e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:10/October-2023 Impact Factor- 7.868 www.irjmets.com

STRATEGIZING CLOUD SECURITY: A COMPARATIVE ANALYSIS OF VENDOR AND NON-VENDOR CLOUD SECURITY MATURITY MODELS (CSMM) AMIDST THE SHARED RESPONSIBILITY PARADIGM AND ITS PRACTICAL IMPLEMENTATION

Amir Schreiber*[2], Ilan Schreiber*[2]

*[1]Doctor & Senior Faculty Member, Department Of Computer Science, Ashkelon Academic College (ACC), Ashkelon, Israel.

*[2]Senior Manager, Head Of Department, Cyber Risk Management Dep., BNHP (The Largest Bank In Israel), Tel-Aviv, Israel.

*Corresponding Author: Amir Schreiber

DOI : https://www.doi.org/10.56726/IRJMETS45402

ABSTRACT

In today's digital age with cloud computing at its forefront, the importance of robust security frameworks, especially the Shared Responsibility Model (SRM) in cloud security, is increasingly recognized. Literature has focused on technical and legal aspects of SRM deployment leaving its strategic integration through Cloud Security Maturity Model (CSMM) underexplored. This research meticulously explores the escalating necessity for employing a CSMM amidst organizations, strategically integrating the deployment of a SRM during their cloud adoption journey. It delves into the nuances of two primary CSMMs: the vendor-specific "AWS Security Maturity Model" and the vendor-neutral "CSA Cloud Security Maturity Model". A detailed comparative analysis reveals the intricacies, benefits, and challenges inherent in each model, offering practical insights for diverse organizational security needs. By blending theoretical and pragmatical perspectives, this study provides actionable recommendations for organizations to customize their cloud security approach. The manifesto not only augments scholarly discussions on cloud security maturity but also equips organizations with a strategic blueprint for tailoring their cloud security initiatives in an ever-evolving digital landscape.

Keywords: Cyber Security, Maturity Model, AWS, CSA.

I. INTRODUCTION

2.1 Relevance of Cloud Computing

In the pulsating heart of today’s digital transformation, cloud computing has emerged as a key component, empowering organizations with an unprecedented ability to orchestrate scalable, flexible, and financially savvy computational capabilities (Jamsa 2022; Mukherjee, 2019). The steady march toward cloud-based solutions, catalyzed by their ability to ingeniously facilitate unencumbered data storage, access, and management, has embedded cloud architectures deeply within organizational operations. This triggers a critical exploration into safeguarding these digital frameworks, making the secure operation of cloud environments a paramount concern in contemporary discussions about data management and cybersecurity (Bharany et al., 2022).

2.2 Shared Responsibility and Security Challenge

The Shared Responsibility Model in cloud computing articulates a complex interplay between cloud service providers and users in sustaining the security and compliance of cloud data and applications. IaaS - Infrastructure as a Service, PaaS - Platform as a Service, and SaaS - Software as a Service (Mohammed & Zeebaree, 2021) represent three well-known service-oriented cloud models, gaining popularity among medium to large businesses due to their cost efficiency, availability, and scalability (IBM Cloud Education, 2021; Chauhan, A., 2023). A Cloud Landing Zone refers to a securely designed and automated environment in the cloud where infrastructure can be set up to host applications and workloads for users (Mastrota, 2022).

However, within this synergy lie myriad challenges and complexities that organizations navigate, often teetering between ensuring operational efficacy and solidifying their security postures and different configurations (Bennett et al., 2019; Rutuja, 2022).

This engenders various quandaries and opportunities for breach within cloud security, marking a significant area that demands meticulous attention and exploration within both academic and practical spheres to safeguard data and functionalities in the cloud.

2.3 Cloud Security Maturity Models

Among the layered complexities and potential vulnerabilities in cloud environments, Cloud Security Maturity Models (CSMM) have surfaced as pivotal guides to assist organizations in systematically enhancing their cloud security protocols (Möller, 2023). These models, ranging from vendor-specific exemplars such as the AWS Security Maturity Model to non-vendor alternatives like the CSA Cloud Security Maturity Model, proffer structured frameworks that aim to fortify cloud security through strategic and practical implementations Akinsanya, O. O., (Papadaki & Sun, 2019; Pereira et al., 2022). The variances and particularities within these models cultivate a rich ground for exploration and comparative analysis, aiming to discern their respective efficacies and limitations.

