Economics
2026, Vol. 15, No. 3, pp. 58–69
https://doi.org/10.11648/j.eco.20261503.11

SciencePG
Science Publishing Group

Research Article

Cybersecurity Challenges in AI - Integrated Accounting and Auditing Systems: Empirical Evidence from Vietnam

Huong Nguyen Thi Mai*

Faculty of Accounting - Auditing, Ho Chi Minh Banking University, Ho Chi Minh City, Viet Nam

Abstract

The rapid proliferation of artificial intelligence (AI) and digital transformation technologies in the Vietnamese business environment has profoundly altered the landscape of accounting and auditing, simultaneously introducing new and complex information security challenges. This study applies the Technology-Organization-Environment (TOE) framework to examine factors affecting Accounting Information Security (AISe) in Vietnamese enterprises during the ongoing digital transformation. The research model integrates four independent variables — Senior Management Support (TMS), Information Security Culture (SC), Quality of Accounting Information Systems (QAIS), and Cybersecurity Readiness (CSR) — and constructs the dependent variable AISe as a second-order formative construct encompassing three dimensions of the CIA triad: Confidentiality (CISe), Integrity (IISe), and Availability (AvISe). Using Partial Least Squares Structural Equation Modeling (PLS-SEM) with SmartPLS 4.0, the study analyzed data collected from 228 respondents across Vietnamese enterprises. Results show that QAIS exerts the strongest positive influence on AISe ($\beta = 0.570$, $p < 0.001$), followed by SC ($\beta = 0.152$, $p = 0.047$) and CSR ($\beta = 0.151$, $p = 0.046$). TMS does not directly affect AISe but exerts a strong indirect effect through SC ($\beta = 0.777$, $p < 0.001$). The model explains 69.4% of variance in AISe ($R^2 = 0.694$). These findings offer empirical evidence supporting the integrated role of technological and organizational factors in securing accounting information within Vietnam's developing digital economy. Recent developments in AI governance, including Resolution No. 57-NQ/TW (2024) and Vietnam's national AI transformation strategy (2025-2026), further underscore the urgency of these findings for policy and practice.

Keywords

Artificial Intelligence, Accounting Information Security, Intelligent Accounting, Audit Automation, Emerging Economies, Vietnamese Enterprises, TOE Framework, Cybersecurity

1. Introduction

The digital transformation of business organizations represents one of the most consequential economic and technological developments of the early twenty-first century. At its core, digital transformation reshapes enterprises through the strategic integration of digital technologies, leading to fundamental changes in the way they operate and deliver value to customers. According to [65], digital transformation is "a process in which organizations change the way they create value for customers through the use of digital technology," emphasizing that it involves not merely technological adoption but a fundamental shift in strategy and organizational structure. Tang

*Correspondence: Huong Nguyen Thi Mai (huongntm@hub.edu.vn)

Received: 5 June 2026; **Accepted:** 22 June 2026; **Published:** 8 July 2026

(2021) [60] further characterizes digital transformation as a comprehensive business restructuring process that simultaneously increases revenue and reduces costs by optimizing processes and resources.

With the rapid rise of artificial intelligence (AI), this transformation is driven by increased operational efficiency, service innovation, and radical redefinitions of customer experience. From an accounting perspective, Izzo et al. (2021) [35] argue that digital transformation supports continuous accounting, thereby enhancing transparency, reliability, and the timeliness of financial decision-making. Rehm (2022) [55] further emphasizes that digital transformation necessitates a fundamental rethinking of accounting information systems, in which the traditional linear chain linking strategy, structure, and systems must become more flexible and adaptive [12]. Busulwa and Evans (2022) [16] observe that technologies such as drones, computer vision, cloud computing, and AI have automated many traditional accounting tasks - from inventory counting to complex data analysis — effectively shifting the accountant's role from "record keeper" to "strategic advisor."

In Vietnam, digital transformation has accelerated dramatically since the issuance of Resolution No. 57-NQ/TW of December 22, 2024, which identifies science, technology, innovation, and national digital transformation as key drivers for rapid and sustainable national development through 2030, with a vision extending to 2045. Building on this foundation, Vietnam has in 2025 articulated a national AI transformation strategy (AIX), positioning the country at the forefront of AI adoption in Southeast Asia [45, 67]. These developments, combined with the rapid digitalization of financial services, e-commerce, and public administration, create both significant opportunities and heightened security risks for accounting and auditing systems.

The digital transformation process simultaneously poses significant information security challenges. When accounting data is stored and processed on digital platforms such as cloud environments, IoT systems, or mobile applications, the risks of data leakage, unauthorized access, and cyberattack increase substantially [55]. Reports by Viettel Cyber Security [66], VNISA [69], and the Vietnam National Cyber Security report [68] confirm that cyberattacks targeting Vietnamese enterprises have grown in frequency and sophistication, with financial and accounting data among the primary targets. This makes Accounting Information Security (AISe) - defined as the protection of accounting information to ensure its confidentiality, integrity, and availability - a matter of critical strategic importance for Vietnamese enterprises operating in an AI-driven digital economy.

Despite the practical urgency of this issue, empirical research on AISe specifically within the Vietnamese context remains limited. Most existing studies focus on technology adoption or general information systems quality without systematically examining the multi-dimensional determinants of accounting information security under the CIA framework. This study addresses that gap by applying the TOE framework to investigate how technological factors (QAIS, CSR) and organizational factors (TMS, SC) jointly determine AISe in Vietnamese enterprises, contributing new empirical evidence to the growing body of literature on accounting security in developing economies.

