A Multi-Criteria Evaluation of Cloud Security Posture Management Aligned with Users' Security Requirements

Lamia Alsakkaf
IU International University of Applied Science
Erfurt, Thüringen, Germany
lamia.alsakkaf@iu.org

Ahmed Taha
IU International University of Applied Science
Erfurt, Thüringen, Germany
ahmed.taha@iu.org

Jörn-Marc Schmidt
IU International University of Applied Science
Erfurt, Thüringen, Germany
joern-marc.schmidt@iu.org

***Abstract*— As organizations increasingly adopt cloud technologies, security remains a major concern. Hence, effective cloud security solutions, such as Cloud Security Posture Management (CSPM), are vital. Selecting an optimal CSPM is a challenge for organizations, since every organization has specific security requirements. In order to address this gap, this study proposes a Multi Criteria Decision Making (MCDM)-based method assisting organizations in selecting the best CSPM solution in alignment with their requirements. The proposed evaluation approach is based on the PROMOTHEE II outranking technique, considering both qualitative and quantitative attributes. The method guides organizations through a step-by-step process, starting from identifying their specific security requirements and ending with the selection of an optimal CSPM solution. This assessment framework enables organizations to confidently differentiate between CSPM solutions that equally satisfy their needs and those that over-provision, ensuring optimal resource allocation and security posture.**

Keywords*— *Cloud Security Posture Management (CSPM), Multi Criteria Decision Making (MCDM), Organization's Requirements.

I. Introduction

Cloud technologies provide numerous benefits, including flexible deployment and good scalability, paired with usage-based cost metrics. When migrating to cloud environments or designing cloud-based applications, trust and data-security are crucial [1],[2]. The responsibility, especially when it comes to security, is shared between the cloud provider and the customer, called the shared responsibility model. While a baseline security is ensured by the cloud provides, the customer is responsible for various configurations, like managing users and their access to data and services. Managing the various configurations while maintaining security and ensure compliance with regulatory requirements can be challenging [3]. In fact, almost all data breaches are a result of misconfigurations and human mistakes [4]. Cloud Security Posture Management (CSPM) solutions are a response to these challenges. Their objective is reducing misconfigurations and demonstrating compliance with industry standards [4].

Since every organization has its own security requirements and constraints, selecting a CSPM tool from the wide range of tools offered in the market can be challenging. Therefore, practitioners need to identify their requirements and select a suitable CSPM tool based on those requirement. Furthermore, CSPM providers want to learn about their clients' needs to shape future roadmaps and marketing decisions.

This study presents an evaluation framework to address both needs. The suggested framework provides:

- A method to identify an organization's specific requirements.
- An adaptable assessment technique to select the best CSPM according to the organization's requirements.
- A usability demonstration using real-world data from the Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) repository [5].

The paper is organized as follows. Section II outlines the related work. Section III describes the evaluation framework and Section IV shows its application in a case study using a sensitivity analysis. Conclusion are drawn in Section V.

II. Related Work

Karim, Ding, and Chi [6] proposed an approach that adds ranked user-specific requirements to the evaluation process. It relies on the application of the PROMOTHEE II method to rank the evaluated web services. While this framework only considered quantitative attributes, expanding it into quantifying qualitative attributes would increase the model's applicability.

Luna, Langenberg, and Suri [7] suggested a framework called Quantitative Policy Trees (QPT) to quantitatively benchmark Security Service Level Agreements (SecSLA). This framework is based on the Reference Evaluation Methodology (REM), but it imposed constraints on how requirements could be specified. This limits the user's ability to define requirements at higher levels of the criteria hierarchy.

To address the limitations of the QPT method, Taha, Luna, and Suri [8] provided an assessment framework built upon one of the common Multi Criteria Decision Making (MCDM) method, the Analytic Hierarchy Process (AHP). It enables users to define their requirements across multiple hierarchy levels while taking their varying levels of expertise into account. This results in quantitative security level values for CSPs based on user-defined security requirements. Both studies conducted an empirical validation based on CSP's data stored in the STAR repository.

