International Journal of
Financial Studies

MDPI

Article

Cybersecurity Effectiveness and Cloud Accounting Risk: The Moderating Role of the COBIT-5 Governance Framework—Evidence from Jordanian Banks

Mohammad Ismail Alawamreh [1,*], Ibrahim Saleh Al-Radaideh [2], Rawan Alshawabkeh [3,*], Mahmoud Abdelrehim [4], Mustafa Saeed Alathamneh [5] and Abutaber Thaer [5]

[1] Department of Accounting, Putra Business School (PBS), Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysia
[2] Finance and Banking Department, Amman Arab University, Amman 11953, Jordan; i.radaideh@aau.edu.jo
[3] Department of Business Administration, Business School, Al-Ahliyya Amman University, Amman 19328, Jordan
[4] School of Business and Economics, Universiti Putra Malaysia, Serdang 43400, Selangor, Malaysia; mahmoudabdelrehim@upm.edu.my
[5] Department of Accounting, Jadara University, Irbid 21110, Jordan; mathamneh@jadara.edu.jo (M.S.A.); thaer@jadara.edu.jo (A.T.)
* Correspondence: pbs22104001@grad.putrabs.edu.my (M.I.A.); r.alshawabkeh@ammanu.edu.jo (R.A.)

Abstract

This study investigates the effect of cybersecurity effectiveness on cloud accounting risk—operationalized through the three dimensions of the confidentiality, integrity, and availability (CIA) triad—within the Jordanian banking sector, comprising the 13 commercial banks listed on the Amman Stock Exchange. It further examines the moderating role of Control Objectives for Information and Related Technologies (COBIT-5) governance maturity in this relationship. Drawing on data from 388 cybersecurity, information technology, network security, and accounting professionals, the study employs Partial Least Squares Structural Equation Modeling (PLS-SEM) via SmartPLS 4 to estimate a single integrated structural model. The results indicate that cybersecurity effectiveness is significantly and negatively associated with all three dimensions of cloud accounting risk. COBIT-5 governance maturity significantly strengthens these negative associations across confidentiality, integrity, and availability, while exerting no statistically detectable direct effect of its own—a pattern consistent with COBIT-5 functioning as a pure moderator. Out-of-sample predictive tests (PLSpredict and the cross-validated predictive ability test, CVPAT) confirm that the model's explanatory power translates into genuine predictive validity. These findings suggest that technical cybersecurity controls alone may be insufficient to secure cloud-stored financial information, and that their risk-mitigating potential appears to be more fully realized when embedded within a mature governance framework that institutionalises accountability, continuous monitoring, and compliance enforcement. The study recommends that Jordanian banks treat cybersecurity investment and COBIT-5 governance maturity as complementary, jointly prioritised strategic initiatives, and that regulatory authorities incorporate explicit COBIT-5 maturity benchmarks into supervisory assessment frameworks.

Keywords: cybersecurity effectiveness; cloud accounting risk; COBIT-5; IT governance; CIA triad; commercial banks; Jordan

Check for updates

Academic Editor: Farid Irani

Received: 19 September 2026
Revised: 12 October 2026
Accepted: 20 October 2026
Published: 23 October 2026

Copyright: © 2026 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Cyber threats have become one of the most critical risks facing organizations in increasingly digitalized business environments, ranking as the leading global business risk for the fifth consecutive year (Allianz, 2026), with the global economic impact of cybercrime estimated to reach approximately US$10.5 trillion annually in 2025 (Cybersecurity Ventures, 2020). This escalating threat landscape has been further intensified by the rapid adoption of cloud computing, which exposes organizations to risks associated with unauthorized access, data breaches, insecure configurations, service disruption, and loss of control over sensitive information stored and processed through external infrastructures (Thales, 2025). These risks are particularly consequential for cloud accounting, given that accounting systems house highly sensitive financial information, including transaction records, customer data, payment information, and financial reporting records (Gupta et al., 2024; Anyanwu et al., 2024). Consequently, cybersecurity failures in cloud accounting environments may compromise the confidentiality, integrity, and availability (CIA) of financial information, ultimately undermining the reliability of accounting records and financial reporting—a concern that is especially pressing for banks, which manage substantial volumes of sensitive financial data and remain prime targets for cybercriminals. In Jordan, this problem has become increasingly evident at the national level: the National Cyber Security Center (2024) reported that Jordan recorded 6758 cyber incidents in 2024 alone, a 175% increase compared with 2023, alongside a rise in cybersecurity alerts from 2609 to 6922 over the same period—underscoring the rapidly escalating threat landscape facing the Kingdom's digital infrastructure, of which the banking sector forms a critical part. Importantly, these threats extend beyond external attacks—such as phishing, malware, ransomware, data breaches, and unauthorized access—to encompass internal threats involving employees and authorized users, including misuse of privileges, employee collusion, manipulation of accounting information, and unauthorized disclosure or trading of organizational data (Kul & Upadhyaya, 2015; Idensohn & Flowerday, 2025). Protecting cloud-based accounting information therefore requires an integrated cybersecurity approach capable of addressing both external and internal threats.

