SEMARAK ILMU
PUBLISHING
202103268166(003316878-P)

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Framework for the Development of Risk-Based Guidelines for Cloud Service Subscribers

Noraida Haji Ali[1,*], Masita Jalil[1], Ahmad Dahari Jarno[2], Norahana Salimin[3], Mohammed Alamiah[4]

[1] Faculty of Ocean Engineering Technology and Informatics, Universiti Malaysia Terengganu, 21030 Terengganu, Malaysia
[2] CyberSecurity Malaysia, 63000 Cyberjaya, Malaysia
[3] Bank Muamalat, Malaysia Berhad, 50100 Kuala Lumpur, Malaysia
[4] Faculty of Information Technology, Aqaba University of Technology, Aqaba 11947, Jordan

ARTICLE INFO

Article history:
Received 19 October 2023
Received in revised form 18 April 2024
Accepted 15 June 2024
Available online 15 July 2024

Keywords:
Cloud Service Subscriber; risk-based guideline; cloud security; public cloud services

ABSTRACT

Cloud computing provides services for Cloud Service Subscriber (CSS) to allow flexible IT solutions to be deployed without the need to procure physical IT infrastructures such as servers, storage, and processing components. Such benefits particularly in terms of cost savings coupled with the need to embrace digitization and a remote workforce have contributed to a surge in cloud service adoption. However, the increase in users and cloud computing service providers' statistics comes with higher rates of security incidents and cyber-attacks targeting cloud computing infrastructure. Therefore, adequate security controls are essential to ensure the confidentiality, integrity, and availability of customer data can be controlled and protected. This paper presents a framework for developing a risk-based guideline for Cloud Service Subscribers (CSS). This framework aims to formalize a generic set of guidelines on cloud security measures and controls for easy reference by CSS. The framework is based on the analysis of existing cloud security literature and existing ISO/IEC, including other best practices and related activities that have been carried out to generate guidelines for cloud security. The outcome is a cloud security guideline modelled into three (3) main stages and seven (7) activities that detail the set of actions. The framework is focused on an IT security perspective covering pre-subscription, during-subscription, and post-subscription of the cloud services. The framework may also serve as the guidelines for organizations or agencies to develop similar guidelines for different service perspectives or different cloud models.

1. Introduction

Cloud computing enables flexible computational resources or IT solutions to be deployed without the need to procure physical IT infrastructures such as servers, storage, and processing components. According to the National Institute of Standards and Technology (NIST), cloud computing enables convenient, on-demand network access to a pool of configurable computing resources that can be quickly provisioned and released with little management work or service provider involvement [1].

[*] *Corresponding author.*
E-mail address: aida@umt.edu.my

https://doi.org/10.37934/araset.48.2.136147

The benefits of cloud computing particularly in terms of cost savings have contributed to the continuous rise in cloud service adoption. According to Gartner, the pandemic has also accelerated cloud adoption to allow for business resilience and evolution and to support remote working and learning [2].

However, the increase in subscribers and cloud computing service providers comes with higher rates of security incidents and cyber-attacks targeting cloud computing infrastructure vulnerabilities [3-5]. Therefore, adequate cloud security controls are essential to ensure customer data's confidentiality, integrity, and availability can be controlled and protected. Public clouds that enable public users to host their services are regarded as the most vulnerable deployment models particularly due to the diversity of users using the services [2,6]. Today's cloud hosting service serves over a billion users worldwide, providing them with stable, low-cost, reliable, high-speed, and globally available resource access [7].

In a typical cloud computing environment, there are two entities involved: a cloud service provider (CSP) and a cloud service subscriber (CSS) or a cloud user. A CSP manages the computing infrastructure and offers services through network access, while a CSS consumes the services without the need to procure physical infrastructures. CSPs must provide adequate cloud security controls to ensure that confidentiality, integrity, and customer data are protected without compromise. It is also crucial for CSS to be aware of the important aspects of the services, understand the security risks involved when subscribing to cloud services as well as responsibilities in terms of security management and associated risks of cloud subscription, and thus appropriate security controls in mitigating them [3,4,8,9].

Cloud security or cloud computing security, refers to the discipline and practice of protecting cloud computing environments, infrastructure, applications, data, and information [10]. It entails securing cloud environments against risks such as unauthorized use or access, cyber-attacks, hackers, malware, insecure APIs, and other security threats [11-13]. Cloud or security controls are countermeasures that can be taken by organizations (CSPs or CSSs) to manage and mitigate the risks [14,15]. Cloud security controls can be in the form of guidelines, policies, procedures, and practices [16-18]. Examples of security controls include managing privileged access rights and policy on the use of cryptographic controls [19].