2. Theoretical Background

2.1. Accounting Information Security

Accounting Information Security (AISe) is an essential element of information systems management, particularly in the context of the current rapid digital transformation. According to [34], information security is defined as the process of protecting information from threats in order to ensure three core attributes — commonly referred to as the CIA triad:

(i) Confidentiality: Ensuring that information is accessible only to authorized individuals and systems;

(ii) Integrity: Ensuring that information is not illegally modified, falsified, or corrupted; and

(iii) Availability: Ensuring that information can be accessed and used by authorized parties whenever required [34].

These three dimensions provide a comprehensive and enduring framework for evaluating information security performance. Alhassan and Adjei-Quaye (2017) [5] define information security broadly as "the practice of protecting information from unauthorized access, use, disclosure, disruption, modification, review, recording, or destruction," with the CIA principles operationalizing these protections in practice. Bishop (2019) [13] further confirms the centrality of the CIA model in academic and applied cybersecurity research.

In the accounting field specifically, information systems store large volumes of sensitive financial data, making security a vital organizational concern. Haapamäki and Sihvonen (2019) [28] emphasize that cybersecurity has become a top priority in the global digital accounting environment, a view reinforced by the American Institute of Certified Public Accountants (AICPA), which recommends that enterprises develop cybersecurity risk management programs to protect accounting information. Steinbart et al. (2018) [59] demonstrate that risks from cybercrime can cause significant financial losses, disrupt operations, and undermine the reliability of financial reporting. Similarly, Abutaber (2023) [3] confirms that accounting information system security directly enhances financial information reliability in organizational settings.

Recent research has further expanded the conceptualization of AISe in the context of AI-driven environments. Rehberger (2024) [54] documents how prompt injection attacks in large language model (LLM) systems directly threaten all three CIA dimensions, representing a novel category of risk for AI-integrated accounting systems. Similarly, the Accenture State of Cybersecurity Resilience Report [2] finds that a majority of organizations across Asia and Europe still lack the foundational data and AI security practices necessary to safeguard

critical models, data pipelines, and cloud infrastructure — underscoring the continuing relevance of CIA-based security frameworks in the age of AI.

In summary, for the purposes of this study, AISe is understood as the process of protecting accounting information through technological measures, human practices, and management processes, to ensure Confidentiality (CISe), Integrity (IISe), and Availability (AvISe) of information in the context of digital transformation. This is not only a legal requirement under Vietnamese law (Accounting Law No. 8/2015/QH13 [46]; Law on Network Information Security No. 86/2015/QH13 [26]; Decree No. 64/2007/ND-CP on IT application in state agencies [25]) but also a core strategic capability for organizations seeking to maintain the reliability of financial reporting and competitive advantage in the digital economy.

2.2. The Technology - Organization - Environment Framework

The Technology - Organization - Environment (TOE) framework, developed by Tornatzky and Fleischer [61], is a widely applied theoretical model for explaining how organizations adopt and implement technological innovations. The framework posits that organizational decision-making with respect to technology adoption is influenced by three contextual dimensions:

1) Technology context: Characteristics of both existing and emerging technologies relevant to the firm, including infrastructure, compatibility, and complexity;
2) Organization context: Internal organizational attributes including size, managerial structure, available resources, human capital, and organizational culture;
3) Environment context: External factors in which the firm operates, including industry characteristics, competitive pressure, regulatory requirements, and government policy.

Oliveira and Martins (2011) [49] and Baker (2012) [9] confirmed TOE as a reliable and widely applicable framework for studying organizational technology innovation. The framework has been applied across diverse domains including e-commerce, ERP systems, cloud computing, and information security [4, 15, 19]. Kim and Kim (2021) [38] used TOE to assess continuity of corporate information security management, and Marei (2024) [43] recently applied TOE to examine cybersecurity's moderating role in e-accounting adoption, further validating its utility in accounting security research.

Von Solms and Von Solms (2006) [53] provide a foundational governance framework linking strategic security oversight to operational security outcomes, a perspective that aligns well with the TOE theoretical lens of this study. In the present study, TOE serves as the primary theoretical lens for explaining how accounting information security is determined by the combined influence of technological capabilities (QAIS and CSR), organizational commitment (TMS), and internal cultural environment (SC). This four-factor model maps onto TOE as follows: QAIS and CSR represent the technology context; SC represents the organizational cultural environment; and TMS represents the organizational leadership and resource allocation dimension. This integrated application of TOE contributes to extending the framework's explanatory scope in the emerging area of accounting security research in developing economies.

2.3. Research Hypotheses Development

Based on the TOE framework and a synthesis of prior empirical studies, this research develops five hypotheses regarding the determinants of AISe.

2.3.1. Senior Management Support (TMS)

Senior management support is widely recognized as a critical organizational factor in shaping information security outcomes. According to [37], senior management has strong potential to influence employee behavior and awareness by promoting information security values and encouraging compliance with security policies. Whitman and Mattord (2018) [70] emphasize that an IT security strategy is only truly effective when it receives substantial participation from organizational leadership - from policy formulation to implementation monitoring.

Empirical evidence from [40, 57-59, 63] consistently confirms the decisive role of TMS in enhancing the effectiveness of information security policies, particularly through resource provision, monitoring mechanisms, and organizational culture-shaping behaviors. AlGhamdi et al. (2020) [7] further demonstrate that top management involvement positively moderates the relationship between security infrastructure and security outcomes. Dutta and McCrohan (2002) [22] similarly emphasize that management commitment to information security governance is foundational to effective security outcomes in cyber-enabled business environments.

In the Vietnamese context, Resolution No. 57-NQ/TW (2024) explicitly assigns leadership at all organizational levels a central responsibility for digital transformation and data security governance. Given these considerations, the following hypotheses are proposed:

H1: Senior Management Support has a positive impact on Accounting Information Security in Vietnamese enterprises.

