013.	Expert A
12.4.3	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance with reference to ISO/IEC 27002:2013.	Expert A
6.1.1	Proposed to include additional controls as contained in the control subsections 14.2.4 (Annex A) and 13.2.2 (Annex A)	Expert B
15.1.1	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance with reference to ISO/IEC 27002:2013.	Expert A
5.1.1	Proposed to include additional controls as in control section 6.1 based on requirements as such: Policies, Principles or Rules that need to be followed in making a decision, in which being able to achieve optimal results in services in an industry.	Expert B
12.1.5	Proposed to include additional controls as found in control subsection 12.3, where it impacts management to make decisions regarding the cost of duplicating data that belong to CSS.	Expert B
16.1.1	Proposed to include additional controls as in all control subsections 16.1.	Expert B
7.2.2	Proposed to include additional controls as in subsection control 7.1 (Annex A) for the previous / current / termination stage for employment.	Expert B
11.2.7	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance	Expert A

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Control in ISO/IEC27017	Recommendation	Expert
	with reference to ISO/IEC 27002:2013.	
	Proposed to consider including all controls in the control subsection 11.2 and not limited to 11.2.7 only.	Expert B
14.1.1	Proposed to consider incorporating all controls in subsection control 14.1 under one statement.	Expert B
14.2.1	Proposed that the checklist be further refined based on the ISO/IEC 27017:2015 Implementation Guidance with reference to ISO/IEC 27002:2013.	Expert A
	Proposed to consider incorporating all controls in subsection control 14.2 under one statement.	Expert B

Pre-Assessment Model Prototype Testing And Findings Analysis

Validation on the feedback provided by experts were from practitioners with vast experienced in the cloud technology, cloud security implementation and ISMS. The validation process involved the respective representatives from the organizations to perform the prototype testing and provided answers to the questionnaires. The overall score from the prototype testing from the respondents presented in Table 4 and Figure 2.

Table 4: Respondents Overall Score

Respondent Code	Overall Score	Level of Readiness
R1	3.64	High
R2	2.95	Intermediate
R3	3.19	High
R4	3.19	High
R5	3.67	High
R6	3.19	High
R7	3.43	High
R8	3.66	High
R9	3.89	High
R10	4.00	High
R11	2.86	Intermediate

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

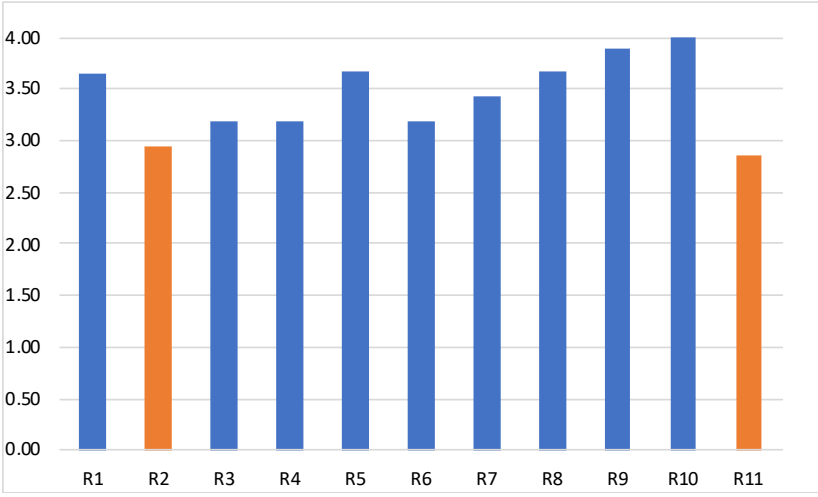


Figure 2: Score for Respondents

Based on these results, there are nine (9) respondents namely R1, R3, R4, R5, R6, R7, R8, R9 and R10 have achieved a high level of readiness while the remaining two (2) practitioners, R2 and R11 indicates intermediate level of readiness.

In addition, out of the seven (7) domains listed, it was found that six (6) domains namely technology, organisation, policy, culture, knowledge and environment recorded a high level of readiness. Meanwhile, stakeholder domain recorded on at the intermediate readiness level. The average score for each domain can be referred in Table 5 and Figure 3.

