

From Expert Consensus to User Perception: How Financial Staff and Independent Auditors Perceive Cloud Accounting Services Risk in the Petrochemical Industry

Mansour Heydari¹, Mohsen Azhdar^{2,*} and Iraj Torabi³



¹ Ph.D. Student, Department of Accounting, ShK.C., Islamic Azad University, Shahr-e Kord, Iran; 

² Department of Accounting, ShK.C., Islamic Azad University, Shahr-e Kord, Iran; 

³ Department of Accounting, ShK.C., Islamic Azad University, Shahr-e Kord, Iran; 

* Correspondence: m.azhdar@iau.ir

Citation: Heydari, M., Azhdar, M., & Torabi, I. (2027). From Expert Consensus to User Perception: How Financial Staff and Independent Auditors Perceive Cloud Accounting Services Risk in the Petrochemical Industry. *Business, Marketing, and Finance Open*, 4(9), 1-18.

Received: 06 May 2026

Revised: 04 October 2026

Accepted: 13 October 2026

Initial Publication: 26 October 2026

Final Publication: 01 September 2027



Copyright: © 2027 by the authors. Published under the terms and conditions of Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0) License.

Abstract: Cloud accounting moves sensitive financial data and processes beyond organizational boundaries, and the risks arising from this transfer are usually identified and prioritized on the basis of expert judgment. This study examines whether a risk framework derived from expert consensus is also supported from the perspective of those who prepare and audit cloud-hosted financial information, and whether the pattern of its dimensions as perceived by these two groups is aligned with expert priorities. A seven-dimension framework of cloud accounting services risk, developed in a prior qualitative study through thematic analysis and the fuzzy Delphi method, was operationalized as an 82-item questionnaire. Data were collected from 154 respondents in the Mahshahr Petrochemical Special Economic Zone, Iran, comprising 88 financial staff of petrochemical companies and 66 independent auditors. A reflective–reflective higher-order model was estimated separately for each group using partial least squares structural equation modeling (PLS-SEM), and the loading patterns were compared across the two groups and with the expert ranking. The results indicate that all seven dimensions had high and significant loadings on overall risk in both groups (0.76 to 0.95). In an exploratory inspection, the loadings fell into two clusters: five dimensions with loadings of 0.90 to 0.95, and the security and data and service quality dimensions with loadings of 0.76 to 0.78. Security risk, ranked first by the experts, fell into the lower cluster in both groups, and the correlation between user and expert rankings, whether based on factor loadings or on mean scores, was close to zero and non-significant. The loading pattern and the overall level of perceived risk were nearly identical for financial staff and auditors ($t = 0.173$, $p = 0.863$). The study tests an expert-derived framework among preparers and auditors in a heavy process industry operating under international sanctions and provides preliminary evidence of misalignment between expert priorities and users' perceptions. The findings are exploratory, and the structure of the dimensions should be confirmed through item-level analysis in future research.

Keywords: Cloud accounting, risk assessment, risk perception, independent auditors, PLS-SEM, petrochemical industry

1. Introduction

Cloud computing has transformed the architecture of contemporary accounting information systems by shifting data storage, transaction processing, financial reporting, and increasingly analytical and assurance functions from locally controlled organizational infrastructures to remotely hosted, network-accessible environments. Within this transformation, cloud accounting has emerged as an important component of digital financial management because it enables organizations to access accounting applications and financial information through internet-based platforms without maintaining the entire technological infrastructure

internally. Recent scholarship indicates that cloud accounting has moved beyond being a technological alternative for small firms and has become part of a broader restructuring of accounting processes, organizational information flows, and relationships between firms, service providers, financial professionals, and auditors [1]. Its appeal derives from several potential advantages, including lower infrastructure and software maintenance costs, scalability, improved accessibility, real-time information sharing, greater flexibility in financial operations, and more efficient collaboration among organizational units and external stakeholders. Empirical research has also associated cloud-based accounting information systems with improvements in organizational efficiency and business performance, particularly where technological capabilities are combined with organizational preparedness and effective implementation practices [2]. Nevertheless, the increasing dependence of accounting functions on externally hosted digital infrastructures creates a corresponding need to reconsider the nature, structure, and perception of the risks associated with cloud-based accounting.

The development of cloud accounting has been especially visible among small and medium-sized enterprises, where resource constraints make externally provided computing services economically attractive. Studies of cloud accounting implementation have shown that technological compatibility, managerial support, perceived benefits, organizational readiness, security concerns, and external environmental conditions can substantially influence adoption decisions [3]. A recent systematic review similarly demonstrates that the cloud accounting literature has concentrated heavily on adoption determinants, implementation drivers, performance consequences, and organizational benefits, with much of the empirical evidence derived from SMEs [4]. Another systematic synthesis of the field confirms the rapid expansion of cloud accounting research while also showing that significant conceptual and empirical gaps remain concerning the risks created after organizations transfer accounting information and processes to cloud environments [1]. Consequently, although the advantages and adoption determinants of cloud accounting have received considerable scholarly attention, less is known about how the multidimensional risks associated with cloud accounting are structured and perceived by the professionals who prepare, manage, and audit financial information.

Cloud accounting risk cannot be reduced to cybersecurity alone. The transfer of accounting systems to cloud infrastructures alters organizational boundaries and redistributes responsibility for data, system availability, processing integrity, access control, regulatory compliance, business continuity, and technological maintenance between the client organization and the cloud service provider. Evidence from accounting practitioners has identified concerns involving confidentiality, privacy, unauthorized access, service interruption, provider dependence, data location, system integration, legal uncertainty, loss of organizational expertise, and difficulties associated with changing service providers [5]. Research focused specifically on external auditors has likewise demonstrated that auditors may be concerned about confidentiality, data security, the physical and legal location of organizational information, the reliability of service providers, and their ability to obtain adequate audit evidence when financial data are maintained in cloud environments [6]. These findings indicate that cloud accounting risk is inherently multidimensional and that a narrow concentration on technical security can obscure legal, financial, operational, organizational, human, and governance-related vulnerabilities.

The multidimensional character of cloud risk is also recognized in contemporary enterprise risk management guidance. The Committee of Sponsoring Organizations of the Treadway Commission emphasizes that the risks associated with cloud computing should be integrated into enterprise risk management because cloud arrangements can simultaneously affect strategy, governance, compliance, business continuity, information reliability, third-party relationships, and internal control [7]. From an accounting perspective, this integration is

particularly important because cloud systems may contain the general ledger, transaction records, supporting documentation, audit trails, tax information, and other data that form the evidential basis for both internal decision-making and external financial reporting. The issue therefore extends beyond whether a cloud application functions effectively; it concerns whether the wider control environment continues to provide reasonable assurance regarding the reliability, accessibility, integrity, and accountability of financial information.