However, the AHP method relies on matrix operations and eigenvector calculations. This may impose significant processing demands as the number of evaluated alternatives increase [9]. To improve efficiency, Modic et al. [9] introduced a simplified version of the framework proposed by [8], along with a method called Moving Intervals Process (MIP) to evaluate CSPs according to the user's requirements.

The MIP method offers a separation between providers that align exactly with the user's requirements and ones that over-provision them.

In [10], the authors suggested a method to handle the user's inconsistent requirements identification between services. This helps customers specify clear security requirements, while considering interdependencies between different services. Thereby, the approach enables users to determine which CSPs satisfy their consistent specified requirements.

Additionally, the study [11] addressed the uncertainty of users' opinions when defining their security requirements by developing a fuzzy AHP framework. It aims at evaluating the security levels of CSPs according to the user's subjective requirements. The method was validated using real-world data that leveraged the standardized Cloud Service Level Agreement structure proposed in the ISO/IEC 19086 standard.

More recently, an assessment of the CSPM tools provided by the three well-known cloud service providers—Amazon Web Services, Microsoft Azure, and Google Cloud Platform—was carried out by Boneder [12]. However, the evaluation method assumed that all of the evaluation criteria had the same weight. Moreover, it did not consider potential diversity of customer needs when only Boolean variable criteria are considered.

In summary, previous work relies on the knowledge of a single user to identify the organization's requirements. In practice, this strategy is not sufficient if the required expertise to address all evaluation criteria is spread across various users or even teams. This paper proposed a method that relies on the aggregated knowledge of multiple users based on the level of their expertise in different areas. It accommodates both qualitative and quantitative criteria. Additionally, the suggested method offers a comparatively simple computational mechanism based on PROMOTHEE II, whereas many existing approaches depend on more complex, matrix-based procedures, resulting in significant resource consumption as the number of evaluated alternatives grows.

III. CSPM Evaluation Methodology

This paper presents an evaluation method based on the MCDM approach which selects the best option from several alternatives considering multiple criteria [13]. In this study, the PROMOTHEE II outranking approach was utilized. To select the optimal choice, the knowledge of multiple experts in various fields builds the foundation of the requirements definition. This allows to take the organization's requirements together with sub-criteria during the assignment of criteria weights into account. Considering the organization's specific required performance related to sub-criteria, the optimal offered CSPM solution satisfying the organization requirements is selected.

The evaluation process, as depicted in Fig. 1, consists of two stages: Stage 1 identifies the organization's specific security requirements and Stage 2 includes utilizing the PROMOTHEE II outranking method to rank the CSPM tools based on the requirements that the organization identified in Stage 1.

The starting point for the evaluation is a template containing the selected evaluation attributes. It is filled by the CSPM vendors and the potential customers. The template was created based on the hierarchy structure shown in Fig. 2. It contains eleven sub-criteria selected from the CSA Consensus Assessment Initiative Questionnaire (CAIQ), grouped into five main criteria [5].

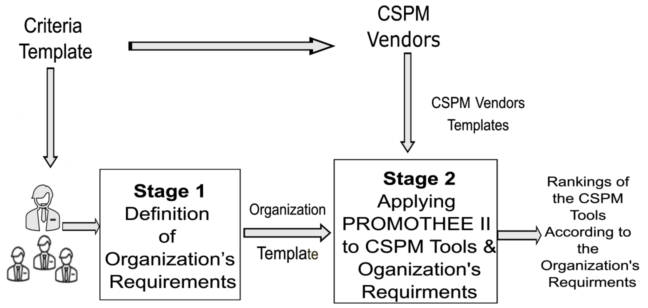

Fig. 1: Framework Stages.

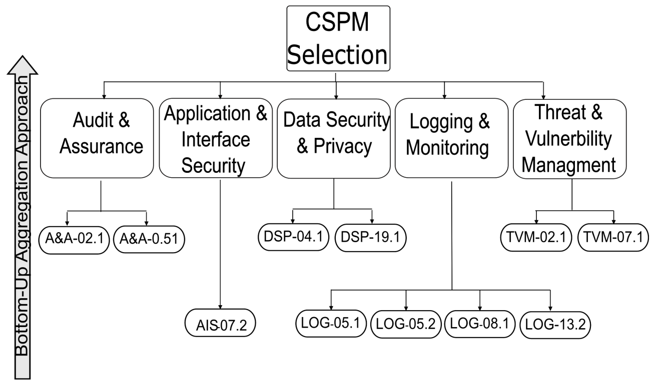

Fig. 2: Criteria Hierarchy.