2.4 Rationale and Scope of the Research

This research endeavors to plunge into the intricate web of CSMM, seeking to unravel the distinctive characteristics, and potential caveats embedded within vendor and non-vendor models through a robust comparative analysis. The objective intertwines with the ambition to not only decode the complexities and potentials inherent within each model but also to weave a comprehensive understanding regarding their practical implementations and alignments with diverse organizational security mandates. The study aspires to bolster the academic and pragmatic dialogue on cloud security maturity, furnishing organizations with enriched insights and guiding lights to navigate their cloud security orchestration with informed and substantiated methodologies.

II. LITRETURE REVIEW

2.1 Two Major Model Types – AWS Vs. CSA

Navigating through the diverse labyrinth of CSMMs reveals a spectrum where two models, AWS, and CSA, have prominently emerged, each encapsulating unique methodologies, criteria, and frameworks in addressing cloud security concerns. The literature unfurls a cascade of findings regarding the AWS Security Maturity Model (Pereira et al., 2022) and the cloud transformation (Pakkala, 2022), predominantly reflecting its deeply intertwined nature with the vendor’s own cloud offerings (Ashok, 2023), embodying a model that provides a pathway that is at once sophisticated yet veiled with intrinsic AWS-centric perspectives.

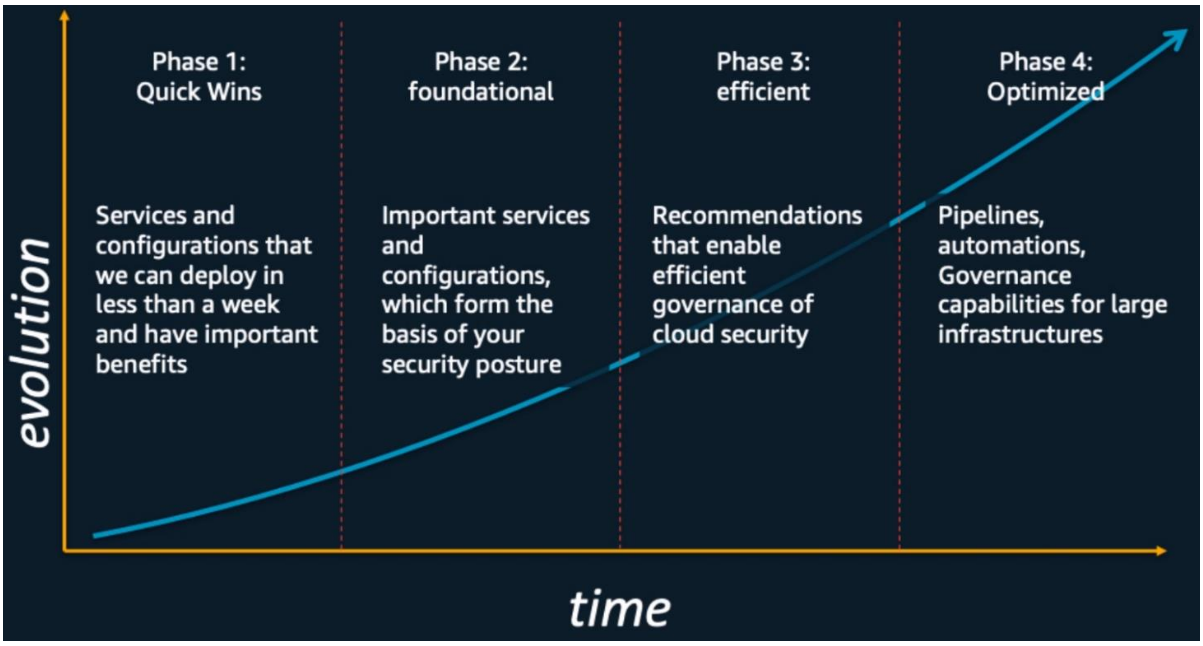
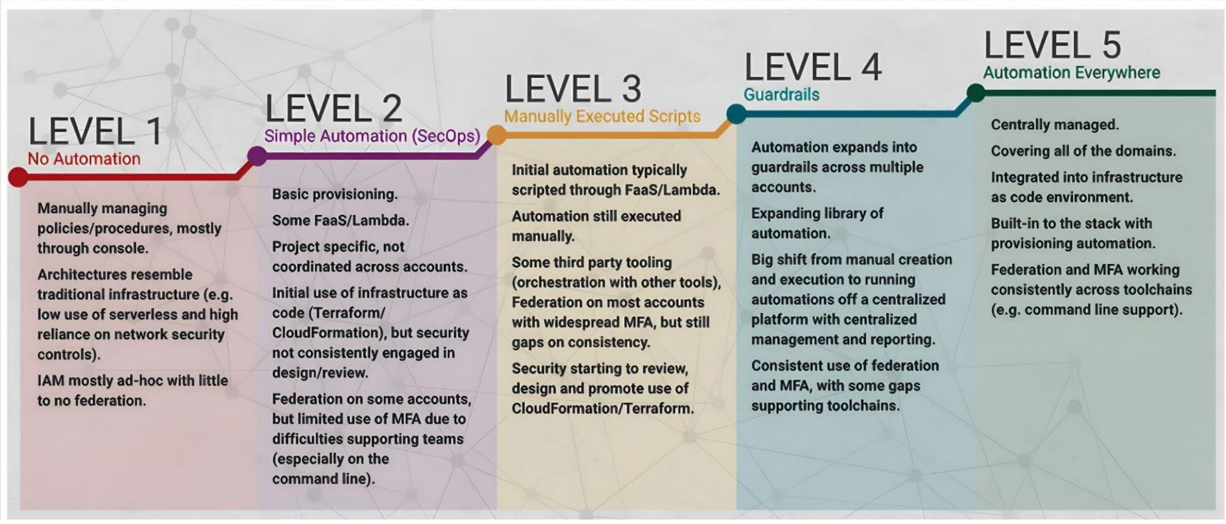