In this work, we propose a framework to formalize a generic set of guidelines on cloud security measures and controls for easy reference by CSSs. The framework is based on the analysis of existing cloud security literature and existing ISO/IEC, including other best practices and related activities that have been carried out to generate guidelines for cloud security. This framework can be used as a reference to develop guidelines for different perspectives, for example, guidelines for Cloud Service Providers (CSPs).

The cloud security guideline covers security requirements for the three (3) main cloud service models: i) Infrastructure as a Service (IaaS); ii) Platform as a Service (PaaS); and iii) Software as a Service (SaaS). It serves as a guide to aid CSS in understanding public cloud security features that should be applied to the different cloud service models at three (3) different subscription stages: i) pre-subscription, ii) during subscription, and iii) post-subscription of the cloud services [19].

2. Related Works

To date, cloud computing has been widely deployed across a wide range of fields, including industry, education, healthcare, construction, and government. One of the largest problems facing CSPs and CSSs from business, government, and academia is that cloud security has not kept up with the rapid uptake of its services [20].

Threats to the confidentiality, integrity, and accessibility of cloud resources are becoming more commonplace in recent years as highlighted in many recent survey findings [21-26]. Hence, it is crucial to take security and privacy into account when designing and using cloud services where security issues indicate potential problems that might arise.

Although there have been signs of improper use of cloud hosting, it can be difficult to comprehend these abuses. CSPs typically avoid reviewing the content of their clients' repositories in the absence of proper authorization because they are constrained by their obligations to protect customer privacy and ethical considerations [5,26].

Many researchers have conducted work related to the security and privacy issues in cloud computing. Popovic and Hocenski [27] presented some standards that can be used to address security issues in cloud computing such as the Information Technology Infrastructure Library (ITIL), International Organization for Standardization (ISO 27001/27002), and Open Virtualization Format (OVF). Guidelines for managing cloud security which include cloud governance, cloud transparency, and cloud computing security impacts were presented by Ramgovind *et al.,* [28].

A cloud security management framework was first proposed by Almorsy *et al.,* [29]. This framework is aligned with the Federal Information Security Management Act (FISMA) standard to work with the cloud computing model. A management layer, an enforcement layer, and a feedback layer are the three principal layers of the framework, each of which is responsible for key security services. Cloud providers can use it to manage their cloud platform security, cloud consumers to manage their cloud-hosted assets, and as a security-as-a-service tool to help cloud consumers outsource their Security Management Process (SMP) to the cloud, which ideally could improve collaboration between the different cloud stakeholders. The validated framework was deployed on a cloud platform test bed and evaluated by managing various secure multi-tenant SaaS applications. The findings simply suggest that more guidelines could be modified to include implementability content. Numerous opportunities were identified by which guidelines could be modified to potentially facilitate their use. New governance structures may be required to accommodate the development of guidelines with these features [30].

Another secure cloud computing framework proposed by Youssef and Alageel [31] consists of three essential security components; each of which includes important challenges related to cloud security and privacy. These components are: (i) security and privacy requirements - identifies security and privacy requirements for the cloud such as authentication, authorization, integrity, etc.; (ii) attacks and threats - warn from different types of attacks and threats to which clouds are vulnerable, and (iii) concerns and risks - pay attention to risks and concerns about cloud computing.

Alenezi *et al.,* [32] presented a three-dimensional framework to facilitate organizations in assessing their readiness to perform cloud forensic investigation on an IaaS service model. The assessment considers influencing factors under three dimensions, namely technological, legal, and organizational factors. When organizations are ready to capture data in advance of an incident, this could translate into potential cost savings.

Another framework by Rupra and Omamo [33] produces a security index to describe the security level of a cloud computing environment. It aims to aid SMEs in analyzing their current level of security and identifying their targeted security index.

A more recent work by Tissir *et al.,* [34] proposed a framework to guide organizations in managing and mitigating cyber risks based on ISO and NIST standards. The work also set the base criteria for measuring the maturity level of organizations that implement the framework.

Table 1 summarizes key related works on the Cloud Computing framework. Collectively, these works contribute a comprehensive perspective on cloud computing security, offering valuable tools and insights for practitioners, organizations, and researchers working in this dynamic and critical domain and highlighting the importance of considering various aspects to ensure robust protection in cloud computing environments.

Table 1
Summary of related works on Cloud Security Framework

Author [Ref]	Type of Document	Focus
Almorsy *et al.,* [29]	Cloud Security Management Framework	Aligned with FISMA standard to work with the cloud computing SaaS model.
Youssef and Alageel [31]	Cloud Computing Framework	Identifying security and privacy requirements, attacks, threats, concerns, and risks associated with cloud deployment.
Alenezi *et al.,* [32]	Framework	Assessing readiness to perform cloud forensic investigation on an IaaS service model.
Rupra and Omamo [33]	Framework	Producing a security index to describe the security level of a cloud computing environment.
Tissir *et al.,* [34]	Framework	Guiding organizations in managing and mitigating cyber risks based on ISO and NIST standards. Establishing base criteria for measuring the maturity level of organizations implementing the framework

Many other works in the literature discuss different issues in cloud computing security. Much of the ongoing work focuses on developing approaches that can address these issues on specific cloud service models. Cloud Security Alliance (CSA) developed a document titled Security Guidance for Critical Area of Focus in Cloud Computing, which identifies specific cloud security risks in different areas including architecture, governance, and operational risks, and provides recommendations for mapping them [10].