A. Stage 1

Stage 1 identifies the organization's specific requirements. The processes include strategic goals, typically defined by a senior expert representing a high management level, and detailed technical requirements, commonly specified within sub-criteria by junior experts with different job roles and expertise. This approach ensures various different perspectives and special knowledge is included in the process. As seen in Fig. 3, there are several tasks completed at this point in the framework development process. Let A= $\{a_1, a_2, a_3, ..., a_{(n+m)}\}$ be the set of n CSPM vendors offerings expanded by m organization's requirements $(a_{(n+1)}, \dots, a_{(n+m)} = U)$. The set $M = m_1, m_2, m_3, \dots., m_q$ denotes the q main criteria. Junior experts are represented by $E = e_1, e_2, e_3, \dots \dots \dots \dots, e_r$; r is the number of junior experts.

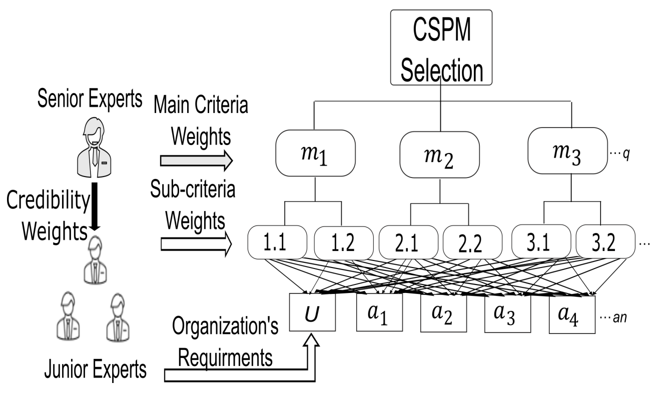

Fig. 3: Expert Engagement Role.

As first step in the process, the senior experts assigns weights to every junior expert, representing his/her impact on the selection process. This weight of a junior expert remains constant across all sub-criteria underneath a particular main criterion. However, the same junior expert may have different creditability when decision making is related to sub-criteria in another main criteria. Next, weights are assigned to each of the two levels of the hierarchy's criteria. The senior expert assigns weights to the main criteria, while junior experts assign weights to the sub-criteria. Lastly, for each sub-criteria seen in Fig. 2, every junior expert defines a specific performance requirement for the organization. The aggregated definition represents the final decision and fills up the same template filled by the CSPM vendors. A summary of the definitions of key terms is given in Table I.

TABLE I. DEFINITION OF KEY TERMS USED IN THE EVALUATION PROCESS

Term	Definition
L_m	Normalized weight of the main criteria *m*
$Cr_m^{e_j}$	Assigned weight by the senior expert to the junior expert $\boldsymbol{e_j}$ as a creditability weight in the criteria *m*
$LW_{m.s}^{e_j}$	Assigned weight by junior expert $\boldsymbol{e_j}$ to the sub-criteria *s* in the main criteria *m*
$LW_{m.s}$	Normalized weight of the sub-criteria *s* in the main criteria *m,* aggregated from the opinions of the multiple junior experts
$U_{m.s}^{e_j}$	Organization's required performance related to the sub-criteria *s* in the main criteria *m*, defined by the junior expert $\boldsymbol{e_j}$
$U_{m.s}$	Organization's required performance related to the sub-criteria *s* within the main criteria *m,* aggregated from the opinions of multiple junior experts

The weight of each main criterion as assigned by the senior expert and the degree of influence of each junior expert in the decision-making process within the main criteria is quantified utilizing the qualitative definition choices listed in Table II. The weights are then normalized such that their sum equals 1. The same definitions are used by the junior experts to allocate weights to each sub-criterion. Their multiple definitions are aggregated with the weighted average operator as shown in (1). The weights of the sub-criteria within each main criteria are also normalized to sum up to 1.