Phase 1:
Quick Wins
Phase 2:
foundational
Phase 3:
efficient
Phase 4:
Optimized
Services and configurations that we can deploy in less than a week and have important benefits
Important services and configurations, which form the basis of your security posture
Recommendations that enable efficient governance of cloud security
Pipelines, automations, Governance capabilities for large infrastructures
evolution
time

Figure 1 - AWS Security Maturity Model

Consequently, this model propounds strategies, practices, and protocols that are inherently streamlined towards AWS environments, offering a rich yet potentially biased viewpoint on cloud security maturation. The model includes 4 phases: Quick wins, Foundational, Efficient, Optimized (see Figure 1 for AWS original diagram) across 9 robust categories: Security governance, Security assurance, Identity and access management, Threat detection, Vulnerability management, Infrastructure detection, Data protection, Application security, Incident response. Each category incorporates a group of questions graded 0%, 25%, 50%, 75%, 100% for implementation. Additionally, there is guidance for propriety AWS security tools which are incorporated into AWS platform (Abhijit & Shailesh, 2022).

On the other hand, the CSA Cloud Security Maturity Model propounds a vendor-agnostic stance, emanating from the Cloud Security Alliance's collective expertise and multidisciplinary insights. The literature reveals that CSA offers a holistic, overarching framework designed to be versatile and adaptable across various cloud environments, eschewing the specificities and potential biases that might be enmeshed within vendor-specific models (CSA publication, 2022). Notwithstanding its universal applicability, critiques within existing studies point towards its potential lack of depth or specificity in certain cloud contexts, given its broad and generalized approach. Moreover, although CSA published a Cloud Control Matrik (CCM), a cybersecurity control framework for cloud computing, their online assessment tool for utilizing the maturity model is not aligned with CCM 16 domains, nor has links for its content. The model includes 5 maturity phases: No automation, Simple automation, Manually executed scripts, Guardrails, Automation everywhere (See Figure 2 for CSA original diagram), across 12 categories: Security governance, Security assurance, Identity and access management, Threat detection, Vulnerability management, Infrastructure detection, Data protection, Application security, Incident response. Each category incorporates a group of questions graded 1 to 10 (10 is maximum) for implementation.



LEVEL 1
No Automation

Manually managing policies/procedures, mostly through console.

Architectures resemble traditional infrastructure (e.g. low use of serverless and high reliance on network security controls).