The increasing use of automated analytics further complicates this risk environment. Developments in artificial intelligence, continuous auditing, and anomaly detection have created opportunities for identifying irregular transactions and strengthening monitoring within cloud accounting systems [8]. At the same time, these developments introduce new dependencies on digital infrastructure, algorithmic processes, data quality, systems integration, and specialized expertise. The value of continuous auditing, for example, depends on reliable access to complete and timely data and on the continuing integrity of interfaces between accounting applications, cloud infrastructures, and auditing technologies. The development of cloud accounting therefore creates a dual dynamic: digitalization can strengthen monitoring and assurance while simultaneously increasing the number and complexity of technological relationships on which financial reporting and auditing depend. This reinforces the need for risk frameworks capable of capturing interactions among technological, operational, legal, economic, organizational, and human factors rather than treating individual risks as isolated phenomena.

Assurance becomes particularly important when financial processing is performed by an external service organization. International assurance standards recognize the significance of controls maintained by service organizations for the entities that rely on them and for auditors evaluating those entities' financial reporting systems. ISAE 3402 provides a framework through which assurance may be obtained regarding controls at service organizations that are relevant to user entities' internal control over financial reporting [9]. In cloud accounting environments, such assurance can become especially important because significant elements of data processing, access management, backup procedures, system continuity, and information security may operate outside the direct control of the reporting organization. Yet the availability and practical usefulness of such assurance can vary considerably across jurisdictions and providers. Consequently, risk assessment must consider not only whether cloud services are technologically secure but also whether organizations and auditors possess sufficient information and assurance regarding the design and operation of provider-side controls.

Cloud computing also operates within a transnational technological and political environment. Cloud infrastructures are frequently distributed across jurisdictions, while data, software, technical support, and security services may depend on multinational providers. This structure creates questions concerning data sovereignty, jurisdiction, governmental access, cross-border control, and the political economy of digital infrastructure [10]. Such issues become particularly consequential in strategic industries and in jurisdictions facing restrictions on access to international technologies or service providers. In these contexts, cloud accounting risks may include not merely generic technological threats but also exclusion from international services, difficulties obtaining software updates, dependence on domestic providers, restricted access to hardware and cybersecurity tools, and interruptions arising from geopolitical developments. Therefore, the meaning of cloud accounting risk is partly context-dependent: risks perceived as peripheral in an open and competitive cloud market may become central where organizations operate under technological, economic, or geopolitical constraints.

This context is especially relevant to Iran's petrochemical industry. Petrochemical companies operate in a capital-intensive, technologically complex, export-oriented environment in which financial information is closely connected to production, taxation, foreign exchange, contracting, supply chains, investment, and regulatory

reporting. Their cloud accounting systems may therefore be expected to interact with legacy accounting applications, enterprise systems, production technologies, governmental reporting platforms, and auditing processes. At the same time, sanctions and restricted access to international digital services may increase dependence on domestic technological infrastructures and create distinctive risks associated with compatibility, continuity, vendor dependence, hardware availability, cybersecurity resources, and cross-border access. Iranian research has begun to address these challenges by developing strategies for mitigating cloud accounting risks, demonstrating growing recognition that the accounting profession must treat cloud risk as a broad managerial and professional problem rather than merely an information technology issue [11]. However, identifying risks and proposing mitigation strategies does not by itself establish whether different professional groups perceive the structure and relative salience of those risks in the same manner.

This distinction between technically or professionally identified risk and perceived risk is theoretically important. Research on risk perception has long demonstrated that judgments concerning hazards are not determined solely by objective estimates of probability and expected loss. Perceived controllability, familiarity, uncertainty, catastrophic potential, immediacy, and the distribution of consequences can influence how individuals evaluate the seriousness of a hazard [12]. Subsequent research has confirmed that risk judgments remain strongly shaped by psychological, social, informational, and contextual processes and that experts and non-experts do not necessarily evaluate identical hazards in identical ways [13]. Although accounting professionals cannot simply be classified as laypeople, the broader principle remains relevant: groups occupying different positions in relation to a technological system may form different judgments because they encounter different manifestations of risk and possess different forms of knowledge and responsibility.

Empirical evidence from other risk domains further supports the importance of distinguishing expert prioritization from stakeholder perception. Comparative research on risk prioritization has shown that experts and members of other stakeholder groups can rank the same hazards differently, even when they are asked to consider a common set of risks [14]. These discrepancies should not automatically be interpreted as evidence that one group is correct and another is mistaken. Rather, they can reflect differences in expertise, direct exposure, professional responsibility, controllability, familiarity, and evaluative criteria. Applied to cloud accounting, this implies that expert consensus may be highly effective for identifying the domain of potential risks, yet it may not reproduce the structure of risk as experienced by financial personnel and auditors in everyday professional practice. Experts considering cloud accounting at a conceptual level may emphasize highly visible threats such as cybersecurity and confidentiality, whereas users who routinely interact with cloud systems may also attach substantial significance to integration difficulties, system interruptions, provider dependence, financial costs, reporting requirements, and organizational capacity.

The possibility of perceptual divergence is also relevant to the relationship between preparers and auditors. Financial personnel are directly responsible for recording, processing, reconciling, and reporting organizational transactions and therefore interact continuously with the operational consequences of system performance. Independent auditors occupy a different institutional role, evaluating the reliability of financial information, audit trails, controls, compliance, and evidence used to support the audit opinion. It might therefore be expected that financial personnel would be particularly sensitive to operational continuity, integration, workload, and usability, whereas auditors might emphasize control reliability, regulatory compliance, data integrity, and the availability of sufficient appropriate audit evidence. Nevertheless, prior research on audit quality perception indicates that differences between auditors and financial statement preparers cannot always be explained simply by their formal

roles. Shared professional expertise, common standards, and common organizational environments may produce substantial convergence between the judgments of auditors and preparers [15]. Whether such convergence occurs in relation to cloud accounting risk, particularly in a sanctions-affected petrochemical environment, remains an empirical question.

Addressing this question requires a framework that treats cloud accounting risk as a multidimensional construct rather than a collection of unrelated threats. The framework examined in the present research originated in a qualitative phase in which professional knowledge concerning cloud accounting risks was systematically organized. Thematic analysis provides a rigorous method for identifying patterned meanings in qualitative data and for progressing from individual codes to broader themes that represent recurring dimensions within a body of evidence [16]. Expert consensus methods can subsequently be used to refine and prioritize such dimensions. In particular, fuzzy decision approaches are useful when expert assessments are expressed through linguistic judgments and uncertainty rather than exact numerical values, because qualitative evaluations can be represented and aggregated through fuzzy numbers [17]. These approaches make it possible to construct an expert-derived risk framework, but they do not establish whether that framework is psychometrically reproduced among the professionals who interact with cloud accounting systems in practice.