In existing cloud systems, the translation or mapping of security risks and controls is however done manually [20]. Such a method can be laborious, and prone to errors which inevitably results in an increased vulnerability to cyber risks. Moreover, CSSs may overlook important security controls due to a lack of awareness or simply not having cloud expertise in the organizations. Tunc *et al.,* [20] demonstrated how a cloud environment may be set up by CSPs to automatically apply the required NIST SP 800-53 security controls. The methodology could regularly check and validate the implemented controls to avoid the drawbacks of the manual approach. The automation by CSPs is however focused only on the IaaS service model.

In this paper, we present a practical framework geared toward creating a Risk-Based Cloud Security Guide, primarily aimed at Cloud Service subscribers. The goal is to develop a comprehensive guide for achieving a higher security level in the cloud. Our framework provides clear advice on various aspects of secure cloud usage, covering security and privacy needs, potential threats and attacks, and addressing the risks and concerns associated with cloud security.

Additionally, we propose a general security model for cloud computing designed to meet its unique security requirements and protect against potential malicious activities. This framework also serves as a helpful tool for organizations, offering guidance on implementing specific security measures at different stages of subscription (Pre, During, and Post), which are based on controls that are defined in ISO/IEC 27036-4:2016(E) as well as mapping of Cloud Security Controls from ISO/IEC 27036-4 with ISO/IEC 27017:2015 for Cloud Service Subscribers [35,36]. By following this approach, organizations can establish a structured and effective strategy to strengthen cloud security, address challenges, and promote a safer cloud computing environment.

3. Methodology

Developing a framework involves a systematic and structured approach to creating a set of guidelines, processes, and structures to address specific challenges or achieve objectives. As illustrated in Figure 1, the six-step methodology is followed in developing the framework.

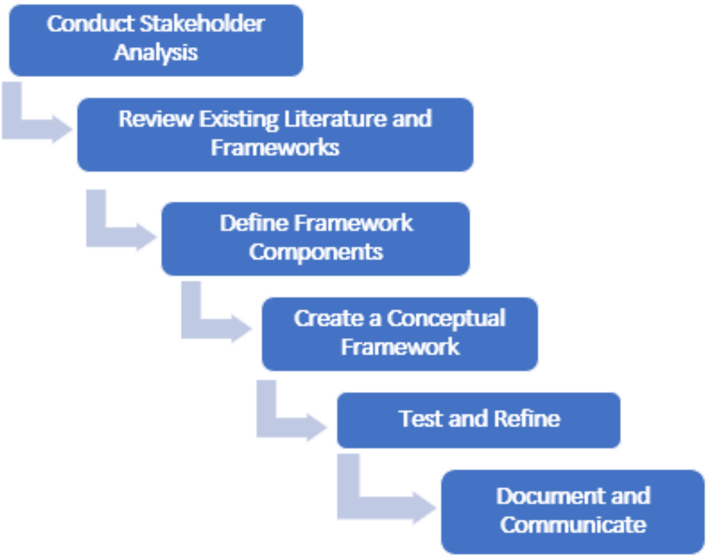
Conduct Stakeholder Analysis
Review Existing Literature and Frameworks
Define Framework Components
Create a Conceptual Framework
Test and Refine
Document and Communicate

Fig. 1. Framework for guideline development

3.1 Conduct Stakeholder Analysis

Conducting a stakeholder analysis is a pivotal step in developing a framework, involving the identification and examination of key individuals, groups, or organizations who either influence or are influenced by the framework. Through methods such as interviews, surveys, and workshops, stakeholders' needs, expectations, and concerns are carefully gathered, categorized based on influence and interest, and then prioritized to ensure their perspectives are integral to the framework's objectives. Communication strategies are tailored to different stakeholder groups, providing regular updates, and seeking feedback to manage expectations and address potential conflicts. This iterative engagement process ensures that the evolving framework aligns with stakeholder interests, fostering acceptance and effectiveness throughout its development.

3.2 Review Existing Literature and Frameworks

Reviewing existing literature and frameworks is a crucial phase in framework development, involving a comprehensive examination of previously published materials, industry standards, and established frameworks relevant to the subject matter. This process aims to identify best practices, lessons learned, and innovative approaches that can inform the design of the new framework. By analyzing this body of knowledge, developers gain insights into the successes and shortcomings of similar initiatives, enabling them to build upon established foundations and avoid potential pitfalls. The review also ensures that the new framework aligns with current industry standards and remains informed by the latest advancements in the field, enhancing its robustness and adaptability to contemporary challenges.