H2: Senior Management Support has a positive impact on Accounting Information Security Culture in Vietnamese enterprises.

2.3.2. Information Security Culture (SC)

Information security culture in accounting is understood as the set of values, perceptions, beliefs, and behavioral norms within an organization that collectively govern how employees approach the protection of accounting information. Knapp et al. (2006) [39] established that the maturity of information

security culture depends directly on organizational commitment and employee attitudes. Cameron and Quinn (2011) [17] emphasize that organizational culture guides behavior and reinforces control systems, while Cram et al. (2021) [31] demonstrates that safety culture is grounded not only in formal control systems but also in internal commitment at all levels of the hierarchy.

Van Niekerk and Von Solms (2010) [64] developed an information security culture model showing that data protection behavior results from awareness shaped by the organizational environment. Chang and Lin (2007) [18] further demonstrate that organizational culture serves as a primary determinant of effective information security management practices. Solomon and Brown (2021) [56] confirm that both organizational culture and information security culture independently and jointly influence employee compliance behavior. In the context of digital transformation, where increasingly complex technological environments amplify human behavioral risks [44], a robust security culture is indispensable. Pham Tra Lam (2024) [52], examining information security culture in Vietnamese AIS contexts, further confirms that cultural dimensions are critical determinants of accounting data protection behavior. Abu Afifa et al. (2025) [1], in a recent study of Vietnamese manufacturing firms, underscore that transformational leadership - closely aligned with strong management support - significantly promotes positive attitudes toward AI adoption and digital security in accounting.

H3: Information Security Culture has a positive impact on Accounting Information Security in Vietnamese enterprises.

2.3.3. Quality of Accounting Information Systems (QAIS)

The quality of accounting information systems reflects the extent to which systems effectively meet requirements for processing, storing, and protecting financial information. Drawing on the Resource-Based View [10, 71], high-quality accounting information systems that are valuable, rare, inimitable, and non-substitutable can generate sustainable competitive advantage in the digital economy. [23, 24] assess AIS quality across three dimensions: system quality (reliability, processing capability, and security), information quality (accuracy, completeness, and decision-support capacity), and service quality (technical support and user satisfaction).

Papiorek and Hiebl (2023) [50] demonstrate that information systems quality significantly enhances management accounting and management control effectiveness. Vietnamese empirical studies corroborate this pattern: Dong Quang Chung (2023) and Tran Nu Hoai Nhu (2024) [21, 62] find that AIS quality plays an intermediary role in mitigating the negative effects of IT risks on accounting information quality and reliability. Nguyen and Vo (2025) [48] further demonstrate that management accounting information systems positively affect competitive advantage and business performance in Vietnamese enterprises, with digital transformation moderating these relationships.

H4: The Quality of Accounting Information Systems has a positive impact on Accounting Information Security in Vietnamese enterprises.

2.3.4. Cybersecurity Readiness (CSR)

Cybersecurity Readiness reflects an organization's preparedness to prevent, detect, and respond to cybersecurity threats — integrating technological capabilities, organizational resources, human awareness, and behavioral compliance. In accounting environments characterized by multi-layered digital platforms such as cloud ERP, distributed systems, and AI-driven analytics, CSR serves as the frontline defense against data corruption, unauthorized access, and information leakage.

Kraemer et al. (2009) [42] identify that human and organizational factors represent a key pathway to information security vulnerabilities, underscoring the need for comprehensive readiness programs. Daud et al. (2018) [20] emphasize that technological investment in cybersecurity must be accompanied by employee training and awareness-building, while Alshaikh and Adamson (2021) [8] find that organizations with a strong security culture consistently outperform others in implementing cybersecurity measures. Hasan et al. (2021) [32] demonstrate that organizations with high readiness outperform counterparts in incident prevention and response. More recently, the World Economic Forum's Global Cybersecurity Outlook 2025 [73] indicates that organizations across Asia and Europe continue to face significant readiness gaps, particularly in the context of AI-enabled threats — findings that are directly relevant to Vietnamese enterprises undergoing rapid AI integration.

Peltier (2016) [47] specifies that an organization achieves high Cybersecurity Readiness when it demonstrates: a periodic risk assessment system, a clear incident response plan, regular employee training, application of encryption and access control technologies, and continuous monitoring of information systems. These specifications reinforce the theoretical basis for CSR as a determinant of AISe within the TOE framework.

H5: Cybersecurity Readiness has a positive impact on Accounting Information Security in Vietnamese enterprises.

3. Materials and Methods

3.1. Research Model

Based on the theoretical foundations of the TOE framework, inherited research instruments, and the practical context of Vietnamese enterprises during the digital transformation period, the study proposes the following research model with four independent factors and one second-order dependent variable.

Table 1. Theoretical basis for the research model.

No.	Factor	Abbreviation	Source
1	Information Security Culture	SC	Hamdan (2017); TOE Framework
2	Senior Management Support	TMS	Knapp et al. (2006); TOE Framework
3	Quality of Accounting Information Systems	QAIS / AIS	Papiorek & Hiebl (2023); TOE Framework
4	Cybersecurity Readiness	CSR	Berlilana et al. (2021); TOE Framework

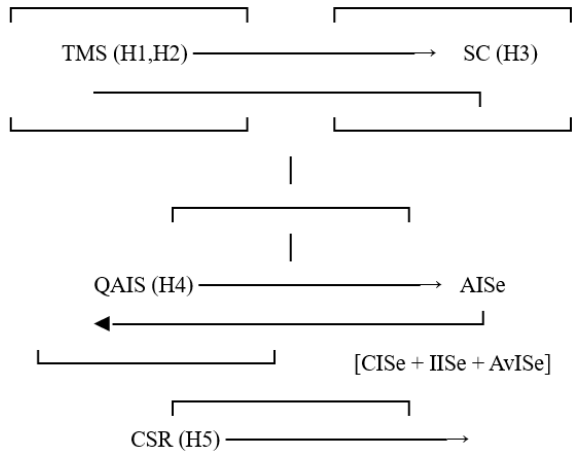

Figure 1. Research Model — Determinants of Accounting Information Security (AISe).