IAM mostly ad-hoc with little to no federation.

LEVEL 2
Simple Automation (SecOps)

Basic provisioning.

Some FaaS/Lambda.

Project specific, not coordinated across accounts.

Initial use of infrastructure as code (Terraform/ CloudFormation), but security not consistently engaged in design/review.

Federation on some accounts, but limited use of MFA due to difficulties supporting teams (especially on the command line).

LEVEL 3
Manually Executed Scripts

Initial automation typically scripted through FaaS/Lambda.

Automation still executed manually.

Some third party tooling (orchestration with other tools), Federation on most accounts with widespread MFA, but still gaps on consistency.

Security starting to review, design and promote use of CloudFormation/Terraform.

LEVEL 4
Guardrails

Automation expands into guardrails across multiple accounts.

Expanding library of automation.

Big shift from manual creation and execution to running automations off a centralized platform with centralized management and reporting.

Consistent use of federation and MFA, with some gaps supporting toolchains.

LEVEL 5
Automation Everywhere

Centrally managed.

Covering all of the domains.

Integrated into infrastructure as code environment.

Built-in to the stack with provisioning automation.

Federation and MFA working consistently across toolchains (e.g. command line support).

Figure 2 - CSA Cloud Security Maturity Model

Both models, while commendable in their structure and approach, evoke certain gaps and unaddressed dimensions in existing research, notably regarding their comparative efficacy, implementational nuances, and adaptability across varied organizational contexts and requirements. The foundational elements of each model, from their respective assessment criteria, strategic implementations to risk management protocols, despite being well-documented, are often explored in isolated contexts, lacking a thorough, side-by-side analytical exploration.

2.2 The Need for Understanding the Two Types

The divergence, as well as the confluence of principles and practices within AWS and CSA models, beckon a nuanced understanding and comparison, precipitating a tangible need to dissect, contrast, and contextualize them both theoretically and practically. From a practical lens, organizations stand on the precipice of choice when it comes to orchestrating their cloud security frameworks. The decision to adhere to a vendor-specific or a vendor-neutral model intrinsically shapes their security strategies, risk management, and compliance protocols, thereby directly impacting their operational efficacy and security robustness in the cloud.

Theoretically, the comparative analysis between the models unveils a fertile ground for academic inquiry, bridging the identified gaps within existing literature, especially concerning their applicability, scalability, and efficacy within diverse organizational contexts. Thus, our research seeks to intertwine practical imperatives with theoretical explorations, aiming to furnish a detailed, comparative insight into AWS and CSA models, thereby illuminating the path for organizations in strategizing their cloud security frameworks, and contributing to the academic discourse with a nuanced. This study ultimately aspires to guide organizations and researchers alike in understanding, selecting, and implementing a CSMM that resonates cohesively with specific needs, objectives, and cloud environments.

III. METHODOLOGY

3.1 Comparative Analysis Methodology

The nucleus of this research pivots around a scrupulous comparative analysis of two eminent models, namely, the AWS Security Maturity Model and the CSA Cloud Security Maturity Model. The methodology espoused here, intends to sieve through each model's intrinsic qualities, frameworks, and assessment criteria while illuminating their distinctive and overlapping characteristics. Initially, a comprehensive literature review establishes a foundational understanding, ensuring a robust theoretical framework encapsulates the subsequent practical analysis.

We employ a dual-phase analysis: the first phase is immersive, where each model is dissected independently to draw out its foundational principles, methodologies, and assessment criteria, facilitating an intrinsic understanding of their operational paradigms.

The second phase endeavors to juxtapose these independently drawn insights, crafting a side-by-side analysis that elucidates similarities, divergences, strengths, and potential limitations inherent within each model. This juxtaposition is meticulously framed to ensure a balanced, unbiased comparative lens, facilitating a coherent and equitable evaluation and comparison.