3.3 Define Framework Components

A framework component refers to a distinct and essential part of the overall framework structure, representing a key element or module with a specific purpose within the system. Each component is carefully defined to contribute to the framework's functionality, and the interplay between these components is orchestrated to achieve the framework's overarching objectives. These components can encompass various aspects, such as guidelines, processes, methodologies, or tools, each playing a unique role in supporting the framework's intended outcomes. The definition and delineation of these components provide a detailed roadmap for the implementation and utilization of the framework, ensuring clarity and coherence in addressing the targeted challenges or goals.

3.4 Create a Conceptual Framework

Creating a conceptual framework is a crucial stage in the development process. It involves constructing a visual representation that outlines the key components, relationships, and flow of the framework. This graphical model serves as a blueprint, illustrating the underlying structure and logic of the framework's design. By visually mapping out the various elements and their interconnections, stakeholders can gain a clear understanding of how the framework functions and how different aspects relate to one another. The conceptual framework not only provides a high-level overview but also guides the subsequent detailed development phases, ensuring consistency and coherence in implementing the framework's principles and concepts.

3.5 Test and Refine

The "Test and Refine" phase is a critical step in the framework development process, involving the practical evaluation and validation of the framework's elements in a controlled environment. During this phase, the framework is subjected to simulations, pilot programs, or other testing methods to assess its effectiveness, identify potential weaknesses, and gather real-world feedback. Stakeholders, including end-users and relevant experts, are actively involved in providing insights and evaluating how well the framework aligns with its intended objectives. Based on the findings from the testing phase, adjustments and refinements are made to enhance the framework's functionality, usability, and overall performance. This iterative approach ensures that the framework evolves to meet the needs of its users and effectively addresses the challenges it was designed to tackle.

3.6 Document and Communicate

The "Document and Communicate" phase is a crucial aspect of framework development, involving the comprehensive documentation of the framework's components, principles, and operational details. This documentation serves as a detailed guide, providing stakeholders with a clear understanding of the framework's structure, purpose, and implementation procedures. Additionally, tailored communication strategies are developed to disseminate this information effectively among stakeholders, ensuring that key messages about the framework's goals and functionalities are conveyed accurately. By documenting and communicating the framework, developers establish a common understanding among all involved parties, fostering transparency and facilitating a smoother implementation process. Regular updates and clear channels of communication further contribute to the ongoing success and acceptance of the framework within the targeted audience.

By adhering to this methodology, a well-defined and purposeful framework can be developed to meet the needs of stakeholders in a dynamic environment.

4. The Proposed Framework for the Development of Risk-Based Cloud Security Guideline

To create a thorough guideline, we suggest employing a three-phase framework that actively engages all stakeholders. This approach allows for a structured and methodical process, ensuring the development of a risk-based guideline that adheres to the recommended cloud security controls.

As depicted in Figure 2, the framework is divided into three (3) phases which are the Requirement, Development, and Endorsement phases. Each phase has different activities as follows:

(i) Requirement Phase
 - Data Gathering, Analysis of Requirement, Mapping and Alignment Process