Note: Solid arrows (→) represent hypothesized direct paths; AISe is a second-order formative construct comprising Confidentiality (CISe), Integrity (IISe), and Availability (AvISe). TMS also has a direct path to AISe (H1). H2 represents the TMS→SC mediation pathway.

3.2. Research Methodology

3.2.1. Survey Design and Sampling

This study employs a quantitative research design using a structured questionnaire based on a five-point Likert scale, ranging from (1) Strongly Disagree to (5) Strongly Agree, to measure respondents' assessments of the latent constructs in the model. The variables include: Senior Management Support (TMS), Information Security Culture (SC), Accounting Information System Quality (QAIS/AIS), Cybersecurity Readiness (CSR), and Accounting Information Security (AISe). All scales were adapted from validated instruments in prior studies and adjusted to suit the Vietnamese enterprise context.

Survey subjects were individuals with knowledge and professional experience in accounting, auditing, information technology, or senior management (CEO, CFO) at enterprises operating in Vietnam. These respondents were selected for their ability to objectively assess factors related to accounting information systems, security policies, and cybersecurity readiness. The survey was administered through both online and direct (face-to-face) channels.

According to [29], when using PLS-SEM, the minimum sample size should be at least 10 times the number of observed variables belonging to the construct with the most indicators. In this study, the largest construct (AISe) has 15 observed variables, yielding a minimum required sample of 150. To further ensure statistical representativeness, the study also applied the probability-based sample size formula for large populations at a 95% confidence level and 5% margin of error ($Z = 1.96$; $p = 0.5$; $E = 0.05$), yielding $N = 384$. The final usable sample comprised 228 valid responses (response rate: 59.4%), exceeding the PLS-SEM minimum threshold of 150 and providing an adequate basis for robust statistical inference.

3.2.2. Measurement Instruments

The TMS scale (6 items) was adapted from [39], with subsequent validation by [6, 27, 33, 63]. The SC scale (7 items) was inherited and adapted from [31], drawing on [14, 51, 72]. The QAIS scale (6 items) was derived from [50], originally developed by [41], focusing on processing speed, flexibility, integration, and data quality. The CSR scale (9 items) was adapted from [11], covering three dimensions: technological capacity, organizational resources, and external environmental interaction. The AISe scale (15 items) was inherited from [36], capturing confidentiality (5 items), integrity (6 items), and availability (4 items) in line with the CIA model.

3.2.3. Analytical Method

The study employs Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS 4.0 software for three primary reasons. First, the research model incorporates both reflective and formative measurement relationships; specifically, AISe is a second-order formative variable comprising three first-order reflective sub-constructs (CISe, IISe, AvISe). PLS-SEM is specifically suited to this reflective-formative structure, whereas Covariance-Based SEM (CB-SEM) is restricted to reflective models [29, 30]. Second, PLS-SEM does not require data to follow a normal distribution, which is appropriate for data collected from organizational surveys in developing economies. Third, the sample

size of 228 is fully adequate for PLS-SEM requirements while falling below the threshold (> 200) typically recommended for CB-SEM. A Two-Stage Approach is employed for the second-order construct AISe, as recommended by [30].

3.2.4. Sample Characteristics

Table 2. Profile of surveyed enterprises (N = 228).

Classification	Frequency	Percentage (%)
Type of Enterprise	228	
State-owned enterprise	130	57%
Private enterprise	17	7%
Limited liability company	44	19%
Joint stock company	26	11%
Foreign-invested enterprise (FDI)	11	5%
Enterprise Size	228	
Micro (fewer than 10 employees)	9	4%
Small (10-100 employees)	99	43%
Medium (100-200 employees)	41	18%
Large (more than 200 employees)	79	35%
Digital Transformation Status	228	
Partially applying digital technology	163	71%
Comprehensive digital transformation	65	29%

Source: Data extracted from SmartPLS 4.0

4. Results

4.1. Measurement Model Evaluation: Dependent Variable Sub-constructs

In the first stage of the Two-Stage Approach, the measurement model was evaluated for the three first-order reflective constructs of AISe: Confidentiality (CISe), Integrity (IISe), and Availability (AvISe). Cronbach's Alpha and Composite Reliability (CR) coefficients for all three constructs exceeded 0.86, indicating high internal consistency (see Table 3). Average Variance Extracted (AVE) values all exceeded the 0.70 threshold, confirming strong convergent validity. All outer loadings exceeded 0.81, demonstrating that each indicator reflects its intended construct well.

Table 3. Reliability and convergent validity — CISe, IISe, AvISe.

Construct	Cronbach's Alpha	CR (rho_a)	CR (rho_c)	AVE
AvISe	0.865	0.866	0.908	0.712
CISe	0.928	0.928	0.945	0.776
IISe	0.941	0.941	0.953	0.773

Source: Data extracted from SmartPLS 4.0

Discriminant validity was assessed using the Heterotrait-Monotrait Ratio (HTMT). Two out of three concept pairs had HTMT < 0.90. The IISe-AvISe pair yielded HTMT = 0.928, marginally exceeding the 0.90 threshold; however, following the recommendation of [30], this is acceptable in second-order models where component constructs share a strong theoretical basis (the CIA triad). After bootstrapping, all 95% HTMT confidence intervals fell below 1.0, confirming discriminant validity according to the criterion of Garson (2016).