3.2 Comparative Analysis Methodology

To distill a substantive comparison and evaluation, specific criteria have been meticulously selected, ensuring a multi-faceted analysis that resonates with both theoretical and practical dimensions of cloud security maturity. The following criteria forge the analytical lens through which the models will be evaluated:

- ❖ **Applicability**: Exploring how each model aligns with varied organizational structures, sizes, and industries, evaluating their versatility and relevance across different cloud environments and organizational needs.
- ❖ **Complexity**: Analyzing the intricacy of each model, deciphering whether their frameworks, guidelines, and protocols are straightforward or convoluted, and how this complexity may impact their implementation and management.
- ❖ **User-Friendliness**: Understanding the ease of adaptation and management from a user perspective, exploring how intuitively organizations can navigate, implement, and uphold the models in their practical environments.
- ❖ **Adaptability**: Investigating the models' capability to be tailored and scaled according to the evolving needs, structures, and objectives of organizations, ensuring that they can remain relevant and efficacious amidst organizational and technological changes.
- ❖ **Compliance and Risk Management**: Scrutinizing how each model addresses, manages, and mitigates compliance and risk within cloud environments, exploring their protocols, guidelines, and strategies in safeguarding organizational data and functionalities.
- ❖ **Cost Implications**: Delving into the financial aspects involved in adopting, implementing, and maintaining each model, exploring the direct and indirect costs, and evaluating whether they proffer a cost-effective strategy in bolstering cloud security maturity.

Each criterion is elaborated through both a theoretical and practical lens, ensuring the analysis is substantiated with relevant literature, case studies, and practical insights, thereby crafting a comprehensive, multi-dimensional exploration into the AWS and CSA models.

IV. ANALYSIS AND DISCUSSION

4.1 Comparison Overview

In the comparative overview, the detailed table expounds the key characteristics of the AWS and CSA models according to the predefined criteria (see Table 1). The contrasting facets of these models are visibly distilled in the tabulated form in Table 1, offering readers a structured perspective into their intrinsic and extrinsic properties. For instance, while AWS demonstrates robust compliance and risk management protocols, particularly within AWS ecosystems, the CSA model's more generalized framework enhances its adaptability across diverse cloud environments.

Table 1 – Comparative Table: AWS vs. CSA Cloud Security Maturity

Criteria	AWS Security Maturity Model	CSA Cloud Security Maturity Model
Applicability	Broad applicability across diverse industries due to its scalable and comprehensive nature. Amazon AWS leading the market with 30% cloud is 32% of its share (Haranas, 2023). Tightly integrated with AWS cloud services, making it somewhat limited to AWS environments.	Widespread applicability given its non-vendor specificity, allowing it to be utilized across various cloud environments. May require more customization in vendor-specific environments. The in no gudance for vendor specific tools or implementation.
Complexity	Highly detailed, offering extensive guidance which might be perceived as complex. Its integration with AWS services can simplify usage for AWS users.	Offers a more generalized framework, which can be easier to digest at first glance. May introduce complexity when adapting to specific vendor environments.
User-Friendliness	Facilitates user interaction by embedding into the AWS ecosystem, but may present a learning curve due to its detail.	Straightforward for users familiar with cloud security, but may need additional specific guidelines for practical application.
Adaptability	Highly adaptable within AWS environments but may lack flexibility outside the AWS ecosystem. Include recomndations for the implementation of AWS security services (e.g: IAM, Guard duty. Cloud trail, etc).	Highly adaptable across various cloud environments and vendors due to its generalized approach. useful for environments with multi- cloud vendors.
Compliance and Risk Management	Strong compliance and risk management protocols, enhanced by AWS's inherent security tools and services.	Provides a strong compliance framework but may require additional tools and services to implement robust risk management in specific cloud environments.
Cost Implications	Tends to be cost-efficient for AWS users due to its seamless integration with AWS services and pricing models. May incur additional costs for extensive adaptation in non-AWS environments.	Potentially higher initial setup costs due to potential need for additional tools/services. Offers flexibility which might enable organizations to control ongoing costs effectively in multi-vendor environments.

4.2 Detailed Insights

Diving into the detailed insights, this comparative table becomes a springboard for in-depth analysis. The evident divergences, such as the AWS model's complexity contrasted with its user-friendly nature within the AWS ecosystem, or the CSA model's adaptable yet potentially complex implementation across various vendor environments, highlight the need for organizations to meticulously assess and align their unique needs, contexts, and objectives with their chosen model. An overview of the proposed implementation path for an organization is described in the following flowchart (see Figure 3).