Testing such a framework requires careful attention to measurement specification. Multidimensional concepts may be represented through higher-order models in which several first-order constructs reflect a broader latent construct. However, the validity of such models depends on whether the conceptual relationship between indicators, dimensions, and the higher-order construct has been correctly specified. Incorrectly treating formative relationships as reflective, or reflective relationships as formative, can materially distort substantive conclusions [18]. Methodological research on hierarchical latent variable models provides procedures for estimating and assessing higher-order constructs within partial least squares structural equation modeling, including models containing reflective and formative components [19]. Subsequent work has further clarified how higher-order constructs should be specified, estimated, validated, and interpreted within PLS-SEM [20]. These considerations are particularly relevant when cloud accounting services risk is conceptualized as an overarching construct manifested through several related dimensions.

PLS-SEM is also suited to research situations involving complex measurement structures, moderate sample sizes, and data that do not necessarily satisfy multivariate normality assumptions. Current methodological guidance emphasizes the importance of assessing construct reliability and validity while interpreting structural and measurement results in accordance with the purpose and specification of the model [21]. More comprehensive guidance further provides criteria for evaluating internal consistency, convergent validity, indicator performance, and higher-order measurement structures in PLS-SEM applications [22]. Importantly, factor loadings in a reflective higher-order model should not automatically be interpreted as direct measures of the objective severity or policy importance of a risk. Instead, they indicate the degree to which each lower-order dimension shares variance with and reflects the broader latent construct. This distinction becomes critical when comparing user-derived loading patterns with expert-derived priority judgments because the two measures represent related but conceptually different aspects of risk assessment.

Against this background, an important gap emerges at the intersection of cloud accounting, risk perception, auditing, and measurement research. Existing studies have provided substantial evidence regarding the benefits and adoption of cloud accounting [2, 3], catalogued its technological and organizational risks [5, 6], examined emerging auditing technologies [8], and highlighted questions of enterprise risk governance and data sovereignty

[7, 10]. Systematic reviews nevertheless suggest that the literature remains uneven and that risk-focused empirical research is less developed than research on adoption and performance [1, 4]. More specifically, limited evidence is available on whether a multidimensional risk framework developed from expert consensus is supported by the perceptions of actual accounting-system users, whether financial staff and independent auditors structure those risks similarly, and whether user perceptions correspond to the priorities established by experts. These questions are particularly consequential in a strategic, sanctions-affected industry where technological, regulatory, economic, and geopolitical conditions may simultaneously shape cloud accounting risk. The present study therefore aims to examine whether the seven-dimensional expert-derived framework of cloud accounting services risk is supported by financial staff and independent auditors in the Mahshahr Petrochemical Special Economic Zone, determine how strongly each dimension reflects overall perceived risk in the two groups, and assess whether users' perceptions are aligned with the risk priorities derived from expert consensus.

2. Methods and Materials

This study is applied in purpose and quantitative in nature, and it adopts a cross-sectional survey design. It constitutes the confirmatory phase of a broader project whose earlier qualitative phase produced the framework tested here.

The study is confirmatory with respect to the structure of the framework and exploratory with respect to its priorities. For this reason, research questions and associated propositions are stated instead of directional hypotheses for each path.

Research Question 1. Is the seven-dimension framework a valid second-order measurement model of cloud accounting services risk from the perspective of internal and external users? If the dimensions identified by the experts are genuine facets of a common risk, each should share substantial variance with the second-order construct in both groups.

Proposition 1. Each of the seven dimensions has a significant factor loading on overall cloud accounting services risk in both the internal and the external user groups.

Research Question 2. To what extent does each dimension reflect overall risk, and do internal and external users differ in how they weight the dimensions and in the overall level of perceived risk? The difference in roles described above suggests that auditors should give greater weight to compliance, reporting, and evidential issues, and financial staff to operational and human issues. Shared industry expertise, however, points in the opposite direction [8].

Proposition 2a. Internal and external users exhibit different loading patterns across the seven dimensions.

Proposition 2b. The overall level of perceived cloud accounting risk differs between internal and external users.

Research Question 3. Is the order of dimensions from the users' perspective consistent with the order derived from expert consensus? Risk perception research indicates that experts judging in the abstract and users judging on the basis of daily exposure do not necessarily agree [6, 7].

Proposition 3. The pattern of dimensions based on user data is not aligned with the priorities derived from expert consensus.

In addition to these three questions, the pattern of dimension loadings is also described in an exploratory manner. This part of the analysis was not planned before data collection, and its results should be read as hypotheses for future research rather than as confirmatory findings.

The study was conducted in the Mahshahr Petrochemical Special Economic Zone in Khuzestan Province, Iran. The zone hosts a cluster of major petrochemical producers, many of which are listed on the Tehran Stock Exchange or the Iran Fara Bourse and which together account for a considerable share of the country's non-oil exports. Companies in the zone are migrating their accounting, treasury, and reporting processes to cloud platforms that, because of sanctions, are hosted mainly within the country. The setting therefore combines high data sensitivity, stringent oversight, and restricted access to global cloud services.

The framework was developed in the qualitative phase of the research, which is reported in full in a companion paper by the authors (forthcoming); it is summarized here only to the extent needed to understand the present analysis. Semi-structured interviews were conducted with 17 finance, accounting, and auditing experts, each with at least 15 years of professional experience. Participants were drawn from petrochemical companies and the audit firms contracted by them, using purposive and snowball sampling until theoretical saturation was reached. The interview transcripts were analyzed through inductive thematic analysis. Basic codes were grouped into organizing themes and then into the seven global dimensions shown in Table 1, and each code was labeled according to whether it reflected an internal or an external perspective. The dimensions were then submitted to the same experts in two rounds of the fuzzy Delphi method. Linguistic judgments were converted into triangular fuzzy numbers, aggregated, and defuzzified. All seven dimensions exceeded the acceptance threshold of 0.70. The difference between the two rounds ranged from 0.002 to 0.01, well below the stopping criterion of 0.1 proposed by Cheng and Lin; the process was therefore terminated after the second round. Table 1 presents the dimensions of the framework and the weight of each dimension in the second Delphi round. This weight is the defuzzified mean of the experts' judgments and exceeds the 0.70 threshold for every dimension.