$$LW_{m.s} = \sum_{j=1}^{r}\left(LW_{m.s}^{e_j} . Cr_m^{e_j}\right) \qquad (1)$$

TABLE II. TRANSLATION OF QUALITATIVE WEIGHT DEFINITIONS TO QUANTITATIVE SCALE

Intensity	Definition
0	None
0.2	Low
0.4	Moderate
0.6	Medium
0.8	High
1	Very high

As a next step, the performance requirements within each sub-criteria is aggregated. These requirements can be expressed by data of one of three types: Boolean variables, numerical values, or linguistic expressions. Boolean variables or numerical values are aggregated using (2) and rounded to the nearest integer. For linguistic expressions, creditability weights of experts with identical definitions are summed up and the definition having the highest weight is considered as the organization's requirement. The results of Stage 1 are requirements weighted to organization-specific needs.

$$U_{m.s} = \sum_{j=1}^{r}\left(U_{m.s}^{e_j} \cdot Cr_m^{e_j}\right) \qquad (2)$$

B. Stage 2

The second stage evaluates CSPM solutions with respect to the ranked requirements using the PROMOTHEE II outranking method. Therefore, customized pairwise comparisons ($d_{m.s}$) are defined and the PROMOTHEE II's original preference function ($P_{m.s}$) is applied [14]. Finally, attribute aggregation provides an overall ranking.

The comparisons highlight scenarios, where requirements are not fulfilled. Hence, it outranks alternatives with lower offerings, while being outranked by alternatives providing better performance. Consequently, the comparison is assigned a value of 1 when the first compared alternative (a_1) offers a performance or capability that is more than the second (a_2), and 0 when the second alternative outperforms or is equivalent to the first.

For every type of data representation (Boolean, numerical and linguistic), a pairwise comparison method is defined. For Boolean variables (Type 1), the comparison results in 1, in case the first solution outperforms the other, and zero otherwise (see (3)).

$$d_{m.s}(a_1, a_2) = \begin{cases} 1 & a_1 = \text{"Yes" and } a_2 = \text{"No"} \\ 0 & \text{otherwise} \end{cases} \qquad (3)$$

For numerical values (Type 2), the values are compared, i.e., the comparison results in 1 in case a_1 is larger then a_2 (see (4)).

$$d_{m.s}(a_1, a_2) = \begin{cases} 1 & a_1 > a_2 \\ 0 & \text{otherwise} \end{cases} \qquad (4)$$

When dealing with linguistic expressions (Type 3), there are two possible scenarios where comparison results in 1. This is, (a) if the second alternative provides a subset of the first one. In case the two alternatives offer totally different services, the comparison results in 1, (b) if the first one is equivalent to what is required by the organization ($U_{m.s}$) (see (5)).

$$d_{m.s}(a_1, a_2) = \begin{cases} 1 & (a_1 \ni a_2) \lor \left((a_1 \not\equiv a_2) \land (a_1 \equiv U_{m.s})\right) \\ 0 & \text{otherwise} \end{cases} \qquad (5)$$

In order to calculate the ranking values in the first level of the hierarchy (sub-criteria level), PROMOTHEE II uses (6), utilizing the original preference function [15]. The preference function is equivalent to the previously defined pairwise comparisons $d_{m.s}$, since the original preference function is known to assign a value 1 only when the pairwise comparison results are greater than zero, and a value 0 otherwise. The number of sub-criteria *s* within a main criteria *m* is *f*.

$$\phi_m(a_i) = \frac{1}{n}\sum_{x\in A}\sum_{s=1}^{f}[LW_{m.s}\cdot P_{m.s}(a_i,x) - LW_{m.s}\cdot P_{m.s}(x,a_i)] \quad (6)$$

In the final phase, the overall ranking of the evaluated CSPM solutions based on the organization's requirements is calculated following a bottom-up approach, employing the weighted sum method using (7) [15].

$$\emptyset_{(a_i)} = \sum_{m=1}^{q}\emptyset_m(a_i).L_m \quad (7)$$

The ranking shows if all requirements are satisfied. In that case, the ranking equals the value of the organization's requirements; a higher value of a CSPM solution implies it exceeds the requirements.