(ii) Development Phase
 - Document Preparation, Focus Group Review Process

(iii) Endorsement Phase
 - Public Review Process, Finalize Document

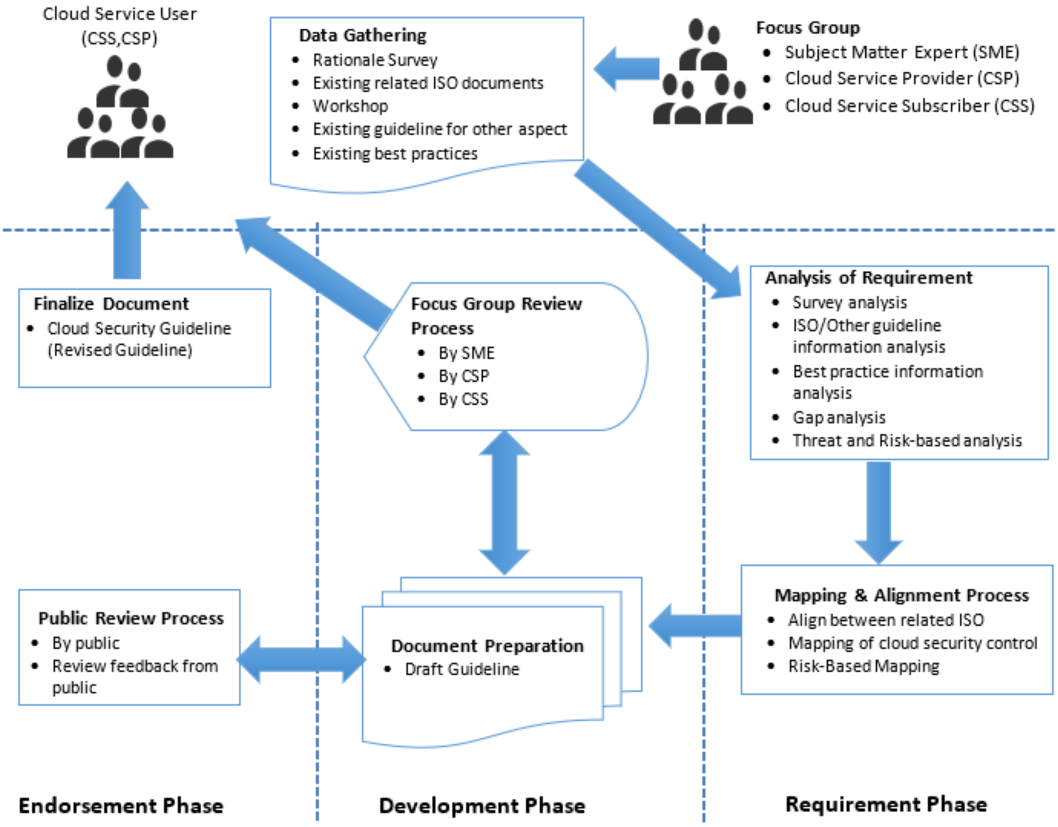
Cloud Service User
(CSS,CSP)
Data Gathering
• Rationale Survey
• Existing related ISO documents
• Workshop
• Existing guideline for other aspect
• Existing best practices
Focus Group
• Subject Matter Expert (SME)
• Cloud Service Provider (CSP)
• Cloud Service Subscriber (CSS)
Finalize Document
• Cloud Security Guideline (Revised Guideline)
Focus Group Review Process
• By SME
• By CSP
• By CSS
Analysis of Requirement
• Survey analysis
• ISO/Other guideline information analysis
• Best practice information analysis
• Gap analysis
• Threat and Risk-based analysis
Public Review Process
• By public
• Review feedback from public
Document Preparation
• Draft Guideline
Mapping & Alignment Process
• Align between related ISO
• Mapping of cloud security control
• Risk-Based Mapping
Endorsement Phase
Development Phase
Requirement Phase

Fig. 2. Framework for guideline development

4.1 Requirement Phase

The requirement phase involves three main activities: data gathering, requirement analysis, and mapping and alignment process, as elaborated below.

4.1.1 Data gathering

Firstly, a rational survey should be conducted to find the problem or issues on cloud security from a cloud subscriber perspective. Existing guidelines and best practices for solving cloud security issues should be referred to as a comparison of what has been developed by the community and industry to avoid redundancy. From there, existing International Organization for Standardization (ISO) documents can be used as a reference to identify the latest standards developed by global experts in the Cloud domain. ISO documents may provide high-level requirements and controls. The guideline to be developed may refine and further elaborate the ISO requirements and controls in terms of practical approach and implementation. A series of workshops which will be attended by experts in relevant areas should be conducted where it will be a platform to discuss the guideline content. It is important to ensure the participants come from different backgrounds such as government agencies, industries, and academics so that views from different perspectives can be obtained.

4.1.2 Analysis of requirement

Next, survey results should be analysed to determine the problem statement that will lead to the objective of developing the guideline. From the survey, cloud security incidents occurred in public cloud services at different subscription stages. The cloud subscriber needs to have different controls taken during different subscription stages. A gap analysis should be conducted between current guidelines that have already been developed by the community and industry and the new guideline that needs to be developed to solve issues related to cloud security. A mapping of the cloud security controls, with the respective standards, for each stage of cloud service subscription should be developed. The mapping should be referred for analysis and provide a quick guide to the cloud subscriber in identifying the required or recommended security controls based on ISO/IEC 27036-4:2016(E), (with cross-references for cloud services and deployment models and relevant standards) at the different stages of the subscription. For this ISO, the security threats and risks that have been determined are mapped to the cloud services models (SaaS, PaaS, IaaS) [19].

4.1.3 Mapping and alignment process

Common threats and risks of the cloud service model are based on the ISO/IEC 27036-4:2016(E). Risks and threats for each stage of the cloud subscription; Pre, During, and Post are associated with risks and threats of ISO/IEC 27036-4:2016(E). Controls for each subscription stage for every cloud service model are referred to relevant controls discussed in ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E). Samples of threats and risks mapped to cloud service models based on subscription stages are given in Table 2.