Table 5: Overall Score according to Domain

Domain	Average Score	Level of Readiness
Technology	3.36	High
Organisation	3.26	High
Policy	3.74	High
Stakeholders	2.73	Intermediate
Culture	3.86	High
Knowledge	3.27	High
Environment	3.76	High

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

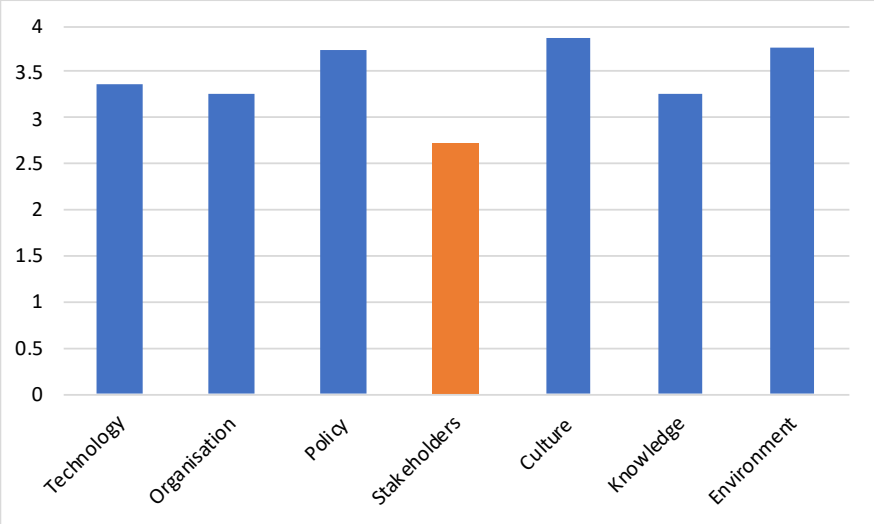


Figure 3: Score for Domain

Among the seven (7) defined domains, the stakeholder domain is registered at the lower value radar compared to other measurements between the other domains, in which this domain obtains intermediate level of readiness as shown in Figure 4.

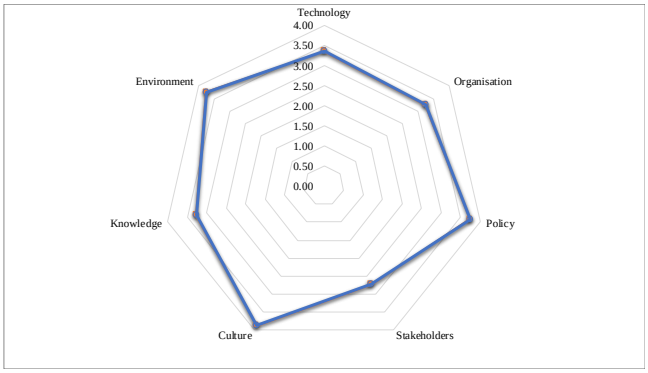


Figure 4: Radar Chart for Readiness Level

The results obtained from validation questions found that the prototype developed has successfully answered. The results show there were 45.5% of practitioners strongly agree with the effectiveness of the prototype testing and the following illustrate the level of effectiveness can be referred in Figure 5.

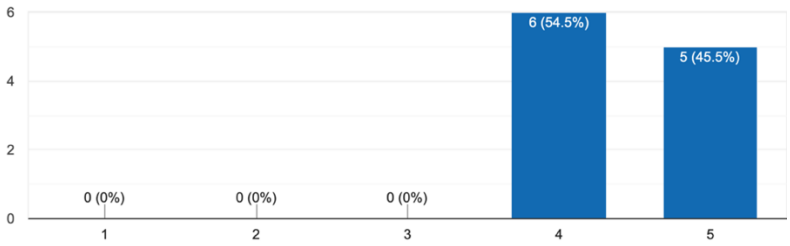


Figure 5: Achievement of Effectiveness Level

In addition, the following results show there were 54.5% of practitioners strongly agreed with the level of the efficiency of the prototype testing can be referred in Figure 6.