IV. Case Study

The presented framework is validated by applying the data stored in the STAR repository related to the three CSPM solutions offered by AWS, Azure, and GCP. A senior expert at a high management level, along with three junior technical experts from different departmental units, provided the data regarding the requirements of a potential adopting organization.

A. Stage 1

Initially, the senior expert assigned a qualitative importance to the different main criteria. The results are given in Table III. Next, the answers regarding the importance of the main criteria are converted to quantitative values based on the definitions in Table II and normalized:

$$L_1 = L_3 = L_5 = \frac{0.8}{0.8+0.6+0.8+0.6+0.8} = 0.222$$

$$L_2 = L_4 = \frac{0.6}{0.8+0.6+0.8+0.6+0.8} = 0.167$$

The senior expert also assigned creditability weights to the juniors. For instance, the normalized values for the first main criteria are denoted as $Cr_1^{e_1}$, $Cr_1^{e_2}$, and $Cr_1^{e_3}$:

$$Cr_1^{e_1} = \frac{0.8}{0.8+0.2+0.2} = 0.667$$

$$Cr_1^{e_2} = \frac{0.2}{0.8+0.2+0.2} = 0.167$$

$$Cr_1^{e_3} = \frac{0.2}{0.8+0.2+0.2} = 0.167$$

TABLE III. Senior Expert Definition to the Importance of Main Criteria and the Influence of Junior Experts

M	Importance of Main Criteria	Influence of Junior Experts		
		1st Junior Expert	*2nd Junior Expert*	*3rd Junior Expert*
1	High	High	Low	Low
2	Medium	Medium	High	Moderate
3	High	High	Low	Moderate
4	Medium	Moderate	Moderate	High
5	High	Medium	Medium	High

Likewise, the normalized creditability weights of the three junior experts in the second main criteria are (0.33, 0.44, and 0.22), (0.57, 0.14, and 0.29) in the third main criteria, (0.3, 0.3, and 0.4) regarding the fourth main criteria, and (0.25, 0.25, and 0.5) in the fifth main criteria.

Next, the three junior experts filled the criteria template given in Table IV. In sub-criteria 1.1 and 5.1, the frequency is specified using linguistic expressions. Those are converted to numerical values. In sub-criteria 1.1, for example, we assign 1 to "Annually". Hence, "Once every two years" maps to 0.5, and "Semi-annually" to 2, the more it is repeated the better. Applying (1) results in $U_{1.1}$ = (1*0.667) +(0.5*0.167) +(2*0.167) = 0.91. This gives the organization's requirement value. Rounded to the nearest defined possibility the result is 1 (Annually).

For sub-criteria 2.1,3.1,4.1,4.2,4.3, and 4.4, Boolean variables are used. Thus, "Yes" is represented by 1, "No" by 0. For instance, the aggregated organization's requirement $U_{2.1}$ = (1*0.333) +(1*0.444) +(1*0.222) = 0.999, which implies 1 or "Yes" after rounding.

For sub-criteria 1.2 and 3.2, a direct transformation is not possible. Therefore, identical opinions are combined. The credibility weights of respective junior experts of the combination are summed up. For example, $U_{1.2}$ = (" Internal & external"* 0.667) +("external"* 0.167) +("Internal & external"* 0.167). For simplification, it is transformed to ("Internal & external" * (0.667+0.167) + ("external"*0.167), resulting in ("Internal & external "*0.834) + (external* 0.167). The final requirement is defined by the highest sum, i.e., "Internal & external".