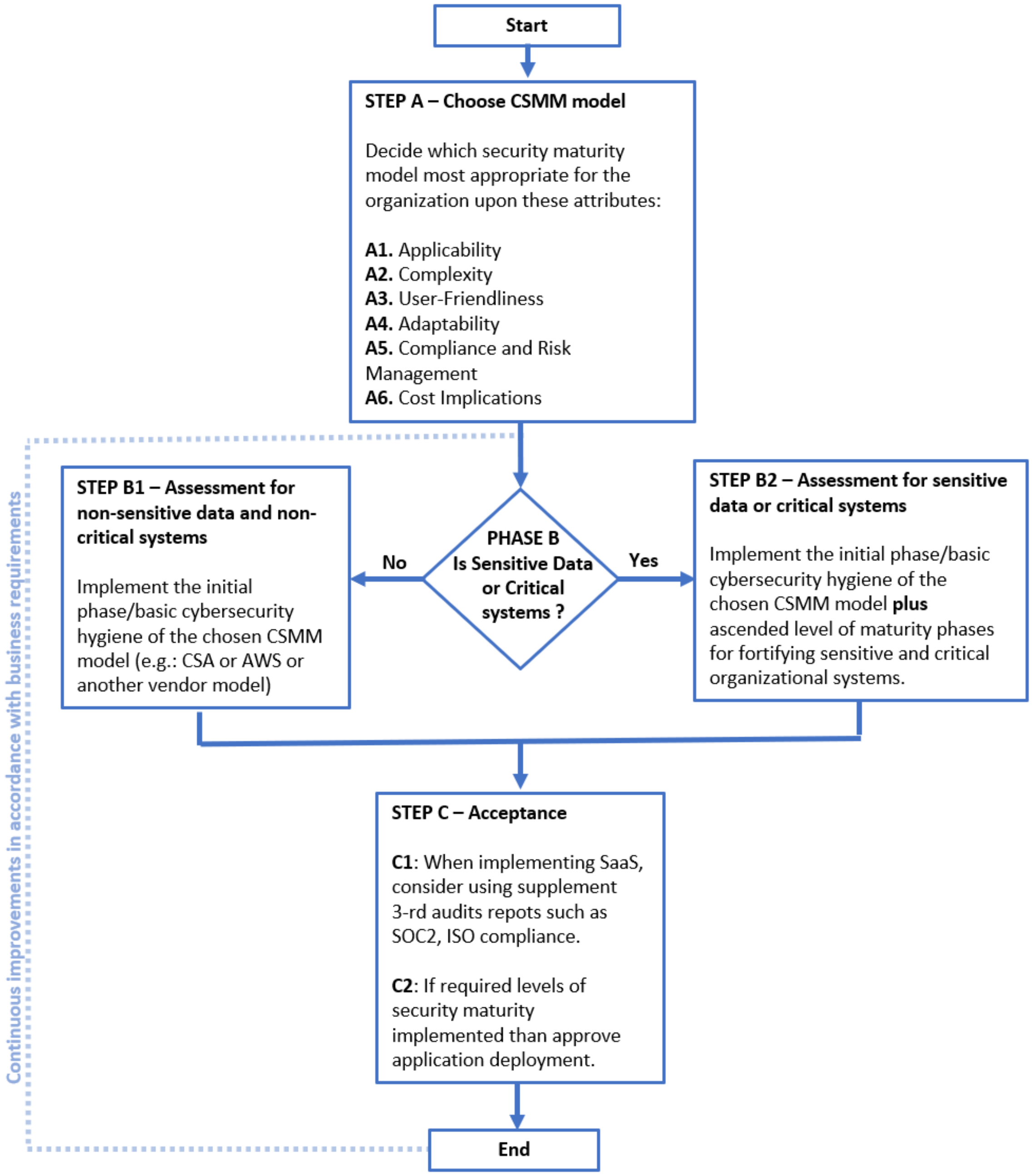

Start
STEP A – Choose CSMM model
Decide which security maturity model most appropriate for the organization upon these attributes:
A1. Applicability
A2. Complexity
A3. User-Friendliness
A4. Adaptability
A5. Compliance and Risk Management
A6. Cost Implications
Continuous improvements in accordance with business requirements
STEP B1 – Assessment for non-sensitive data and non-critical systems
Implement the initial phase/basic cybersecurity hygiene of the chosen CSMM model (e.g.: CSA or AWS or another vendor model)
No
PHASE B
Is Sensitive Data or Critical systems ?
Yes
STEP B2 – Assessment for sensitive data or critical systems
Implement the initial phase/basic cybersecurity hygiene of the chosen CSMM model plus ascended level of maturity phases for fortifying sensitive and critical organizational systems.
STEP C – Acceptance
C1: When implementing SaaS, consider using supplement 3-rd audits repots such as SOC2, ISO compliance.
C2: If required levels of security maturity implemented than approve application deployment.
End