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972
IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

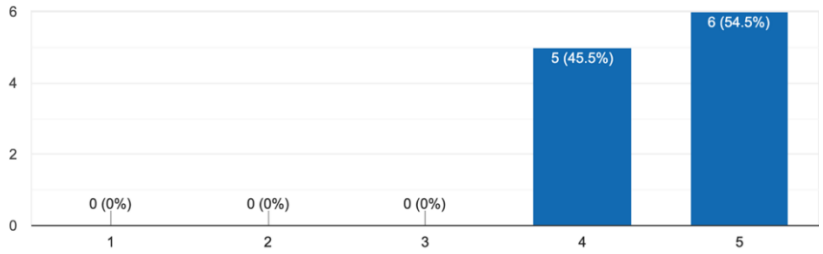


Figure 6: Achievement of Efficiency Level

Overall, the findings from the prototype testing and validation has showed that the pre-assessment model for the cloud security readiness assessment is reliable to assist CSP in evaluating the cloud service security readiness level effectively and effortlessly being performed without wasting the organisation resources.

Limitation and Future Work

In this study, there are definite limitations was found, in which this study focuses on organisations that have been accredited and in practice ISO/IEC 27001:2013. With the increasing of cyber security incidents, it is crucial to perform further study on the level of cloud security readiness of organisations that has not yet accredited and practice ISO/IEC 27001:2013. Future study of the pre-assessment model on cloud security readiness can be further improved by incorporating on method of handling privacy requirements for both CSP and CSS.

Recommendation and Conclusion

The study conducted has successfully met its objectives and providing beneficial to the organization specifically CSP. Through this study, it has successfully identified the factors that affect the CSP in the aspects of cloud readiness level of cloud services operations. Besides, it became the starting point in the development of the pre-assessment model consist of (7) domains that mapped towards the forty-four (44) controls based in ISO/IEC 27017:2015.

Based on the prototype developed, it was able to be used in assessing the cloud security implementation in the CSP by determined the cloud security readiness level, whilst organisation is guided with tool that able to assist them in evaluating their cloud security readiness level effectively, thus promoting organisation awareness in cloud computing security. Ultimately, the agreed model can serve as a guideline for any organisation in the effort to provide secure cloud computing services that can be accredited by a worldwide recognised certification standard.

References

Abbas, A., & Khan, S. U. (2014). A Review on the State-of-the-Art Privacy-Preserving Approaches in the E-Health Clouds. *IEEE J Biomed Health Inform, 18*(4), 1431-1441. Retrieved from https://www.ncbi.nlm.nih.gov/pubmed/25014943

Abolfazli, S., Sanaei, Z., Tabassi, A., Rosen, S., Gani, A., & Khan, S. U. (2015). Cloud Adoption in Malaysia: Trends, Opportunities, and Challenges. *IEEE Cloud Computing, 2*(1), 60-68.

Alemeye, F., & Getahun, F. (2015). *Cloud Readiness Assessment Framework and Recommendation System.* Paper presented at the AFRICON 2015.

International Journal of Innovation and Industrial Revolution
IJIREV
EISSN: 2637-0972
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Ali, M., Dhamotharan, R., Khan, E., Khan, S. U., Vasilakos, A. V., Li, K., & Zomaya, A. Y. (2017). Se.Da.S.C: Secure Data Sharing in Clouds. *IEEE Systems Journal, 11*(2), 395-404.

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.

Benslimane, Y., Yang, Z., & Bahli, B. (2015). *Key Topics in Cloud Computing Security: A Systematic Literature Review.* Paper presented at the 2015 2nd International Conference on Information Science and Security (ICISS).

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.

C.N.I.I. (2020). Information Security Management System (ISMS). Retrieved from https://cnii.cybersecurity.my/main/isms.html

C.S.M. (2013). *ISMS Implementation Guideline: A Practical Approach*(pp. 1-58). Retrieved from https://www.cybersecurity.my/data/content_files/11/1170.pdf?.diff=1375349394

Catteddu, D., Chin, V., Cordero, S., Foo, A.-P., Laris, K., Maaloul, A., . . . Tierling, E. (2018). *Methodology for the Mapping of the Cloud Controls Matrix (CCM)*(pp. 1-12). Retrieved from https://downloads.cloudsecurityalliance.org/assets/research/cloud-controls-matrix/ccm-mapping-methodology.pdf

Giulio, C. D., Sprabery, R., Kamhoua, C., Kwiat, K., Campbell, R., & Bashir, M. N. (2017). *IT Security and Privacy Standards in Comparison: Improving FedRAMP Authorization for Cloud Service Providers*. Paper presented at the 2017 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID).