4.2. Measurement Model Evaluation: Independent Variables

All four independent variables (TMS, SC, QAIS/AIS, CSR) demonstrated strong reliability and convergent validity. Cronbach's Alpha and CR exceeded 0.94 for all constructs; AVE ranged from 0.749 to 0.802. All outer loadings exceeded 0.70. HTMT values for all pairs of independent variables were below 0.85, satisfying the more conservative discriminant validity threshold of [30]. These results confirm that the measurement model is robust and appropriate for structural model testing.

Table 4. *Reliability and convergent validity - Independent variables.*

Variable	Cronbach's Alpha	CR (rho_a)	CR (rho_c)	AVE
AIS (QAIS)	0.942	0.943	0.954	0.775
CSR	0.968	0.969	0.973	0.799
SC	0.944	0.945	0.954	0.749
TMS	0.951	0.951	0.960	0.802

Source: Data extracted from SmartPLS 4.0

4.3. Structural Model Testing and Hypothesis Results

The structural model was evaluated using path coefficients and bootstrapping significance tests (5,000 subsamples), along with coefficients of determination (R^2), predictive relevance (Q^2), effect sizes (f^2), and multicollinearity diagnostics (VIF). Of the five proposed hypotheses, four were supported at the 5% significance level; one (H1: TMS → AISe) was not statistically supported.

Table 5. *Structural model path coefficients and hypothesis tests.*

Hypothesis / Path	β (Original)	β (Mean)	SD	T-stat	T-value
H4: AIS → AISe	0.570	0.571	0.067	8.539	0.000 ***
H5: CSR → AISe	0.151	0.151	0.076	1.994	0.046 *
H3: SC → AISe	0.152	0.152	0.076	1.989	0.047 *
H1: TMS → AISe	0.087	0.086	0.081	1.070	0.285 (ns)
H2: TMS → SC	0.777	0.776	0.048	16.255	0.000 ***

Source: Data extracted from SmartPLS 4.0.
Note: *** $p < 0.001$; * $p < 0.05$; ns = not significant.

The model demonstrates strong explanatory power for the central dependent variable AISe ($R^2 = 0.694$, adjusted $R^2 = 0.689$), which exceeds the threshold of 0.26 considered indicative of high explanatory power in social science research [30]. The mediating variable SC also shows strong explanatory power ($R^2 = 0.604$). The Q^2_predict value for AISe (0.667) and SC (0.600) both substantially exceed the minimum threshold of 0, confirming strong out-of-sample predictive relevance.

All VIF values remained below the threshold of 5.0, indicating no significant multicollinearity.

Effect size analysis (f^2) confirms that QAIS/AIS is the dominant determinant of AISe ($f^2 = 0.565$, large effect according to Cohen's (1988) benchmarks of 0.02/small, 0.15/medium, 0.35/large), while TMS exerts the largest effect on SC ($f^2 = 1.525$, a very large effect). CSR ($f^2 = 0.036$) and SC ($f^2 = 0.027$) both yield small but statistically significant effects on AISe, consistent with the complex, multi-determined nature of security outcomes in organizational settings.

5. Discussion

The empirical results of this study provide several theoretically and practically significant contributions to the understanding of accounting information security in the context of digital transformation in Vietnam. The five hypotheses were evaluated using PLS-SEM path analysis with bootstrapping (5,000 subsamples), with results interpreted against established benchmarks [29, 30].

First, the overwhelming dominance of QAIS in determining AISe ($\beta = 0.570$, $f^2 = 0.565$) underscores that the technical quality of accounting information systems is the single most important driver of security outcomes. This finding is consistent with [50], who demonstrate that well-designed information systems with high processing, integration, and data quality capabilities are foundational to effective management control. It further aligns with recent findings by [48] in the Vietnamese context, confirming that AIS quality is a strategic organizational resource. As Vietnamese enterprises accelerate AI adoption in accounting — as documented by [1] — investment in robust, high-quality AIS infrastructure becomes even more critical, since AI-powered systems introduce new attack surfaces including adversarial attacks, data poisoning, and model inversion [54].

Second, the significant but smaller impacts of SC ($\beta = 0.152$) and CSR ($\beta = 0.151$) highlight that organizational and behavioral factors complement technical safeguards. Security culture shapes voluntary compliance behavior [56], while cybersecurity readiness ensures that organizational responses to threats are timely and coordinated [32]. The Accenture State of Cybersecurity Resilience Report [2] estimates that more than 90% of organizations globally still fall short of full cybersecurity resilience, suggesting that Vietnamese enterprises have significant room to strengthen both dimensions.

Third, the finding that TMS does not directly affect AISe ($\beta = 0.087$, $p = 0.285$) but exerts a strong indirect effect through SC ($\beta = 0.777$, $p < 0.001$) is theoretically meaningful and novel. It implies that senior management influence on security outcomes is primarily channeled through the cultural and behavioral norms it shapes rather than through direct operational interventions. This is consistent with [39], who characterize security culture as the primary organizational mediator of leadership commitment. From a practical standpoint, this finding suggests that management training programs, security awareness campaigns, and visible leadership endorsement of security values may be more impactful than formal policy directives alone.