Table 2
Threats and risk mapped to cloud service models based on subscription stages

Typical Threats and Risks	Subscription Stage	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Lack of control over where the subscriber data are stored	PRE DURING	Where the Subscriber data are stored?		Not applicable to the Subscriber
	POST	Not applicable to the Subscriber		
Unknown access to store the subscriber data	PRE	Who has access to the stored Subscriber data?	Who has access to or availability of stored the Subscriber data?	
	DURING	Who has access to or availability of the stored subscribers' data?		
	POST	Not applicable to the Subscriber		

If the controls do not apply to the cloud subscriber, it is recommended for the cloud provider to comply with minimum security controls defined in the ISO/IEC 27017:2015(E) and ISO/IEC 27002:2013(E). Otherwise, the cloud subscriber should perform a proper risk assessment to understand the risk that might be present.

4.2 Development Phase

Once controls for each service delivery are identified and correctly mapped to the right subscription stages, this phase concentrates on the development of the risk-bask cloud security guideline.

4.2.1 Document preparation

The guideline is drafted based on the mapping and alignment process between related ISO documents, security controls, and risk that is associated with the threats. The structure of the guideline should contain:

(i) Introduction - Overview, Scope, Objective, Intended Audience, Rationale of developing the guideline
(ii) Overview of Cloud Computing – Cloud Computing Service Model, Cloud Deployment Model, Cloud Security Controls, Risk Assessment, Selection Criteria of the Cloud Service Provider, Responsibilities of Cloud Subscriber and Provider, Cloud Deployment Models
(iii) Threats and Risk in the Cloud Service model based on subscription stages (pre-subscription, during subscription, and post-subscription)
(iv) Mappings of Cloud Security controls between ISOs
(v) Guidance for cloud subscribers of SaaS, PaaS, and IaaS during each subscription Stage (pre-subscription, during subscription, and post-subscription)

4.2.2 Focus group review process

The focus group consists of subject matter expert members from the public (government agencies), private (CSP, application developer), and academic (higher learning institution) sectors related to Cloud. The public sector can give their perspective from the user or CSS point of view. Private sectors like application developers can also give their view from a cloud subscriber or cloud tenant context. Private sectors like CSP can give their view from the service provider angle. The private sector is also the party that will have the most exposure to the latest technologies used in cloud architecture and deployment, which will greatly assist in ensuring the content of the guideline is up-to-date and practical. Academic sectors can give their perspective from the latest research and development context.

Typically, the focus group will have three (3) rounds of review process. The review process can be conducted individually or in groups among members during the workshop. The first round of review is on the first draft of the guideline. The members can give out their comments or feedback. The second round of review is on the second draft of the guideline which already incorporates the feedback received or discusses certain feedback which may require further elaboration or input from the group members. The feedback needs to be evaluated to see whether it is acceptable or not. If it is not acceptable, a rationale needs to be stated as the reason for not accepting the feedback. For feedback that is not acceptable, members can appeal for the comment to be reviewed if it is likely to have an impact on the public interest. If there will be no impact, the focus group should reach a consensus to decide on the feedback received. The third round of review is on the third draft of the guideline which has incorporated all accepted feedback from the group members. If there is no more comment or feedback, this version of the guideline will be used for public review.

4.3 Endorsement Phase

The final phase involves a reviewing process by the public before the guideline is finalized.

4.3.1 Public review process

The public review process is important to ensure the content of the guideline is agreed upon and endorsed by the public. The target audiences from the public are generally from the public, private, and academic sectors. The public can give out their comments or feedback. The focus group should evaluate the feedback to see whether it is acceptable or not acceptable. A rationale needs to be stated for rejected feedback. Members can appeal for the comments to be reviewed again if it is going to damage the public interest. Typically, a public review will be conducted for three (3) months. Guidelines can be uploaded on a website for users to download the file or it can be attached in the email that is circulated to the public for the review process.

4.3.2 Finalize document

After all the feedback has been reviewed and agreed upon, the guideline should be finalized and circulated to the public. The finalized guideline should have versioning control to keep track of future changes to the guideline. The guideline can be hosted in a publicly accessed location, typically on a website to be obtained by the public.

5. Conclusions

In this paper, we present a framework used in developing a cloud security guideline. The framework enables us to take a formal and systematic approach towards producing a risk-based guideline that aligns with the recommended cloud security controls based on the respective ISO standards: ISO/IEC 27017:2015(E) and ISO/IEC 27036-4:2016. The outcome is a security framework modelled into three (3) main phases with seven (7) activities that detail the set of actions to follow in developing the guideline.

The guideline focuses on cloud security, covering three (3) stages of subscription (Pre, During, and Post) for the different deployment models: IaaS, PaaS, and SaaS. It aims to provide a quick guide to CSS in identifying the required or recommended cloud security controls from two interrelated dimensions, service delivery, and subscription stages. These dimensions add complexity to the mapping process, hence requiring a more structured framework to ensure all aspects of development are considered.