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An Analysis of Security Issues for Cloud Computing. *Journal of internet services and applications, 4*(1), 5.

I.S.O./I.E.C. (2015). ISO/IEC 27017:2015 Code of Practice for Information Security Controls Based on Iso/Iec 27002 for Cloud Services. In.

I.S.O./I.E.C. (2018). The ISO Survey of Management System Standard Certifications 2018. Retrieved from https://isotc.iso.org/livelink/livelink/fetch/-8853493/8853511/8853520/18808772/0._Explanatory_note_on_ISO_Survey_2018_results.pdf?nodeid=20719021&vernum=-2

Jansen, W., & Grance, T. (2011). *Guidelines on Security and Privacy in Public Cloud Computing*. Retrieved from

Jasmin, N. E., & Hasan, M. K. (2018). Framework for the Implementation of E-Government System Based on Cloud Computing for Malaysian Public Sector. *Asia-Pacific Journal of Information Technology and Multimedia, 7*(1), 1-18.

Latif, R., Abbas, H., Assar, S., & Ali, Q. (2014). Cloud Computing Risk Assessment: A Systematic Literature Review. In *Future information technology* (pp. 285-295): Springer.

Nur Ilyani, A., Ibrahim, M., Maslina, D., Ahmad Dahari, J., & Norlaili, A. H. (2019, 9-10 July 2019). *Cloud Service Provider Security Readiness Model: The Malaysian Perspective.* Paper presented at the 2019 International Conference on Electrical Engineering and Informatics (ICEEI).

P.C.I Security Standards Council. (2018). *Payment Card Industry (PCI) Data Security Standard (DSS)*. Retrieved from https://www.pcisecuritystandards.org/

International Journal of Innovation and Industrial Revolution
EISSN: 2637-0972 IJIREV
Volume 2 Issue 5 (December 2020) PP. 01-17
DOI 10.35631/IJIREV.25001

Pauley, W. (2010). Cloud Provider Transparency: An Empirical Evaluation. *IEEE Security & Privacy, 8*(6), 32-39.

Rasheed, H. (2014). Data and Infrastructure Security Auditing in Cloud Computing Environments. *International Journal of Information Management, 34*(3), 364-368. Retrieved from http://www.sciencedirect.com/science/article/pii/S026840121300145X

Shackleford, D. (2012). Using SSAE 16 Standard, SOC Reports to Assess Cloud Provider Security. Retrieved from https://searchcloudsecurity.techtarget.com/tip/Using-SSAE-16-standard-SOC-reports-to-assess-cloud-provider-security

Shahzad, F. (2014). State-of-the-Art Survey on Cloud Computing Security Challenges, Approaches and Solutions. *Procedia Computer Science, 37*, 357-362.

Susanto, H., & Almunawar, M. N. (2012). Information Security Awareness within Business Environment: An IT Review. *Available at SSRN 2150821*.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2012). Information Security Challenge and Breaches: Novelty Approach on Measuring ISO 27001 Readiness Level. *International Journal of Engineering and Technology, 2*(1), 67-75.

Tweneboah-Koduah, S., Endicott-Popovsky, B., & Tsetse, A. (2014). Barriers to Government Cloud Adoption. *International Journal of Managing Information Technology, 6*(3), 1-16.

Xiang, O. X., Shahpasand, M., & Jarno, A. D. (2019). A Systematic Review on Could Security Auditing. *Journal of Advanced Research in Dynamical and Control Systems, 11*(1 Special Issue), 1526-1532. Retrieved from https://www.scopus.com/inward/record.uri?eid=2-s2.0-85071004581&partnerID=40&md5=bcb2dff8f9031b36208e7d66f23f15ab