Figure 3 – CSMM implementation flowchart

This proposed implementation path for an organization will include these adaptive A to C steps:

❖ **Step A:** The organization will prudently choose a CSMM that aligns closely with its distinct needs, carefully weighing whether to adhere to or deviate from a vendor-agnostic approach, ensuring harmony with the organization's landing zone on its cloud platforms. The decision will hinge upon six criteria (A1-A6). For an organizational landing zone with or aim to multiple cloud vendor platforms (e.g.: mixed landing zone of AWS, Azure, GCP), the focus will undeniably shift towards a maturity model that isn't tied to a specific vendor but can navigate through all the available solutions.

❖ **Step B:** A comprehensive assessment of the cloud environment implementation will be undertaken by the organization. This entails striving for foundational cybersecurity hygiene, adhering to the initial maturity phases of the chosen CSMM for systems that are deemed non-sensitive and non-critical (flow to B1), while ensuring an ascended level of maturity phases for fortifying sensitive and critical organizational systems (flow to B2). An organization may strategically channel defense resources towards specific domains within the model, particularly those demanding a superior level of maturity to safeguard sensitive and critical systems, encompassing areas like information protection, infrastructure safeguarding, identity management, and incident response. Alternatively, it may segment its investment into phases; for instance, during the initial phase, they might focus on establishing the landing zone for non-sensitive systems, while concurrently progressing the model and preparing for advanced maturity levels for crucial and sensitive systems.

❖ **Step C:** Subsequent to the aforementioned steps, a decision will be rendered regarding the approval of the cloud environment, contingent upon the attainment of compliance with the criteria, as determined and scrutinized in the second stage (C1). It is imperative to note that, particularly for Software as a Service (SaaS) applications, complete data might not be readily available from the vendor. Consequently, there may arise circumstances necessitating the incorporation of additional, supplementary third-party security reports, such as SCO2 and ISO, to ascertain the degree of maturity (C2).

The process involves continuous improvement of cybersecurity while adjusting maturity targets according to the business requirements and the dynamic environment of the organization. For example, if the organization merged or acquired a subsidiary involved in sensitive information, it should set new objectives according to path B2 and aim for a corresponding maturity level of cybersecurity.

4.3 Practical and Theoretical Implications

Exploring the practical and theoretical implications, the comparative findings, such as the cost implications and adaptability of each model, forge a rich discourse that intertwines practical organizational strategies with academic discussions on cloud security maturity. The comparison seeds potential pathways for further research, exploring the depths of each model's applicability, complexity, and practicality within varied and evolving cloud environments.

V. CONCLUSION

5.1 Summative Insights

A labyrinthine journey through the realms of AWS and CSA Cloud Security Maturity Models has unveiled a tapestry of insights, each model embedding its own set of strengths and weaknesses, providing distinct navigational paths through the cloud security landscape. The AWS model, with its tight-knit integration with the AWS ecosystem, brings forth a dexterous, albeit complex, framework that harmonizes seamlessly with AWS environments, offering robust compliance and risk management but with potential constraints in non-AWS platforms. Contrarily, the CSA model, emblematic of a more generalized approach, fosters widespread applicability and adaptability across varied cloud environments but may meander into complexities when steering through vendor-specific terrains, necessitating nuanced customization and potentially incurring divergent cost structures.

5.2 Summative Insights Recommendations and Applicability

Navigating through the cascading waterfall of findings, structured recommendations surface from the analytical depths. Organizations embedded within the AWS ecosystem, seeking a comprehensive, albeit intricate, security framework, might gravitate towards the AWS Security Maturity Model, capitalizing on its integration, compliance protocols, and potentially streamlined cost structures within AWS environments. Conversely, entities operating across multifaceted cloud environments, or those desiring a more vendor-neutral approach, might find solace in the CSA model, leveraging its adaptability but must remain cognizant of potential complexities in practical implementations and manage initial setup and ongoing costs judiciously. The decision matrix invariably intertwines with organizational needs, technical expertise, vendor relationships, and strategic objectives, thereby necessitating a meticulous alignment of model characteristics with organizational contexts.