Table 1. Dimensions of Cloud Accounting Services Risk and Expert Consensus Weights

Dimension	Scope	No. of Items	Fuzzy Delphi Weight	Expert Rank
Security and Data	Unauthorized access, confidentiality, data loss during transfer, sanctions-related restrictions on security tools, national data sovereignty	10	0.808	1
Legal Compliance and Reporting	Compliance with national and international standards, audit trail, regulatory penalties, contractual ambiguity over data ownership	13	0.788	2
Financial and Economic	Hidden implementation and maintenance costs, exchange-rate volatility, recovery costs after cyberattacks, uncertain return on investment	10	0.778	3
Compatibility and Technology	Integration with legacy systems, vendor lock-in, offline backup, bandwidth, access to hardware under sanctions	12	0.776	4
Service Quality and Operational	Network instability, scalability for high transaction volumes, power outages, delays in data access	10	0.768	5
Geopolitical and Competitive	Exclusion from global services due to sanctions, regional cyber threats, data-center supply chain, falling behind competitors	15	0.766	6
Cultural, Social, and Human	Resistance to change, digital skills gap, emigration of skilled staff, trust in the system, decisions based on incomplete reports	12	0.756	7

The questionnaire was constructed directly from the qualitative codes. Each of the 82 items describes a specific risk event or condition and can be traced back to the code from which it was derived. Examples include “disruption in the online submission of invoices to the Taxpayers' System due to cloud technical failures” and “exclusion from global cloud services due to direct foreign sanctions.” The items were grouped under the seven dimensions (10 to

15 items per dimension; Table 1), and the complete list is provided in the Appendix. Respondents rated the level of risk that each item poses to their organization's cloud accounting on a five-point scale ranging from 1 (very low risk) to 5 (very high risk).

Content validity was assessed by the supervisors, advisors, and subject-matter specialists, who confirmed the wording and relevance of each item. Face validity was also confirmed by several members of the target population. In a pilot test with 30 respondents, Cronbach's alpha exceeded 0.70 for all dimensions, after which the questionnaire was distributed to the main sample.

The research population comprised two groups. The first consisted of the financial staff of petrochemical companies located in the zone, including chief financial officers, heads of accounting, internal audit managers, and financial members of audit committees (internal users). The second consisted of the independent auditors who audit these companies (external users). The sample size was set at 154 using the Krejcie and Morgan table, and respondents were selected through convenience sampling.

The final sample included 88 internal users (57.1%) and 66 external users (42.9%); 94 respondents (61%) were men and 60 (39%) were women. Mean professional experience was 15.7 years ($SD = 6.2$; range = 1 to 28 years). Most respondents had long professional experience, but the range is wide and respondents with limited experience are also represented in the sample.

The Kolmogorov–Smirnov test rejected normality for five of the seven dimensions ($p < 0.05$). In addition, the model comprises 82 indicators and one second-order construct, and each group is of moderate size. For these reasons, partial least squares structural equation modeling (PLS-SEM) was used, which is suitable for complex models with moderate samples and does not require the assumption of multivariate normality.

Cloud accounting services risk was specified as a reflective–reflective second-order construct (Figure 1). The seven dimensions are first-order constructs measured by their respective items, and overall risk is a second-order construct that accounts for their shared variance. The model was estimated using the repeated indicators approach. In this specification, overall risk denotes the perceived vulnerability of the finance function to the cloud environment—an environment shaped by sanctions, infrastructure, and a common provider, which is expected to affect all dimensions simultaneously.

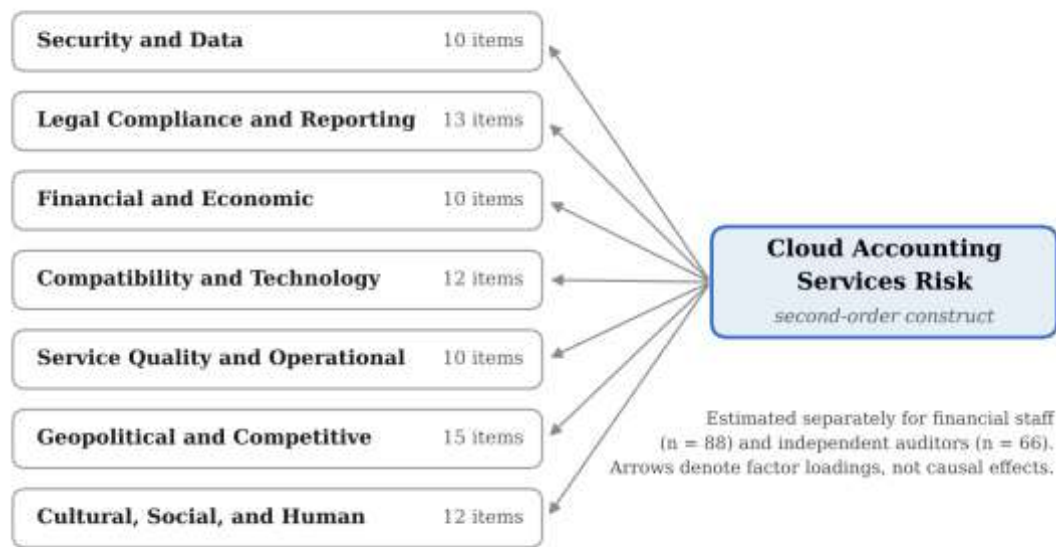


Figure 1. Conceptual model of the research

Interpreting factor loadings in this model requires care. In a reflective model, the loading of each dimension indicates how strongly that dimension is correlated with overall risk and what share of its variance is explained by the common factor. A loading is not a measure of the “importance” or “severity” of a risk; a dimension with a lower loading may represent a serious risk that is nevertheless independent of the other dimensions. Accordingly, this article interprets the loading of each dimension as “the extent to which it reflects overall risk” and avoids terms such as priority or importance weight.

The model was estimated separately for internal and external users in SmartPLS. The measurement model was evaluated in terms of internal consistency reliability (Cronbach's alpha and composite reliability) and convergent validity (average variance extracted, AVE). The overall level of perceived risk in the two groups was compared using an independent-samples t-test, and its effect size (Cohen's d) was computed from the t statistic. The loading patterns of the two groups were compared directly and descriptively. The grouping of dimensions based on the distance between loadings is an exploratory inspection conducted after the results were observed and has not been confirmed by a statistical test.

For the comparison with the experts, the dimensions were ranked on the basis of each group's factor loadings, and Spearman's rank correlation (ρ) and Kendall's tau with the fuzzy Delphi ranking were computed. Because the Delphi weight reflects “importance” whereas a factor loading reflects “correlation,” the comparison was repeated using users' raw mean scores. Like the Delphi weight, the mean score reflects the level of risk.

3. Findings and Results

In this section, the descriptive statistics of the research variables are presented first, followed by the evaluation of the measurement model, the second-order model, the comparison of the two user groups, and the comparison between users and experts.

Table 2 reports the descriptive statistics of the seven dimensions for the full sample. Mean perceived risk is slightly above the midpoint of the scale for all dimensions, ranging from 3.08 for legal compliance and reporting to

3.23 for geopolitical and competitive risk. The range of the means is only 0.15, and no dimension shows a clear advantage in terms of risk level.