The increasing complexity of these threats highlights the importance of cybersecurity effectiveness and appropriate information technology (IT) governance: effectiveness cannot depend solely on technical controls but also requires governance structures establishing accountability, risk management, and compliance. The Control Objectives for Information and Related Technologies (COBIT-5) provide such a structured framework for aligning IT processes with organizational objectives and strengthening controls over information resources (Adrian & Wang, 2023; Al-Fatlawi et al., 2021; Al-Hakim et al., 2021). Cyber risk also carries behavioral dimensions—including privilege misuse, weak security practices, and information asymmetry—that effective IT governance can address through accountability, monitoring, and control enforcement. Although previous studies have examined cybersecurity challenges in financial institutions and cloud computing adoption in banking (Asadi et al., 2017), several important gaps remain. First, cybersecurity research has predominantly focused on advanced economies and Western or East Asian contexts, leaving developing-country banking environments comparatively underexplored (Yau-Yeung et al., 2020). Second, studies addressing cybersecurity have often examined general information-security outcomes rather than its specific role in mitigating cloud accounting risks, despite the particular sensitivity and financial significance of accounting information (Cram et al., 2023). Third, previous research has frequently emphasized confidentiality and availability while paying comparatively less attention to integrity, despite its fundamental importance to the accuracy and reliability of financial records (Maurer & Nelson, 2021). Finally, limited empirical research has examined whether IT governance frameworks such

as COBIT-5 strengthen the effectiveness of cybersecurity in mitigating cloud accounting risks, particularly within emerging banking contexts.

Against this background, the present study develops and empirically tests a governance-based model of cloud accounting risk mitigation in Jordanian commercial banks, with COBIT-5 governance maturity positioned as a boundary condition of cybersecurity effectiveness. The study moves beyond the conventional view that stronger cybersecurity controls automatically translate into better security outcomes by examining whether their risk-mitigation value depends on the maturity of the governance environment in which they operate. By examining confidentiality, integrity, and availability simultaneously, the study also provides a more comprehensive assessment of cloud accounting risk than approaches that emphasize selected security dimensions in isolation. This perspective offers a more nuanced explanation of how technical cybersecurity capabilities can be translated into effective protection of accounting information and provides empirical evidence relevant to banks, auditors, IT governance professionals, and regulators operating in increasingly cloud-dependent financial environments. The study also differs from the two closest prior studies of Jordanian banks. Ali et al. (2020) examined cyber governance as a direct determinant of cloud accounting risk; the present study instead treats cybersecurity effectiveness as the predictor and COBIT-5 governance maturity as a boundary condition, and tests the direct and moderating effects separately for confidentiality, integrity, and availability. AL-Alawamreh et al. (2026) examined whether two technologies—digital twins and artificial intelligence—interact with cybersecurity in shaping cloud accounting outcomes; the present study shifts the focus from technological to governance moderators, asking whether the protective value of cybersecurity depends on the maturity of the IT governance framework within which it operates. The two studies are based on separate questionnaires and datasets: AL-Alawamreh et al. (2026) measured digital twin and artificial intelligence adoption, constructs that were not measured in the present survey.

2. Literature Review and Hypotheses Development

This study advances the literature in four ways. First, rather than proposing a new theory, it combines two established theories—IT Governance Theory and Risk Management Theory—into a single governance-contingent explanation of risk mitigation: governance is modeled not as an antecedent of security outcomes, nor as a parallel driver of risk reduction, but as the boundary condition that determines whether a risk-treatment capability translates into measurable protection at all—a role that is empirically supported by the pure-moderator pattern (Section 5.3) rather than assumed. Second, it operationalizes this logic within a single integrated structural model spanning all three CIA dimensions simultaneously, a specification that remains rare in prior IT-governance research and allows the conditioning effect to be tested, not merely asserted, across confidentiality, availability, and integrity at once. Third, disaggregating cloud accounting risk into its three CIA sub-dimensions reveals that the governance-contingency effect is not uniform: the interaction is largest for integrity risk ($\beta = -0.296$, $f^2 = 0.141$), and for both integrity and availability risk the association between cybersecurity effectiveness and risk is statistically non-significant at low governance maturity, whereas it remains significant for confidentiality risk, suggesting that governance maturity is most consequential in the dimensions where cybersecurity alone offers the least detectable protection—a pattern with direct implications for how institutions sequence governance versus technical investment, and one that a single-dimension or additive-effects specification would not have revealed. Fourth, by showing that COBIT-5 fits the statistical pattern of a pure moderator, the study offers a testable empirical proposition—rather than a general association—that future research can test against alternative governance frameworks—COBIT 2019 (ISACA, 2019), ISO/IEC

27001 of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC, 2022), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2024)—to determine whether this conditioning role is specific to COBIT-5 or general to mature IT governance as such.