5.3 Future Work

Peering into the future, several research avenues unfurl, inviting deeper exploration and diversification of the discourse surrounding CSMMs. A potential trajectory could encompass a granular examination of model implementations within specific industry contexts, dissecting the nuanced challenges, successes, and learnings embedded within each journey. Another avenue might traverse through the landscapes of small and medium enterprises (SMEs), exploring how their unique challenges, resource constraints, and objectives shape, and are shaped by, their chosen models. Additionally, exploring alternative models or developing hybrid approaches that merge the strengths of existing models might forge new pathways, thereby enhancing the strategic and tactical toolkits available to organizations navigating through their cloud security maturity journey.

VI. REFERENCES

[1] Abhijit, M. & Shailesh, B. (2022). CLOUD SECURITY WITH AWS. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS).
DOI : https://www.doi.org/10.56726/IRJMETS30997

[2] Akinsanya, O. O., Papadaki, M., & Sun, L. (2019, January). Current cybersecurity maturity models: How effective in healthcare cloud?

[3] Ashok, D. S (2023). A REVIEW ON AWS - CLOUD COMPUTING TECHNOLOGY. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS).
DOI: https://www.doi.org/10.56726/IRJMETS42351

[4] Bharany, S., Sharma, S., Khalaf, O. I., Abdulsahib, G. M., Al Humaimeedy, A. S., Aldhyani, T. H., ... & Alkahtani, H. (2022). A systematic survey on energy-efficient techniques in sustainable cloud computing. Sustainability, 14(10), 6256.

[5] Bennett, K. W., & Robertson, J. (2019, May). Security in the Cloud: understanding your responsibility. In Cyber Sensing 2019 (Vol. 11011, p. 1101106). SPIE.

[6] Chauhan, A. (2023). CLOUD COMPUTING SERVICES AND SECURITY. International research journal of modernization in engineering technology and science (IRJMETS).
DOI: https://www.doi.org/10.56726/IRJMETS42729

[7] CSA (2022). Four Ways to Use the Cloud Security Maturity Model. [Online] Jamsa, K. (2022). Cloud computing. Jones & Bartlett Learning.

[8] Haranas, M. (2023). AWS, Microsoft, Google's Cloud Market Share Q1 2023, CRN publication. [Online] https://www.crn.com/news/cloud/aws-microsoft-google-s-cloud-market-share-q1-2023/4

[9] IBM Cloud Education (2021). "Iaas vs. paas vs. saas, understand and compare the three most popular cloud computing service models,". [Online] https://www.ibm.com/cloud/learn/iaas-paas-saas

[10] Mastrota, M. (2022). Enterprise scale cloud landing zone to design, provision, operate, manage and dispose a multi-account AWS Cloud environment (Doctoral dissertation, Politecnico di Torino).

[11] Mohammed, C. M., & Zeebaree, S. R. (2021). Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. International Journal of Science and Business, 5(2), 17-30.

[12] Mohite, M. R. CLOUD SECURITY PROBLEMS AND SOLUTIONS. International Research Journal of Modernization in Engineering Technology and Science (IRJMETS).
DOI: https://www.doi.org/10.56726/IRJMETS30200

[13] Möller, D. P. (2023). Cybersecurity Maturity Models and SWOT Analysis. In Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices (pp. 305-346). Cham: Springer Nature Switzerland.

[14] Mukherjee, S. (2019). Benefits of AWS in modern cloud. arXiv preprint arXiv:1903.03219.

[15] Pakkala, L. (2022). Measuring Capability for Cloud Infrastructure Adoption in Software Production for Finnish Non-profit Organisations. https://cloudsecurityalliance.org/blog/2022/04/22/four-ways-to-use-the-cloud-security-maturity-model/

[16] Pereira, C. D. C., Costa Filho, C. A., & Ferraz, F. S. (2022). Cloud Maturity Framework. ICSEA 2022, 63.