The framework may serve as a reference for organizations or agencies to develop similar guidelines for different service perspectives or different cloud models.

Acknowledgment

We would like to thank Universiti Malaysia Terengganu (UMT) and CyberSecurity Malaysia (CSM) for their support throughout the project.

References

[1] Mell, Peter, and Timothy Grance. "The NIST Definition of Cloud Computing (Draft)." *NIST Special Publication 800-145* (2011). https://doi.org/10.6028/NIST.SP.800-145

[2] Aggarwal, Gaurav. "How the Pandemic Has Accelerated Cloud Adoption." *Forbes Technology Council*. January 15, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/01/15/how-the-pandemic-has-accelerated-cloud-adoption/?sh=517678d66621.

[3] Alani, Mohammed M. "Securing the cloud: Threats, attacks and mitigation techniques." *Journal of Advanced Computer Science & Technology* 3, no. 2 (2014): 202. https://doi.org/10.14419/jacst.v3i2.3588

[4] Verma, Garima, and Sandhya Adhikari. "Cloud computing security issues: a stakeholder's perspective." *SN Computer Science* 1, no. 6 (2020): 329. https://doi.org/10.1007/s42979-020-00353-2

[5] Williams, Christina Meilee, Rahul Chaturvedi, and Krishnan Chakravarthy. "Cybersecurity risks in a pandemic." *Journal of Medical Internet Research* 22, no. 9 (2020): e23692. https://doi.org/10.2196/23692

[6] Tabrizchi, Hamed, and Marjan Kuchaki Rafsanjani. "A survey on security challenges in cloud computing: issues, threats, and solutions." *The Journal of Supercomputing* 76, no. 12 (2020): 9493-9532. https://doi.org/10.1007/s11227-020-03213-1

[7] Liao, Xiaojing, Sumayah Alrwais, Kan Yuan, Luyi Xing, XiaoFeng Wang, Shuang Hao, and Raheem Beyah. "Cloud repository as a malicious service: challenge, identification and implication." *Cybersecurity* 1 (2018): 1-18. https://doi.org/10.1186/s42400-018-0015-6

[8] Kumar, Rakesh, and Rinkaj Goyal. "On cloud security requirements, threats, vulnerabilities and countermeasures: A survey." *Computer Science Review* 33 (2019): 1-48. https://doi.org/10.1016/j.cosrev.2019.05.002

[9] Suárez, Javier Jerónimo, and Jorge López Hernández-Ardieta. "Enforcing cloud security controls." *No. 34: Cybersecurity Research. National Cybersecurity Research Conferences* (2021).

[10] Cloud Security Alliance. "Security Guidance for Critical Areas of Focus in Cloud Computing." *Cloud Security Alliance*, 2011. https://cloudsecurityalliance.org/research/guidance/.

[11] Alani, Mohammed M. "Prioritizing cloud security controls." In *Proceedings of the Second International Conference on Advanced Wireless Information, Data, and Communication Technologies*, pp. 1-6. 2017. https://doi.org/10.1145/3231830.3231831

[12] Myeonggil, Choi. "The Security Risks of Cloud Computing." In *2019 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 330-330. IEEE, 2019. https://doi.org/10.1109/CSE/EUC.2019.00069

[13] Alghofaili, Yara, Albatul Albattah, Noura Alrajeh, Murad A. Rassam, and Bander Ali Saleh Al-Rimy. "Secure cloud infrastructure: A survey on issues, current solutions, and open challenges." *Applied Sciences* 11, no. 19 (2021): 9005. https://doi.org/10.3390/app11199005

[14] Pericherla, Suryateja S. "Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art." *International Journal of Information Security (ISeCure)* 15, no. 1 (2023): 1-58.

[15] Díaz de León Guillén, Miguel Ángel, Víctor Morales-Rocha, and Luis Felipe Fernández Martínez. "A systematic review of security threats and countermeasures in SaaS." *Journal of Computer Security* 28, no. 6 (2020): 635-653. https://doi.org/10.3233/JCS-200002

[16] Shreyas, Sakharkar. "Security Model for Cloud Computing: Case Report of Organizational Vulnerability." *Journal of Information Security* 14, no. 4 (2023): 250-263. https://doi.org/10.4236/jis.2023.144015

[17] Mahmoud, Magdi S., and Yuanqing Xia. *Networked control systems: cloud control and secure control*. Butterworth-Heinemann, 2019. https://doi.org/10.1016/B978-0-12-816119-7.00012-5

[18] Xia, Yuanqing, Yuan Zhang, Li Dai, Yufeng Zhan, and Zehua Guo. "A brief survey on recent advances in cloud control systems." *IEEE Transactions on Circuits and Systems II: Express Briefs* 69, no. 7 (2022): 3108-3114. https://doi.org/10.1109/TCSII.2022.3178975

[19] Ministry of Communications and Multimedia Malaysia. "Cloud Security Implementation for Cloud Service Subscriber (CSS) Guideline." *CyberSecurity Malaysia*, 2019.