TABLE IV. Juniors Experts Definitions of the Sub-criteria Importance & the Related Required Performance

Sub-Criteria	Importance (Weight)			Required Performance		
	1st Junior Expert	*2nd Junior Expert*	*3rd Junior Expert*	*1st Junior Expert*	*2nd Junior Expert*	*3rd Junior Expert*
1.1(A&A-02.1)	High	medium	Moderate	Annually	Every 2 years	Semi-annually
1.2(A&A-05.1)	Medium	Low	Moderate	Internal & external	External	Internal & external
2.1(AIS-07.2)	-	-	-	Yes	Yes	Yes
3.1(DSP-04.1)	High	Medium	High	Yes	Yes	Yes
3.2(DSP19.1)	Medium	Moderate	High	Twice	Twice	Twice
4.1(LOG-05.1)	High	Medium	High	Yes	Yes	Yes
4.2(LOG-05.2)	High	High	Very High	Yes	Yes	Yes
4.3(LOG-08.1)	Medium	Medium	High	Yes	Yes	Yes
4.4(LOG-13.2)	High	Medium	High	Yes	Yes	Yes
5.1(TVM7.1)	High	Medium	High	Monthly	Monthly	Monthly
5.2(TVM-02.1)	High	Medium	High	Yes	Yes	Yes

B. *Stage 2*

After defining the requirements of the organization, Stage 2 maps it to the potential solutions. The data representing the features of the CSPM tools offered by AWS, Azure, and GCP is given in Table V [16],[17],[18].

Next, the "Audit & Assurance" main criterion is considered. It includes two sub-criteria. The previous stage determined the requirements weights $LW_{1.1} = 0.583$ and $LW_{1.2} = 0.417$. The feature sets are compared with preferences functions (see section 3.2). The first feature specifies a frequency, where a shorter interval is better. Hence, the preference function $\boldsymbol{P_{1.1}}$ is 1 if and only if the first frequency value is higher than the second one. As there is no difference between the features of sub-criterion 1.2, it will not impact the assessment. The rankings are computed using (6) within the first main criteria and for all providers along with organization's requirements $A = AWS, Azure, GCP, U$ for all $a_i \in A$ as follows:

$$\emptyset_1(a_i) = \frac{1}{3}\sum_{x\in A}\sum_{s=1}^{2}[LW_{1.s} \cdot P_{1.s}(a_i, x) - LW_{1.s} \cdot P_{1.s}(x, a_i)] \quad (8)$$

Starting with the ($\emptyset_1(a_{AWS})$), applying (8) result as follows:

$$\begin{aligned}\emptyset_1(\mathrm{a_{AWS}}) = \frac{1}{3}\Big[&\big[[(0.583 * 0) - (0.583 * 0)]\\ &+ [(0.417 * 0) - (0.417 * 0)]\big]\\ &+ \big[[(0.583 * 0) - (0.583 * 1)]\\ &+ [(0.417 * 0) - (0.417 * 0)]\big]\\ &+ \big[[(0.583 * 0) - (0.583 * 0)]\\ &+ [(0.417 * 0) - (0.417 * 0)]\big]\Big] = -0.19\end{aligned}$$

TABLE V. CSPM' CSA CAIQ SUB-CRITERIA SCORES AGAINST ORGANIZATION'S REQUIREMENTS

$m.s$	U	a_1 (AWS)	a_2 (Azure)	a_3 (GCP)
1.1	Annually	Annually	Annually	Semi-annually
1.2	Internal & external	Internal & External	Internal & External	Internal & External
2.1	Yes	Yes	Yes	Yes
3.1	Yes	No	Yes	Yes
3.2	Twice	0 (not offered)	Upon request	Twice
4.1	Yes	Yes	Yes	Yes
4.2	Yes	Yes	Yes	Yes
4.3	Yes	Yes	Yes	Yes
4.4	Yes	Yes	Yes	Yes
5.1	Monthly	Quarterly	Monthly	Monthly
5.2	Yes	Yes	Yes	Yes

A similar computation for Azure, GCP and the organization's requirements provides the respective results for the first main criteria. According to the data related to the first main criteria (1.1&1.2) seen in Table V, the organization requires an annual assessment to be applied in sub-criteria 1.1. Therefore, the CSPM tool from GCP is the only option that offers a preference feature among the evaluated alternatives since it applies to the assessments twice a year, whereas the other two tools apply them once. As a result, the pairwise comparison results boosted its ranking value $\emptyset_1(a_3)$ to the highest value (0.58), as shown in Table VI.

The same steps are repeated for the remaining four main criteria using (6) and the results are shown in Table VI. The rankings of two main criteria are zero as the preference function for them zero, which implies that all tools equally fulfill what the organization requires.