2.1. Cloud Accounting Risks

Cloud accounting, which integrates accounting information systems with cloud computing infrastructure, enables financial data to be processed, stored, and accessed remotely through internet-based platforms (Eldalabeeh et al., 2021). Cloud computing revenues are projected to reach approximately US$2.27 trillion globally by 2031, growing at a compound annual growth rate (CAGR) of 15.34% from 2026 (Statista, 2026). Despite this growing adoption, cloud accounting exposes banking institutions to significant cybersecurity risks. These risks are primarily classified into three dimensions: confidentiality, availability, and integrity, encompassing unauthorized access, service interruptions, and manipulation of financial records (Agarwal et al., 2023; AL-Alawamreh et al., 2026; Mather et al., 2009). Confidentiality risks include data breaches, theft of sensitive financial information, collusion between hackers and internal employees, and violations of customer privacy (van Wyk & Rudman, 2019). Availability risks involve internet outages and service disruptions that directly affect banking operations and financial reporting continuity (Hon & Millard, 2018). Integrity risks involve unauthorized modification, corruption, or manipulation of financial records that compromise the accuracy and reliability of accounting data (Tchernykh et al., 2019; Jouini et al., 2014). Banks face additional risks as a result of their reliance on external cloud service providers operating across multiple jurisdictions, complicating regulatory compliance with international standards, particularly regarding data sovereignty and cross-border transfers (Cheng et al., 2022). Furthermore, the multi-tenant nature of cloud platforms raises concerns regarding data segregation, while cross-border data storage intensifies sovereignty and legal compliance challenges (Berry & Reisman, 2012). Confidentiality, integrity, availability, and safety risks are among the most important risks of cloud accounting, mainly due to the direct relationship between these dimensions and the effectiveness of cybersecurity in banking institutions (Agarwal et al., 2023; Tchernykh et al., 2019). Beyond these technological vulnerabilities, cloud accounting risk also has a behavioral dimension, since employees, cloud providers, and other stakeholders hold differing levels of information and responsibility for cybersecurity—underscoring the importance of governance and monitoring mechanisms.

2.2. Cybersecurity Effectiveness and Cloud Accounting Risks

Building on the IT governance perspective outlined above, cybersecurity effectiveness in this study is understood not as a purely technical attribute, but as an organizational capability whose actual value is determined by the extent to which security resources are governed, directed, and appropriately overseen. Consistent with this view, Kankanhalli et al. (2003) define cybersecurity effectiveness as the capacity of an organization's technical and organizational security infrastructure to detect, prevent, and mitigate cyber threats targeting the organization's digital assets, while Héroux and Fortin (2025) similarly frame cybersecurity as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." In the banking sector, this effectiveness manifests through technical controls—including encryption protocols, multi-factor authentication, and intrusion detection and prevention systems (IDS/IPS)—alongside organizational controls such as security awareness training and incident response planning (Anyanwu et al., 2024); however, con-

sistent with IT governance theory, these controls generate protective value only to the extent that they are integrated into a governance structure that aligns them with enterprise risk objectives, rather than functioning as isolated technical investments. The stakes of this alignment are particularly high in banking, where financial services are reported to be targeted by cyberattacks at a rate approximately 300 times higher than other service industries (Boston Consulting Group, 2019), and where the reputational damage from security breaches—though not easily quantifiable—represents the most significant cost of data breaches in terms of brand erosion (Liu & Babar, 2026). This has driven sustained growth in cybersecurity investment in the banking sector (Lee, 2021), with global information security spending projected by Gartner (2024) to continue rising sharply. Organizations that invest in advanced cybersecurity technologies demonstrate greater capacity to protect accounting data from breaches, financial errors, and fraudulent manipulation (Novianti & Dewayanto, 2025; Morshed & Khrais, 2025). Viewed through risk management theory, however, this assumption warrants scrutiny: risk mitigation is not a direct function of investment volume but of how systematically threats are identified, assessed, treated, and monitored (Rausand, 2011)—processes that themselves depend on governance maturity rather than technical spending alone. In other words, cybersecurity effectiveness may reduce cloud accounting risk unevenly across organizations with comparable investment levels but differing governance capabilities, suggesting that the effectiveness–risk relationship is conditional rather than uniformly linear. A substantial share of current spending targets cloud computing environments specifically, against the three CIA-based risk categories examined in this study—confidentiality, availability, and integrity—each discussed in turn below. It is precisely this conditionality that motivates the governance-maturity perspective developed in this study: cybersecurity effectiveness is treated not only as a technical capability but as an organizational risk-control mechanism whose impact on cloud accounting risk is expected to strengthen under higher COBIT-5 governance maturity.