Table 2. Descriptive Statistics and Normality Test (n = 154)

Dimension	Mean	Median	Std. Dev.	K-S Statistic	Sig. Level
Security and Data	3.15	3.20	0.60	1.485	0.024
Legal Compliance and Reporting	3.08	3.15	0.63	1.714	0.006
Financial and Economic	3.20	3.20	0.61	1.725	0.005
Compatibility and Technology	3.13	3.17	0.66	1.969	0.001
Service Quality and Operational	3.13	3.11	0.64	1.307	0.066
Geopolitical and Competitive	3.23	3.27	0.70	1.199	0.113
Cultural, Social, and Human	3.18	3.17	0.61	0.999	0.271

Table 3 summarizes reliability and convergent validity for both groups. Cronbach's alpha ranges from 0.780 to 0.920 in the internal group and from 0.766 to 0.922 in the external group, and all constructs exceed the 0.70 threshold. Composite reliability in the internal group ranges from 0.850 to 0.950. The AVE of every construct exceeds 0.50 in both groups (0.541 to 0.863 in the internal group and 0.524 to 0.865 in the external group), confirming convergent validity. Composite reliability was not reported for the external group; Cronbach's alpha, which provides a conservative estimate of reliability, was used as the reliability criterion for this group.

Table 3. Reliability and Convergent Validity

Construct	α (Internal)	CR (Internal)	AVE (Internal)	α (External)	AVE (External)
Cloud Accounting Services Risk (second-order)	0.907	0.931	0.729	0.912	0.740
Security and Data	0.832	0.887	0.663	0.838	0.670
Legal Compliance and Reporting	0.840	0.893	0.677	0.851	0.692
Financial and Economic	0.867	0.903	0.651	0.875	0.664
Compatibility and Technology	0.920	0.950	0.863	0.922	0.865
Service Quality and Operational	0.787	0.854	0.541	0.772	0.524
Geopolitical and Competitive	0.780	0.850	0.592	0.766	0.569
Cultural, Social, and Human	0.804	0.875	0.650	0.805	0.654

Note: α = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted. Internal group n = 88; external group n = 66.

Table 4 presents the loadings of the seven dimensions on overall cloud accounting services risk. All loadings are large and significant at $p < 0.001$ in both groups (0.762 to 0.946). Proposition 1 is therefore supported: each of the dimensions identified by the experts is a facet of the overall risk perceived by users.

Table 4. Second-Order Factor Loadings

Dimension	Loading (Internal)	t (Internal)	Loading (External)	t (External)
Compatibility and Technology	0.944	73.47	0.946	56.28
Geopolitical and Competitive	0.922	53.35	0.930	48.50
Financial and Economic	0.918	42.91	0.933	37.83
Legal Compliance and Reporting	0.908	44.11	0.913	35.46
Cultural, Social, and Human	0.905	66.54	0.904	48.98
Service Quality and Operational	0.780	22.04	0.762	18.13
Security and Data	0.775	15.30	0.774	12.05

Note: All loadings are significant at $p < 0.001$. Internal group n = 88; external group n = 66.

Exploratory inspection of the loading pattern. In both groups, the loadings fall into two clusters. The first cluster comprises five dimensions—compatibility and technology, geopolitical and competitive, financial and economic, legal compliance and reporting, and cultural, social, and human—whose loadings lie within a range of less than 0.04 (0.905 to 0.944 in the internal group and 0.904 to 0.946 in the external group). The second cluster comprises service quality and operational risk and security and data risk, with loadings between 0.762 and 0.780. The gap between the two clusters is approximately 0.12 to 0.14 and appears in the same form in both groups.

This grouping is subject to three important caveats. First, it was performed after the results were observed, and the differences between loadings were not tested statistically; the internal order of the first cluster is therefore not meaningful, and the boundary between the two clusters is not confirmed. Second, both dimensions in the second cluster have the smallest number of items (10). Under the repeated indicators approach, dimensions with more items contribute more to the construction of the second-order construct and may receive higher loadings [22]. Third, some items overlap in content with more than one dimension (see the limitations in Section 4). The two-tier pattern should therefore be regarded as a hypothesis to be tested in future research.

The overall level of perceived risk did not differ significantly between the two groups ($t = 0.173$, $p = 0.863$), and the effect size was virtually zero ($d = 0.03$). Proposition 2b is therefore not supported. The loading patterns of the two groups are also nearly identical: the largest between-group difference in the loading of any dimension is 0.018, for service quality and operational risk, and the exploratory grouping of the dimensions is the same in both groups. The rank correlation between the two groups' loadings is high: Spearman's $\rho = 0.93$ ($p = 0.003$) and Kendall's $\tau = 0.81$ ($p = 0.011$). This comparison is descriptive, and no formal multigroup analysis was performed. With this caveat, the available evidence does not support a difference between the two groups, and Proposition 2a is not supported.

Table 5 places the position of each dimension among experts and users side by side. The clearest pattern appears at the level of clusters rather than ranks. Security and data risk, which the experts considered the most important dimension, falls into the lower-loading cluster in both user groups. Conversely, compatibility and technology risk and geopolitical and competitive risk, which the experts ranked fourth and sixth, belong to the first cluster among users.

Table 5. Position of the Dimensions Among Experts and Users

Dimension	Delphi Weight (Expert Rank)	Loading Cluster: Financial Staff	Loading Cluster: Auditors	Mean Score (Rank)
Security and Data	0.808 (1)	Second	Second	3.15 (4)
Legal Compliance and Reporting	0.788 (2)	First	First	3.08 (7)
Financial and Economic	0.778 (3)	First	First	3.20 (2)
Compatibility and Technology	0.776 (4)	First	First	3.13 (5)
Service Quality and Operational	0.768 (5)	Second	Second	3.13 (6)
Geopolitical and Competitive	0.766 (6)	First	First	3.23 (1)
Cultural, Social, and Human	0.756 (7)	First	First	3.18 (3)

Note: First cluster = loadings of 0.90 to 0.95; second cluster = loadings of 0.76 to 0.78 (exploratory grouping). Mean scores are based on the full sample ($n = 154$); for the rank of means, the two dimensions with a mean of 3.13 were separated on the basis of their medians.

At the level of ranks, the correlation between the expert ranking and the ranking of each group is close to zero and non-significant (internal group: $\rho = -0.25$, $p = 0.59$; external group: $\rho = 0.00$, $p = 1.00$). This result should be read with caution. With only seven observations, the power of the test is low, and the absence of a significant correlation

does not imply a “reversal” of priorities. The Delphi weights also fall within a very narrow range (0.756 to 0.808), and their middle ordering depends on very small differences.

To rule out the non-equivalence of the two metrics, the expert ranking was also compared with the users' raw mean scores (Table 2). Like the Delphi weight, the mean score measures the level of risk. This correlation is also negative and non-significant ($q = -0.41$, $p = 0.36$). On this metric, geopolitical and financial risks have the highest means, and security risk ranks fourth—in the middle of the list rather than at the top. Thus, under both metrics, there is no evidence that user priorities are aligned with expert consensus. Proposition 3 is supported, with the qualification that the finding is one of “non-alignment” rather than a complete reversal. Table 6 summarizes the results for all propositions.