TABLE VI. ALTERNATIVE'S RANKINGS WITHIN INDIVIDUAL MAIN CRITERIA

a_i	$\emptyset_1(a_i)$	$\emptyset_2(a_i)$	$\emptyset_3(a_i)$	$\emptyset_4(a_i)$	$\emptyset_5(a_i)$
a_1	-0.19	0	-3	0	-0.5
a_2	-0.19	0	1	0	0.17
a_3	0.58	0	1	0	0.17
U	-0.19	0	1	0	0.17

Using the bottom-up aggregation approach through the application of (7), the aggregation procedure to determine the final ranking value ($\emptyset(a_{AWS})$) of the AWS-provided CSPM tool, for instance, is computed as follows:

$$\begin{aligned}\phi(a_1) = [(\phi_1(a_1) \cdot L_1) + (\phi_2(a_1) \cdot L_2) + (\phi_3(a_1) \cdot L_3)\\ + (\phi_4(a_1) \cdot L_4) + (\phi_5(a_1) \cdot L_5)]\\ = -0.82\end{aligned}$$

For the other alternatives, similar computations are performed to determine their overall ranking values $\emptyset(a_2)$, $\emptyset(a_3)$, and $\emptyset(U)$ are 0.22, 0.39, and 0.22, respectively.A CSPM tool satisfies the organization's requirements if its final ranking meets or exceeds the organization's threshold (U). In our case study, GCP's tool exceeds U, Azure's tool meets U, and AWS's tool falls below U. Thus, GCP over-provisions, Azure fully satisfies, and AWS falls short of the organization's requirements.

C. *Sensitivity Analysis*

One of PROMOTHEE II's well-known limitations is the ranking reversal issues causing a change of preference between two alternatives after the addition or removal of a third one [14]. In order to demonstrate that addition or deletion of evaluated CSPM tools has no impact on the appropriate tool selection decision, three tests were carried out. In particular, (1) the worst alternative was removed, (2) the best alternative was deleted, and (3) a new tool (Alibaba) was added to the ranking [19].

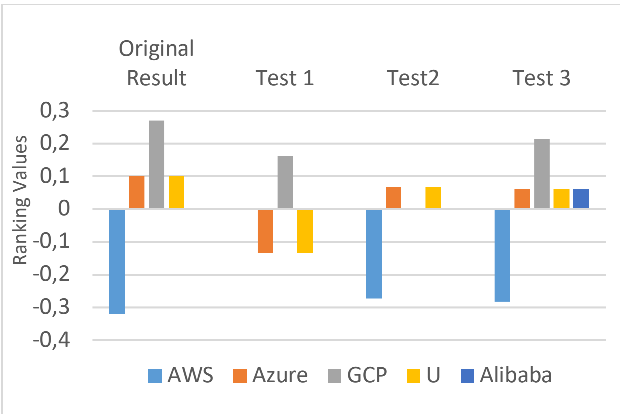

Fig. 4: Diverse Input Ranking Results.

Fig. 4 gives the results. They show that incorporating the GCP's CSPM tool consistently outperformed the organization's requirements (*U*), while Azure's solution always exactly fulfilled those needs. In contrast, AWS obtained lower rankings than the organization's required performance. These tests demonstrated that the proposed framework reliably generates consistent selections, regardless of the number of alternatives assessed.

V. Conclusions

This study presents an enhanced CSPM assessment methodology by integrating organizational requirements and introducing a structured method to identify them. A multi-expert approach addresses potential gaps in any single assessor's expertise, ensuring a comprehensive understanding of specific needs. The evaluation clearly distinguishes between alternatives that meet requirements and those that exceed them, aiding at an optimal selection. This provides guidance for both, practitioners and vendors involved in cloud security decision-making.

References

[1] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, "Cyberattacks and Security of Cloud Computing: A Complete Guideline," Symmetry, vol. 15, no. 11, p. 1981, Oct. 2023, doi: 10.3390/sym15111981.

[2] P. K. Tiwari and B. Mishra, "Cloud Computing Security Issues, Challenges and Solution," Int. J. Emerg. Technol. Adv. Eng., vol. 2, no. 8, pp. 306–310, Aug. 2012.