Fourth, these findings must be interpreted against Vietnam's rapidly evolving national AI governance landscape. Vietnam's Resolution No. 57-NQ/TW (2024) and its emerging national AI transformation strategy (AIX) (Vietnam Digital Transformation Program, 2025-2026) signal a government commitment to AI-driven economic development that will place additional demands on accounting security infrastructure. Organizations that proactively strengthen QAIS, cultivate a robust security culture, and develop comprehensive CSR will be best positioned to capitalize on AI-driven transformation while managing the associated security risks.

6. Conclusions

This study applies the TOE framework to empirically examine the determinants of Accounting Information Security (AISe) in Vietnamese enterprises during the digital transformation era, using PLS-SEM with data from 228 respondents. The key findings are:

1) H4 (QAIS → AISe): Supported. QAIS is the strongest determinant ($\beta = 0.570$, $p < 0.001$), confirming the primacy of technical system quality in securing accounting information.
2) H3 (SC → AISe): Supported. Information security culture has a positive effect on AISe ($\beta = 0.152$, $p = 0.047$), highlighting the importance of behavioral and cultural dimensions.
3) H5 (CSR → AISe): Supported. Cybersecurity readiness positively predicts AISe ($\beta = 0.151$, $p = 0.046$), consistent with the TOE technology context.
4) H2 (TMS → SC): Supported. Senior management support strongly shapes security culture ($\beta = 0.777$, $p < 0.001$), confirming TMS as an indirect organizational driver of AISe.
5) H1 (TMS → AISe): Not supported ($\beta = 0.087$, $p = 0.285$), suggesting that TMS operates through SC as a mediating variable rather than directly.

The model explains 69.4% of variance in AISe ($R^2 = 0.694$), demonstrating strong explanatory power. The Q^2 index (0.667) confirms robust predictive ability.

For practitioners, the findings recommend a three-pronged approach to strengthening accounting information security: (1) systematically upgrading the quality of accounting information systems to ensure robust processing, security, and data integrity capabilities; (2) investing in security culture development through leadership modelling, training programs, and awareness campaigns; and (3) building comprehensive cybersecurity readiness programs that integrate technology, processes, and people in accordance with NIST SP 800-12 and ISO/IEC 27001: 2022 standards. As AI tools become increasingly integrated into Vietnamese accounting and auditing

practice - a trend accelerating under national digital transformation policy [67] - these foundations will be essential to managing the novel security risks introduced by AI systems.

For researchers, this study makes methodological and theoretical contributions by: (a) successfully operationalizing AISe as a second-order formative construct within the CIA framework using the Two-Stage Approach in PLS-SEM; (b) demonstrating the mediated pathway TMS → SC → AISe; and (c) providing empirical validation of the TOE framework's applicability to accounting security in Vietnam, a developing economy context underrepresented in the extant literature. Future research may extend this model by incorporating additional variables (e.g., regulatory pressure, AI governance quality), examining sector-specific moderating effects, or adopting longitudinal designs to capture the dynamics of security improvement over time.

Abbreviations

AI	Artificial Intelligence
AICPA	American Institute of Certified Public Accountants
AIS	Accounting Information System(s)
AISe	Accounting Information Security
AvISe	Availability of Accounting Information Security
CIA	Confidentiality, Integrity, and Availability
CISe	Confidentiality of Accounting Information Security
CSR	Cybersecurity Readiness
ERP	Enterprise Resource Planning
IISe	Integrity of Accounting Information Security
IoT	Internet of Things
LLM	Large Language Model
PLS-SEM	Partial Least Squares Structural Equation Modeling
QAIS	Quality of Accounting Information Systems
SC	Information Security Culture
TMS	Senior Management Support (Top Management Support)
TOE	Technology-Organization-Environment (Framework)
VIF	Variance Inflation Factor

Acknowledgments

The author gratefully acknowledges the experts and colleagues of the Vietnam Chief Accountants and Chief Financial Officers Forum (VCCA) for their valuable assistance in facilitating data access, providing professional insights, and offering constructive feedback on earlier drafts of this manuscript. Their contributions have substantially improved the quality and rigor of this research.

Author Contributions

Huong Nguyen Thi Mai: Conceptualization, Data curation, Formal Analysis, Investigation, Methodology, Project administration, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing

Data Availability Statement

The data supporting the outcome of this research work has been reported in this manuscript.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Abu Afifa, M. M., Nguyen, T. H., Le, M. T. T., Nguyen, L., & Tran, T. T. H. (2025). Accounting going digital: A Vietnamese experimental study on artificial intelligence in accounting. VINE Journal of Information and Knowledge Management Systems. https://doi.org/10.1108/vjikms-10-2023-0266

[2] Accenture. (2025). State of cybersecurity resilience 2025. Accenture Research. https://www.accenture.com/us-en/insights/security/state-cybersecurity-2025

[3] Abutaber, T. (2023). The impact of accounting information systems on enhancing financial information security in Jordanian banks. International Journal of Data and Network Science, 7(5), 1067-1076. https://doi.org/10.5267/j.ijdns.2023.5.017

[4] Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. Journal of Intelligent Manufacturing, 25(2), 357-370. https://doi.org/10.1007/s10845-012-0683-x

[5] Alhassan, M. M., & Adjei-Quaye, A. (2017). Information security in an organization. International Journal of Computer (IJC), 24(1), 100-116.

[6] Alnatheer, M., Chan, T., & Nelson, K. (2012). Understanding and measuring information security culture. In Proceedings of the 10th Australian Information Security Management Conference (pp. 1-11). Edith Cowan University.