Table 6. Summary of Results for the Propositions

Proposition	Evidence	Result
P1: All dimensions have significant loadings in both groups	Factor loadings of 0.762 to 0.946; $p < 0.001$	Supported
P2a: The loading patterns of the two groups differ	Maximum loading difference = 0.018; identical clustering; $q = 0.93$	Not supported (descriptive comparison)
P2b: The overall level of risk differs between the two groups	$t = 0.173$, $p = 0.863$, $d = 0.03$	Not supported
P3: The users' pattern is not aligned with that of the experts	Security in the second cluster; $q = -0.25$ and 0.00 (loadings), -0.41 (means)	Supported (non-alignment, not reversal)

4. Discussion and Conclusion

The present study examined whether a seven-dimensional framework of cloud accounting services risk, initially developed through expert consensus, was supported by the perceptions of financial staff and independent auditors in the Mahshahr Petrochemical Special Economic Zone, and whether the structure of risk perceived by these two groups corresponded with expert priorities. The results provide several noteworthy findings. First, all seven dimensions—security and data, legal compliance and reporting, financial and economic, compatibility and technology, service quality and operational, geopolitical and competitive, and cultural, social, and human risk—loaded significantly on the higher-order construct of cloud accounting services risk in both groups, with loadings ranging from 0.762 to 0.946. T article Heydari bmf This finding supports the multidimensional conceptualization of cloud accounting risk and indicates that the expert-derived framework is broadly meaningful from the perspective of those who directly prepare and audit cloud-hosted financial information. The result is consistent with prior research showing that cloud accounting risk extends beyond information security to include technological integration, service dependence, compliance, organizational readiness, economic consequences, and human factors [5, 6]. It is also compatible with enterprise risk management guidance emphasizing that cloud-related exposures should be treated as cross-functional organizational risks rather than as narrowly technical concerns belonging exclusively to information technology departments [7].

The support for all seven dimensions is also consistent with the broader evolution of cloud accounting research. Systematic reviews indicate that the field has moved from an initial focus on adoption and technological acceptance toward a more comprehensive consideration of governance, organizational readiness, service-provider relationships, and risk consequences [1, 4]. Studies of cloud accounting adoption have similarly shown that implementation outcomes are shaped by interacting technological, organizational, and environmental conditions rather than by a single determinant [2, 3]. In the present study, the empirical support for the seven dimensions suggests that users do not experience cloud accounting risk as a collection of isolated events. Instead, they appear

to perceive a broader vulnerability structure in which regulatory, financial, technological, operational, geopolitical, and human conditions jointly contribute to overall risk. Such a result is theoretically compatible with the use of a higher-order construct, because multidimensional organizational phenomena may be represented through interrelated first-order dimensions when those dimensions share substantial variance with an overarching latent concept [19, 20]. At the same time, the interpretation of these loadings should remain consistent with reflective measurement logic: higher loadings indicate stronger correspondence with the general risk construct, not necessarily greater objective severity or managerial priority [18, 21].

A second important finding was the exploratory emergence of a two-cluster loading pattern. Five dimensions—compatibility and technology, geopolitical and competitive, financial and economic, legal compliance and reporting, and cultural, social, and human risk—showed very high loadings of approximately 0.90 to 0.95, whereas security and data risk and service quality and operational risk showed lower, though still substantial, loadings of approximately 0.76 to 0.78 in both groups. This pattern is particularly noteworthy because security and data risk had been ranked first by the expert panel, yet it did not emerge as the dimension most closely associated with overall perceived risk among users. One substantive explanation is that financial staff and auditors in this context may experience cloud risk primarily through the combined effects of technological dependence, economic constraints, regulatory requirements, sanctions, and organizational capabilities. In an environment where access to international providers, hardware, software updates, support services, and advanced security tools may be constrained, risk may be experienced as an interconnected structural condition rather than predominantly as a cybersecurity problem.

This interpretation is consistent with research emphasizing the transnational and political character of cloud infrastructures. Tang argued that cloud computing cannot be understood solely as a technical service because control over data, infrastructures, providers, and jurisdictions is embedded in broader questions of sovereignty and transnational power [10]. In the context of the present study, geopolitical and competitive risk included sanctions-related exclusion from global cloud services, regional cyber threats, supply-chain restrictions affecting data centers, and the possibility of falling behind international competitors. These exposures may therefore become closely intertwined with compatibility problems, financial costs, and organizational dependence on domestic providers. Yau-Yeung et al. similarly identified vendor dependence, integration problems, data location, service reliability, and legal uncertainty as important cloud accounting risks, demonstrating that practitioners consider a considerably broader range of risks than data security alone [5]. Tejari et al. also emphasized the need for multidimensional strategies to mitigate cloud accounting risks, reinforcing the argument that effective risk management requires coordinated responses across technological, managerial, legal, and organizational domains [11].

The relatively lower loading of security and data risk should not be interpreted as evidence that users considered this dimension unimportant. The mean score for security and data risk was 3.15, placing it close to the means of the other six dimensions and approximately in the middle of the ranking based on perceived risk levels. Rather, its lower loading means that variation in security-risk perceptions corresponded less closely with variation in the overall latent risk construct than did several other dimensions. Risk perception theory offers a useful explanation for this result. Individuals evaluate hazards not only according to their probability or technical consequences but also according to familiarity, perceived control, uncertainty, dread, and the extent to which responsibility is attributed to others [12]. Later work has likewise demonstrated that risk judgments depend substantially on the institutional and experiential context in which hazards are evaluated [13]. Financial personnel

and auditors may regard cybersecurity as a specialized responsibility of cloud providers and IT departments, whereas risks related to system incompatibility, reporting constraints, sanctions, vendor dependence, or regulatory disruptions may be experienced more directly in daily work. This explanation also aligns with evidence showing that expert and non-expert groups may prioritize the same risk set differently because they use different frames of reference and possess different forms of exposure [14].

The finding that security risk did not occupy the same position among users as among experts is therefore one of the most theoretically important results of the study. The rank correlation between the expert ordering and the loading-based ordering of users was close to zero and statistically non-significant; the same general pattern remained when expert Delphi weights were compared with users' mean scores, with a negative and non-significant correlation. This result supports the proposition that expert consensus and user perception represent different forms of evidence. Experts may evaluate cloud accounting risks according to technical knowledge, professional standards, anticipated consequences, or abstract judgments of severity, whereas system users may evaluate risk through repeated exposure to operational failures, institutional constraints, practical workarounds, and organizational consequences. Slovic's foundational work demonstrated that experts and other stakeholders often differ in their ordering of hazards because they emphasize different risk characteristics [12]. Siegrist et al. likewise showed that expert and public risk prioritization can diverge even when groups consider the same set of hazards [14]. The present findings extend this principle into the domain of cloud accounting by suggesting that an expert-derived taxonomy may successfully identify the relevant dimensions of risk without necessarily reproducing the relative structure that emerges from user experience.