[20] Tunc, Cihan, Salim Hariri, Mheni Merzouki, Charif Mahmoudi, Frederic J. De Vaulx, Jaafar Chbili, Robert Bohn, and Abdella Battou. "Cloud security automation framework." In *2017 IEEE 2nd International Workshops on Foundations and Applications of Self* Systems (FAS* W)*, pp. 307-312. IEEE, 2017. https://doi.org/10.1109/FAS-W.2017.164

[21] Parast, Fatemeh Khoda, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, and Saqib Hakak. "Cloud computing security: A survey of service-based models." *Computers & Security* 114 (2022): 102580. https://doi.org/10.1016/j.cose.2021.102580

[22] Jawed, Md Saquib, and Mohammad Sajid. "A comprehensive survey on cloud computing: architecture, tools, technologies, and open issues." *International Journal of Cloud Applications and Computing (IJCAC)* 12, no. 1 (2022): 1-33. https://doi.org/10.4018/IJCAC.308277

[23] Li, Yuchong, and Qinghui Liu. "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments." *Energy Reports* 7 (2021): 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

[24] Hong, Jin B., Armstrong Nhlabatsi, Dong Seong Kim, Alaa Hussein, Noora Fetais, and Khaled M. Khan. "Systematic identification of threats in the cloud: A survey." *Computer Networks* 150 (2019): 46-69. https://doi.org/10.1016/j.comnet.2018.12.009

[25] Parast, Fatemeh Khoda, Chandni Sindhav, Seema Nikam, Hadiseh Izadi Yekta, Kenneth B. Kent, and Saqib Hakak. "Cloud computing security: A survey of service-based models." *Computers & Security* 114 (2022): 102580. https://doi.org/10.1016/j.cose.2021.102580

[26] Iosif, Andrei-Cristian, Tiago Espinha Gasiba, Tiange Zhao, Ulrike Lechner, and Maria Pinto-Albuquerque. "A large-scale study on the security vulnerabilities of cloud deployments." In *International Conference on Ubiquitous Security*, pp. 171-188. Singapore: Springer Singapore, 2021. https://doi.org/10.1007/978-981-19-0468-4_13

[27] Popović, Krešimir, and Željko Hocenski. "Cloud computing security issues and challenges." In *The 33rd International Convention MIPRO*, pp. 344-349. IEEE, 2010.

[28] Ramgovind, Sumant, Mariki M. Eloff, and Elme Smith. "The management of security in cloud computing." In *2010 Information Security for South Africa*, pp. 1-7. IEEE, 2010. https://doi.org/10.1109/ISSA.2010.5588290

[29] Almorsy, Mohemed, John Grundy, and Amani S. Ibrahim. "Collaboration-based cloud computing security management framework." In *2011 IEEE 4th International Conference on Cloud Computing*, pp. 364-371. IEEE, 2011. https://doi.org/10.1109/CLOUD.2011.9

[30] Gagliardi, Anna R., Melissa C. Brouwers, Valerie A. Palda, Louise Lemieux-Charles, and Jeremy M. Grimshaw. "How can we improve guideline use? A conceptual framework of implementability." *Implementation Science* 6 (2011): 1-11. https://doi.org/10.1186/1748-5908-6-26

[31] Youssef, Ahmed E., and Manal Alageel. "A framework for secure cloud computing." *International Journal of Computer Science Issues (IJCSI)* 9, no. 4 (2012): 487-500.

[32] Alenezi, Ahmed, Hany F. Atlam, and Gary B. Wills. "Experts reviews of a cloud forensic readiness framework for organizations." *Journal of Cloud Computing* 8 (2019): 1-14. https://doi.org/10.1186/s13677-019-0133-z

[33] Rupra, Satwinder Singh, and Amos Omamo. "A cloud computing security assessment framework for small and medium enterprises." *Journal of Information Security* 11, no. 4 (2020): 201-224. https://doi.org/10.4236/jis.2020.114014

[34] Tissir, Najat, Said El Kafhali, and Noureddine Aboutabit. "Cybersecurity management in cloud computing: semantic literature review and conceptual framework proposal." *Journal of Reliable Intelligent Environments* 7, no. 2 (2021): 69-84. https://doi.org/10.1007/s40860-020-00115-0

[35] International Organization for Standardization. *Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services, ISO/IEC 27036-4:2016(en)*. ISO, 2016.

[36] International Organization for Standardization/International Electrotechnical Commission. *Information technology-Security Techniques-Code of practice for information security controls based on ISO/IEC 27002 for cloud services (ISO, Geneva, Switzerland), ISO/IEC 27017: 2015*. ISO, 2015.