[7] AlGhamdi, S., Win, K. T., & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. Computers & Security, 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

[8] Alshaikh, M., & Adamson, G. (2021). From policy to practice: Towards a process for managing cybersecurity behaviour in the workplace. International Journal of Information Security, 21, 1413-1425. https://doi.org/10.1007/s10207-022-00572-z

[9] Baker, J. (2012). The technology-organization-environment framework. In Y. K. Dwivedi et al. (Eds.), Information systems theory: Explaining and predicting our digital society (Vol. 1, pp. 231-246). Springer. https://doi.org/10.1007/978-1-4419-6108-2_12

[10] Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99-120. https://doi.org/10.1177/014920639101700108

[11] Berlilana, B., Hariguna, T., Sari, R. N. P., Tarihoran, N., & Purwati, A. A. (2021). Understanding cybersecurity readiness: Integrating TOE and information security culture. International Journal of Safety and Security Engineering, 11(5), 565-575. https://doi.org/10.18280/ijsse.110501

[12] Bhimani, A., & Willcocks, L. (2014). Digitisation, 'Big Data' and the transformation of accounting information. Accounting and Business Research, 44(4), 469-490. https://doi.org/10.1080/00014788.2014.910051

[13] Bishop, M. (2019). Computer security: Art and science (2nd ed.). Pearson Education.

[14] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security. European Journal of Information Systems, 18(2), 151-164. https://doi.org/10.1057/ejis.2009.8

[15] Bradford, M., Earp, J. B., & Grabski, S. (2014). Centralized end-to-end identity and access management and ERP systems: A multi-case study of enterprise software users. International Journal of Accounting Information Systems, 15(2), 179-195. https://doi.org/10.1016/j.accinf.2014.02.003

[16] Busulwa, R., & Evans, N. (2022). Digital disruption and digital transformation of accounting. In R. Busulwa & N. Evans (Eds.), Digital transformation in accounting (pp. 43-51). Routledge.

[17] Cameron, K. S., & Quinn, R. E. (2011). Diagnosing and changing organizational culture: Based on the competing values framework (3rd ed.). Jossey-Bass.

[18] Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial Management & Data Systems, 107(3), 438-458. https://doi.org/10.1108/02635570710734316

[19] Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2021). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. MIS Quarterly, 45(1), 525-554. https://doi.org/10.25300/MISQ/2021/15604

[20] Daud, N. M., Rasiah, R. T. R., Abidin, F. Z., & Hashim, H. (2018). A study of cybersecurity readiness among internet users in Malaysia. Jurnal Teknologi, 80(1), 11-20. https://doi.org/10.11113/jt.v80.10063

[21] Dong Quang Chung. (2023). The impact of information technology risks on the quality of accounting information in enterprises in Vietnam. University of Economics Ho Chi Minh City. https://digital.lib.ueh.edu.vn/handle/UEH/68941

[22] Dutta, A., & McCrohan, K. F. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87. https://doi.org/10.2307/41166156

[23] Gable, G. G., Sedera, D., & Chan, T. (2008). Re-conceptualizing information system success: The IS-impact measurement model. Journal of the Association for Information Systems, 9(7), 377-408. https://doi.org/10.17705/1jais.00164

[24] Gorla, N., Somers, T. M., & Wong, B. (2010). Organizational impact of system quality, information quality, and service quality. Journal of Strategic Information Systems, 19(3), 207-228. https://doi.org/10.1016/j.jsis.2010.05.001

[25] Government of the Socialist Republic of Vietnam. (2007). Decree No. 64/2007/ND-CP on application of information technology in state agency activities. https://thuvienphapluat.vn

[26] Government of the Socialist Republic of Vietnam. (2015). Law on Network Information Security No. 86/2015/QH13. https://thuvienphapluat.vn

[27] Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. Journal of Management Information Systems, 28(2), 203-236. https://doi.org/10.2753/MIS0742-1222280208

[28] Haapamäki, E., & Sihvonen, J. (2019). Cybersecurity in accounting research. Managerial Auditing Journal, 34(7), 808-834. https://doi.org/10.1108/MAJ-09-2018-2002

[29] Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2017). When to use and how to report results of PLS-SEM. European Business Review, 31(1), 2-24.

[30] Hair, J. F., Sarstedt, M., Ringle, C. M., & Gudergan, S. P. (2022). Advanced issues in partial least squares structural equation modeling (2nd ed.). SAGE Publications.

[31] Hamdan, A., Hamdan, R., & Razzaque, A. (2017). Accounting information security culture: Auditors' perceptions in Bahraini firms. Journal of Financial Regulation and Compliance, 25(4), 413-428. https://doi.org/10.1108/JFRC-01-2017-0009

[32] Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58, 102726. https://doi.org/10.1016/j.jisa.2020.102726

[33] Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

[34] International Organization for Standardization. (2022). ISO/IEC 27001: 2022 - Information security, cybersecurity and privacy protection - Information security management systems. ISO.

[35] Izzo, M. F., Fasan, M., & Tiscini, R. (2021). Accounting for the digital transformation: An empirical analysis. Accounting in Europe, 18(3), 336-360. https://doi.org/10.1080/17449480.2021.1937558

[36] Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In Proceedings of the 3rd International Conference on Research and Innovation in Information Systems (ICRIIS'13). IEEE.

[37] Kayworth, T., & Whitten, D. (2010). Effective information security requires a balance of social and technology factors. MIS Quarterly Executive, 9(3), 163-175.

[38] Kim, Y., & Kim, B. (2021). The effective factors on continuity of corporate information security management: Based on TOE framework. Information, 12(11), 446. https://doi.org/10.3390/info12110446

[39] Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2006). Information security: Management's effect on culture and policy. Information Management & Computer Security, 14(1), 24-36. https://doi.org/10.1108/09685220610648355

[40] Knapp, K. J., Marshall, T. E., Rainer, R. K., & Morrow, D. W. (2007). The top information security issues facing organizations: What can government do to help? Information Systems Security, 16(1), 51-58. https://doi.org/10.1080/10658980601051186

[41] Knauer, T., Sommer, F., & Wohrmann, A. (2020). Success factors of forward-looking performance measurement systems: Evidence from the field. Journal of Accounting & Organizational Change, 16(4), 575-602.