The comparison between financial staff and independent auditors produced a different result: rather than diverging, the two professional groups showed strikingly similar perceptions. Their overall perceived risk levels did not differ significantly, with $t = 0.173$, $p = 0.863$ and an effect size of $d = 0.03$, while the maximum difference between corresponding factor loadings was only 0.018. Their loading rankings were also strongly associated, with Spearman's $\rho = 0.93$ and Kendall's $\tau = 0.81$. This result was contrary to the expectation that auditors would place greater emphasis on reporting, compliance, audit trail, and evidence-related issues, whereas financial staff would attach greater weight to operational, technological, and human concerns. The absence of such differences suggests that role-based distinctions may be less important than shared professional knowledge and shared exposure to the same institutional environment.

This interpretation is consistent with Gonthier-Besacier et al., who found that perceptions of audit quality did not simply divide along auditor-versus-preparer lines and suggested that expertise and shared professional values could reduce role-perception differences [15]. Financial staff and independent auditors working with petrochemical companies in Mahshahr operate within a common regulatory, technological, and geopolitical environment and are exposed to many of the same constraints on systems, data access, reporting, and service continuity. Consequently, differences in formal organizational position may be outweighed by common environmental pressures. External auditors may also develop extensive familiarity with the operational systems of recurring clients, while financial personnel may become highly aware of audit and compliance requirements through repeated interaction with auditors. The resulting professional convergence could explain why the two groups exhibited almost identical loading structures and overall risk evaluations.

The convergence between auditors and financial staff is also understandable in light of the assurance challenges created by cloud accounting. Under ISAE 3402, organizations and their auditors may rely on assurance reports concerning controls at service organizations, particularly where outsourced processing affects financial reporting

[9]. When such assurance is limited or unavailable, auditors must devote greater attention to client-side controls, system interfaces, audit trails, provider arrangements, and alternative sources of evidence. Simultaneously, financial personnel must ensure that the same systems permit reliable processing, reporting, regulatory submission, and data retrieval. Thus, both groups may encounter the consequences of service-provider controls in different professional functions but ultimately perceive similar sources of vulnerability. Yigitbasioglu's study of external auditors similarly showed that auditors' concerns about cloud adoption encompass data confidentiality, provider reliability, data location, and control-related issues rather than being confined to traditional audit procedures [6].

The results also carry implications for the growing integration of continuous auditing, artificial intelligence, and anomaly detection into cloud accounting. Kitsantas et al. demonstrated that cloud accounting can support continuous auditing and automated anomaly detection, potentially improving the timeliness and scope of assurance [8]. However, such benefits presuppose stable connectivity, interoperable systems, reliable data, and continuous access to the accounting environment. The high loadings observed for compatibility and technology and for geopolitical and competitive risk suggest that these enabling conditions may themselves constitute important sources of vulnerability. Automated assurance tools cannot compensate fully for fragmented system architectures, restrictions on access to providers, unstable infrastructures, or inadequate integration with legacy systems. Consequently, technological advancement in auditing should be accompanied by broader attention to system architecture, continuity, provider dependence, and environmental constraints.

Methodologically, the results support the usefulness of PLS-SEM for assessing the multidimensional structure of cloud accounting risk, particularly given the complexity of the 82-item instrument and the moderate size of the two groups. Guidance on PLS-SEM emphasizes its suitability for complex latent-variable models and its capacity to estimate higher-order constructs under conditions in which conventional distributional assumptions may not be satisfied [21, 22]. The significant loadings and acceptable reliability and convergent validity reported for the constructs provide preliminary support for the measurement framework. T article Heydari bmf Nevertheless, the exploratory two-tier pattern should not be treated as definitive evidence of substantive hierarchy because repeated-indicator higher-order models can be affected by unequal numbers of indicators across first-order constructs [19]. The interpretation of higher-order structures also depends on careful specification of reflective and formative relationships [18, 20]. Accordingly, the most defensible conclusion is that the seven dimensions are empirically supported as components of overall perceived cloud accounting risk, while their precise relative structure requires further confirmation.

Overall, the study suggests that cloud accounting risk in a sanctions-affected strategic industry is both multidimensional and context-sensitive. Expert consensus successfully identified dimensions that were validated among system users, but expert prioritization did not correspond closely to the way financial staff and auditors structured or ranked those dimensions. At the same time, internal and external professional users showed substantial convergence in their perceptions. These findings extend the cloud accounting literature by connecting technological and accounting risk research with risk perception theory and by demonstrating that identifying a risk domain and understanding how that domain is perceived in practice are related but distinct analytical tasks. They also reinforce the argument emerging from systematic reviews that future cloud accounting research should move beyond adoption intentions and performance benefits toward more sophisticated analyses of governance, risk, professional judgment, and contextual variation [1, 4].

Several limitations should be considered when interpreting the findings. First, the exploratory division of the seven dimensions into two loading clusters was identified after observing the results and was not subjected to a

formal statistical test; it should therefore be interpreted as a provisional pattern rather than a confirmed latent structure. Second, the seven dimensions contained unequal numbers of questionnaire items, ranging from 10 to 15, and the repeated-indicators approach may have influenced second-order loading estimates. Some questionnaire items also overlapped conceptually across dimensions, and two items were effectively duplicated, which may have increased correlations among constructs. Third, the study relied on a cross-sectional, single-instrument survey and did not formally assess common method bias or discriminant validity. The comparison between financial staff and auditors was descriptive, and no measurement invariance assessment or formal multigroup analysis was conducted. Fourth, convenience sampling limits generalizability, while respondents may have been nested within the same companies or audit firms and thus not statistically independent. Finally, the study was confined to one petrochemical zone, one national and regulatory context, and one point in time, and the measures captured professional perceptions rather than objectively recorded cloud-related incidents or losses.

Future studies should refine and retest the measurement instrument using item-level confirmatory analysis and should examine whether the proposed two-cluster pattern is reproduced in independent samples. Researchers could reassess item classification, remove duplicated or cross-loading indicators, balance the number of indicators across dimensions, and compare reflective, formative, and alternative higher-order specifications. Formal measurement invariance procedures and multigroup analysis should be used before drawing stronger conclusions regarding differences or similarities between financial staff, auditors, IT personnel, managers, regulators, and service providers. Longitudinal research would also help determine whether risk perceptions change after major technological disruptions, regulatory reforms, sanctions changes, cyber incidents, or organizational cloud migration. Multi-industry and cross-country studies could establish whether the strong influence of geopolitical, compatibility, and economic dimensions is specific to sanctions-affected petrochemical firms or generalizes to other strategic sectors. Future research could also combine survey data with objective indicators such as outage frequency, audit adjustments, cybersecurity incidents, reporting delays, compliance violations, switching costs, and recovery expenditures, thereby linking perceived risk to observable operational and financial outcomes.