[3] R. Vázquez González, "Cloud Security Posture Management (CSPM)," Master's thesis, Universitat Oberta de Catalunya (UOC), 2021. [Online]. Available: https://hdl.handle.net/10609/132146.

[4] N. MacDonald, "Innovation Insight for Cloud Security Posture Management," Gartner, Stamford, CT, USA, Rep. G00377795, Jan. 25, 2019. [Online]. Available: https://www.gartner.com/en/documents/3899373/innovation-insight-for-cloud-security-posture-management

[5] CSA, "Cloud Controls Matrix | CSA." https://cloudsecurityalliance.org/research/cloud-controls-matrix/.

[6] R. Karim, C. Ding, and C.-H. Chi, "An enhanced PROMETHEE model for QOS-Based web service selection," *IEEE*, pp. 536–543, Jul. 2011, doi: 10.1109/scc.2011.81.

[7] J. Luna, R. Langenberg, and N. Suri, "Benchmarking cloud security level agreements using quantitative policy trees," ACM, pp. 103–112, Oct. 2012, doi: 10.1145/2381913.2381932.

[8] A. Taha, R. Trapero, J. Luna, and N. Suri, "AHP-Based Quantitative Approach for Assessing and Comparing Cloud Security," IEEE, Sep. 2014, doi: 10.1109/trustcom.2014.39.

[9] J. Modic, R. Trapero, A. Taha, J. Luna, M. Stopar, and N. Suri, "Novel efficient techniques for real-time cloud security assessment," *Computers & Security*, vol. 62, pp. 1–18, Jun. 2016, doi: 10.1016/j.cose.2016.06.003.

[10] A. Taha, P. Metzler, R. Trapero, J. Luna, and N. Suri, "Identifying and utilizing dependencies across cloud security services," ACM, pp. 329–340, May 2016, doi: 10.1145/2897845.2897911.

[11] A. Taha, R. Trapero, J. Luna, and N. Suri, "A framework for ranking cloud security services," *IEEE*, vol. 48, pp. 322–329, Jun. 2017, doi: 10.1109/scc.2017.48.

[12] S. Boneder, "Evaluation and comparison of the security offerings of the big three cloud service providers Amazon Web Services, Microsoft Azure and Google Cloud Platform," Bachelor Thesis, Technische Hochschule Ingolstadt, Ingolstadt, 2023. [Online]. Available: urn:nbn:de:bvb:573-37359.

[13] H. Taherdoost and M. Madanchian, "Multi-Criteria Decision Making (MCDM) methods and Concepts," Encyclopedia, vol. 3, no. 1, pp. 77–87, Jan. 2023, doi: 10.3390/encyclopedia3010006.

[14] J.-P. Brans and Y. De Smet, "PROMETHEE methods," in International series in management science/operations research/International series in operations research & management science, 2016, pp. 187–219. doi: 10.1007/978-1-4939-3094-4_6.

[15] J.-P. Brans and B. Mareschal, "Promethee Methods," in Multiple Criteria Decision Analysis: State of the Art Surveys, 2006, pp. 163–186. Doi: 10.1007/0-387-23081-5_5.

[16] Amazon Web Services, "CSA Consensus Assessments Initiative Questionnaire," Whitepaper, Jan. 2025. [Online]. Available: https://d1.awsstatic.com/whitepapers/compliance/CSA_Consensus_Assessments_Initiative_Questionnaire.pdf.

[17] Cloud Security Alliance, "Azure CAIQ," 2023. [Online]. Available: https://cloudsecurityalliance.org/star/registry/microsoft/services/microsoft-azure/download/uVd6bQ.

[18] Cloud Security Alliance, "GCP CAIQ," 2023. [Online]. Available: https://cloudsecurityalliance.org/star/registry/google/services/google-cloud/download/FP7YsA.

[19] Cloud Security Alliance, "Alibaba Cloud CAIQ," 2023. [Online]. Available: https://cloudsecurityalliance.org/star/registry/amazon/services/amazon-web-services/download/kwdz8Q.