[42] Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, 28(7), 509-520. https://doi.org/10.1016/j.cose.2009.04.006

[43] Marei, A. (2024). An empirical study on the impact of TOE factors on E-accounting adoption: The moderating role of cybersecurity. Journal of System and Management Sciences, 14(3), 266-292. https://doi.org/10.33168/JSMS.2024.0319

[44] Meraghni, S., Bendiabdellah, A., Terrissa, L. S., Marzak, H., & Zerhouni, N. (2021). Challenges of data collection in developing countries. In Proceedings of the 2021 International Conference on Applied Automation and Industrial Diagnostics (ICAAID). IEEE.

[45] Ministry of Information and Communications. (2023). Report on digital transformation of Vietnamese enterprises in 2023. SMEdx Program. https://smedx.vn

[46] National Assembly of the Socialist Republic of Vietnam. (2015). Accounting Law No. 8/2015/QH13. https://thuvienphapluat.vn

[47] National Institute of Standards and Technology (NIST). (2017). An Introduction to Information Security (NIST Special Publication 800-12 Revision 1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-12r1

[48] Nguyen, O. K. T., & Vo, T. H. V. (2025). The relationship between management accounting information systems, competitive advantage and performance: The moderating role of digital transformation. International Journal of Innovative Research and Scientific Studies, 8(3), 4593-4601. https://doi.org/10.53894/ijirss.v8i3.5670

[49] Oliveira, T., & Martins, M. F. (2011). Literature review of information technology adoption models at firm level. The Electronic Journal Information Systems Evaluation, 14(1), 110-121.

[50] Papiorek, K., & Hiebl, M. R. W. (2023). Information systems quality in management accounting and management control effectiveness. Journal of Accounting & Organizational Change, 19(1), 1-24. https://doi.org/10.1108/JAOC-12-2021-0179

[51] Peltier, T. R. (2016). Information security policies, procedures, and standards: Guidelines for effective information security management. Auerbach Publications.

[52] Pham Tra Lam. (2024). Information security culture model in accounting information systems: An empirical study in Vietnam. University of Economics Ho Chi Minh City. https://digital.lib.ueh.edu.vn/handle/UEH/71747

[53] Posthumus, S., & von Solms, R. (2004). A framework for the governance of information security. Computers & Security, 23(8), 638-646. https://doi.org/10.1016/j.cose.2004.10.006

[54] Rehberger, J. (2024). Trust no AI: Prompt injection along the CIA security triad. arXiv preprint arXiv: 2412.06090.

[55] Rehm, S.-V. (2022). Accounting information systems and how to prepare for digital transformation. In M. G. Quinn, E. Strauss, & F. J. Martin (Eds.), The Routledge Companion to Accounting Information Systems (pp. 69-79). Routledge.

[56] Solomon, G., & Brown, I. (2021). The influence of organisational culture and information security culture on employee compliance behaviour. Journal of Enterprise Information Management, 34(1), 1-26. https://doi.org/10.1108/JEIM-08-2019-0217

[57] Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. MIS Quarterly, 34(3), 503-522. https://doi.org/10.2307/25750689

[58] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs. Journal of Information Systems, 26(1), 93-116. https://doi.org/10.2308/isys-10255

[59] Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. Accounting, Organizations and Society, 71, 15-29. https://doi.org/10.1016/j.aos.2018.04.005

[60] Tang, M. (2021). Digital transformation: The essentials of e-business leadership. McGraw-Hill.

[61] Tornatzky, L. G., & Fleischer, M. (1990). The processes of technological innovation. Lexington Books.

[62] Tran Nu Hoai Nhu. (2024). Research on the impacts of information technology risks on the quality of accounting information in enterprises in Vietnam. University of Economics Ho Chi Minh City. https://digital.lib.ueh.edu.vn/handle/UEH/72783

[63] Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2018). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. Information & Management, 55(2), 189-204. https://doi.org/10.1016/j.im.2017.05.001

[64] Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. Computers & Security, 29(4), 476-486. https://doi.org/10.1016/j.cose.2009.10.005

[65] Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

[66] Viettel Cyber Security. (2023). Cyber Security Report for the first half of 2023. Military Industry and Telecommunications Group (Viettel). https://viettelcybersecurity.com

[67] Vietnam Digital Transformation Program. (2025). National AI Transformation Strategy (AIX) 2025-2030. Ministry of Information and Communications. https://smedx.vn

[68] Vietnam National Cyber Security Technology Joint Stock Company. (2023). Vietnam Cyber Security Summary Report 2023. https://ncs.vn

[69] VNISA - Vietnam Information Security Association. (2024). Survey report on the current state of cybersecurity in Vietnam in 2024. Hanoi: VNISA.

[70] Von Solms, R., & Von Solms, S. H. (2006). Information security governance: A model based on the Direct-Control Cycle. Computers & Security, 25(5), 408-412. https://doi.org/10.1016/j.cose.2006.07.005

[71] Wernerfelt, B. (1984). A resource-based view of the firm. Strategic Management Journal, 5(2), 171-180. https://doi.org/10.1002/smj.4250050207

[72] Whitman, M. E., & Mattord, H. J. (2018). Management of information security (6th ed.). Cengage Learning.

[73] World Economic Forum. (2025). Global cybersecurity outlook 2025. WEF. https://www.weforum.org