For practice, petrochemical companies should adopt a broad cloud accounting risk-management framework that gives comparable attention to technological compatibility, provider dependence, service continuity, economic exposure, regulatory compliance, human capabilities, geopolitical vulnerability, and information security. Risk assessments should combine expert evaluations with structured input from financial staff, auditors, and other system users because the groups responsible for day-to-day operation may identify patterns that are not reflected in expert priority rankings. Organizations should strengthen integration testing before migration, maintain offline and independent backups, establish tested exit and data-portability arrangements, assess concentration risk associated with dependence on a single provider, and develop continuity plans for internet, power, hardware, and provider disruptions. Contracts with cloud providers should clearly define data ownership, recovery obligations, audit access, service-level expectations, security responsibilities, incident notification, and termination procedures. Audit planning should explicitly address interface completeness, continuity of the audit trail, data transfer between systems, provider-side controls, and the availability of alternative evidence when direct access is restricted. Finally, organizations should invest in recurring cloud-risk training for financial personnel, auditors, managers, and governance bodies so that cloud accounting is treated as an enterprise-wide financial reporting and risk-management issue rather than merely an IT implementation project.

Authors' Contributions

Authors equally contributed to this article.

Ethical Considerations

All procedures performed in this study were under the ethical standards.

Acknowledgments

Authors thank all participants who participate in this study.

Conflict of Interest

The authors report no conflict of interest.

Funding/Financial Support

According to the authors, this article has no financial support.

References

- [1] D. Vo Van, M. Abu Afifa, P. Nguyen, and T. Van Bui, "Cloud accounting: A systematic literature review," *Global Knowledge, Memory and Communication*, vol. 74, no. 7/8, pp. 4173-4195, 2025, doi: 10.1108/GKMC-04-2024-0246.
- [2] M. Al-Okaily, A. F. Alkhwalidi, A. A. Abdulmuhsin, H. Alqudah, and A. Al-Okaily, "Cloud-based accounting information systems usage and its impact on Jordanian SMEs' performance: The post-COVID-19 perspective," *Journal of Financial Reporting and Accounting*, vol. 21, no. 1, pp. 126-155, 2023, doi: 10.1108/JFRA-12-2021-0476.
- [3] O. I. Tawfik, O. Durrah, K. Hussainey, and H. E. Elmaasrawy, "Factors influencing the implementation of cloud accounting: Evidence from small and medium enterprises in Oman," *Journal of Science and Technology Policy Management*, vol. 14, no. 5, pp. 859-884, 2023, doi: 10.1108/JSTPM-08-2021-0114.
- [4] B. Septiawan, N. S. Mohamed, N. Zakaria, and S. Hermawan, "A systematic review of cloud accounting adoption in SMEs: A thematic synthesis of factors, impacts, and research directions," *Asia-Pacific Management Accounting Journal*, vol. 20, no. 3, pp. 115-148, 2025, doi: 10.24191/apmaj.v20i3.05.
- [5] D. Yau-Yeung, O. Yigitbasioglu, and P. Green, "Cloud accounting risks and mitigation strategies: Evidence from Australia," *Accounting Forum*, vol. 44, no. 4, pp. 421-446, 2020, doi: 10.1080/01559982.2020.1783047.
- [6] O. M. Yigitbasioglu, "External auditors' perceptions of cloud computing adoption in Australia," *International Journal of Accounting Information Systems*, vol. 18, pp. 46-62, 2015, doi: 10.1016/j.accinf.2015.09.001.
- [7] C. Committee of Sponsoring Organizations of the Treadway, "Enterprise Risk Management for Cloud Computing," COSO, 2021. [Online]. Available: <https://www.coso.org/erm-cloud-computing>
- [8] T. Kitsantas, M. Sarris, and E. Chytis, "Continuous auditing, artificial intelligence and anomaly detection in cloud accounting information systems," *Journal of Financial Crime*, vol. 30, no. 5, pp. 1256-1271, 2023, doi: 10.1108/JFC-08-2022-0205.
- [9] *International Standard on Assurance Engagements (ISAE) 3402: Assurance Reports on Controls at a Service Organization*, A. International and B. Assurance Standards, New York, NY, USA, 2011.
- [10] M. Tang, "The challenge of the cloud: Between transnational capitalism and data sovereignty," *Information, Communication & Society*, 2022, doi: 10.1080/1369118X.2022.2128598.
- [11] S. Tejari, A. Khozin, M. Ashrafi, and J. Gorganli Doji, "Cloud computing in the accounting profession: Designing a model of strategies for mitigating cloud accounting risks," (in Persian), *Accounting and Management Auditing Knowledge*, vol. 14, no. 54, pp. 331-346, 2025. [Online]. Available: https://www.jmaak.ir/article_23583.html.
- [12] P. Slovic, "Perception of risk," *Science*, vol. 236, no. 4799, pp. 280-285, 1987, doi: 10.1126/science.3563507.
- [13] M. Siegrist and J. Árvai, "Risk perception: Reflections on 40 years of research," *Risk Analysis*, vol. 40, no. S1, pp. 2191-2206, 2020, doi: 10.1111/risa.13599.
- [14] M. Siegrist, P. Hübner, and C. Hartmann, "Risk prioritization in the food domain using deliberative and survey methods: Differences between experts and laypeople," *Risk Analysis*, vol. 38, no. 3, pp. 504-524, 2018, doi: 10.1111/risa.12857.
- [15] N. Gonthier-Besacier, G. Hottegindre, and S. Fine-Falcy, "Audit quality perception: Beyond the 'role-perception gap'," *International Journal of Auditing*, vol. 20, no. 2, pp. 186-201, 2016, doi: 10.1111/ijau.12066.
- [16] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77-101, 2006, doi: 10.1191/1478088706qp063oa.

- [17] C. H. Cheng and Y. Lin, "Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation," *European Journal of Operational Research*, vol. 142, no. 1, pp. 174-186, 2002, doi: 10.1016/S0377-2217(01)00280-6.
- [18] C. B. Jarvis, S. B. MacKenzie, and P. M. Podsakoff, "A critical review of construct indicators and measurement model misspecification in marketing and consumer research," *Journal of Consumer Research*, vol. 30, no. 2, pp. 199-218, 2003, doi: 10.1086/376806.
- [19] J. M. Becker, K. Klein, and M. Wetzels, "Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models," *Long Range Planning*, vol. 45, no. 5-6, pp. 359-394, 2012, doi: 10.1016/j.lrp.2012.10.001.
- [20] M. Sarstedt, J. F. Hair, J. H. Cheah, J. M. Becker, and C. M. Ringle, "How to specify, estimate, and validate higher-order constructs in PLS-SEM," *Australasian Marketing Journal*, vol. 27, no. 3, pp. 197-211, 2019, doi: 10.1016/j.ausmj.2019.05.003.
- [21] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review*, vol. 31, no. 1, pp. 2-24, 2019, doi: 10.1108/EBR-11-2018-0203.
- [22] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, 3 ed. Thousand Oaks, CA, USA: Sage, 2022.