2.2.1. Cybersecurity Effectiveness and Data Confidentiality Risk

Data confidentiality constitutes a foundational pillar of institutional integrity in the banking sector, encompassing the protection of sensitive financial information, including transaction records, customer data, and regulatory disclosures, against unauthorized access, exploitation, or inadvertent disclosure throughout the data lifecycle: processing, transmission, and storage (Gawande & Kapse, 2014; Petcu & Crăciun, 2014). Breaches of confidentiality can result in regulatory sanctions, customer attrition, reputational damage, and deterioration of competitive positioning and market value (Liu & Babar, 2026). In cloud accounting environments, the interconnected nature of digital infrastructures increases the importance of effective cybersecurity controls for protecting sensitive accounting information. Technical measures such as encryption, role-based access control, intrusion detection, and continuous monitoring can restrict unauthorized access and reduce exposure to confidentiality breaches. In the Jordanian banking context, these measures are further supported by the Central Bank of Jordan's financial-sector cybersecurity framework, launched in 2021 with the participation of all operating banks (Central Bank of Jordan, 2021). From an IT Governance perspective, effective cybersecurity also depends on accountability, access authorization, monitoring, and appropriate control structures that align IT practices with organizational objectives (Weill & Ross, 2004). Empirical evidence from the Jordanian banking sector indicates that cybersecurity dimensions, including confidentiality, integrity, and availability, are strongly and positively associated with banking performance outcomes (Al-Khatib et al., 2025). Similarly, Amer and Al-Omar (2023) found that cybersecurity plays a crucial role in preventing and mitigating breaches involving confidential customer and organizational information. Adrian and Wang (2023) further demonstrated

that IT governance-aligned cybersecurity programs based on COBIT-5 can improve the effectiveness of cybersecurity-related internal controls. Collectively, these theoretical and empirical arguments suggest that stronger cybersecurity effectiveness should reduce data confidentiality risk in cloud accounting environments, leading to the following hypothesis:

H1a. *Cybersecurity effectiveness has a significant negative effect on data confidentiality risk within cloud accounting systems in Jordanian banks.*

2.2.2. Cybersecurity Effectiveness and Data Availability Risk

Data availability constitutes a critical dimension of cloud accounting risk, defined as the capacity of systems to reliably store, preserve, and retrieve financial data on demand; failures in this dimension—whether arising from data theft, unauthorized access, or system inaccessibility—directly undermine operational continuity and expose institutions to cascading financial and reputational losses (AL-Alawamreh et al., 2026; Yau-Yeung et al., 2020). IT governance theory (Weill & Ross, 2004) offers a direct explanation for why cybersecurity effectiveness should reduce this specific risk. Because the theory reconceptualizes security as an organizational rather than purely technical phenomenon, availability failures are understood not as isolated technical breakdowns but as governance failures—breakdowns in the alignment between IT decision rights, control mechanisms, and enterprise continuity requirements. Accordingly, an organization's ability to sustain data availability during an attack depends less on the sophistication of any single control and more on whether cybersecurity capabilities are embedded within a governance structure that continuously directs, monitors, and escalates response to disruptions (Weill & Ross, 2004; De Haes et al., 2013). Risk management theory (Rausand, 2011) supplies the complementary mechanism by which this governance translates into measurable availability outcomes. Treating data availability as one of three CIA dimensions subject to systematic identification, assessment, treatment, and monitoring implies that cybersecurity effectiveness reduces availability risk specifically through the treatment and monitoring stages—detection of anomalies, incident containment, and restoration of service—rather than through prevention alone. This distinction matters because much of the surrounding literature discusses cybersecurity effectiveness primarily in terms of breach prevention, leaving this recovery-oriented pathway to availability under-examined. Within cloud-based environments, this gap is consequential: dependence on external service providers introduces a governance dependency that regulators increasingly evaluate in terms of operational resilience rather than perimeter defense alone (Koh & Prenio, 2023), and COBIT-5 operationalizes exactly this resilience-oriented governance—translating IT governance and risk-management principles into structured processes for continuous monitoring, accountability, and control (ISACA, 2012). Existing evidence supports COBIT-5's role in mitigating cloud computing and cloud accounting risks generally (Okour, 2019; Al-Fatlawi et al., 2021; Ali et al., 2020; van Wyk & Rudman, 2019), yet none of this evidence isolates data availability as a distinct outcome of cybersecurity effectiveness—a gap this study addresses directly. Accordingly, the following hypothesis is posited:

H1b. *Cybersecurity effectiveness has a significant negative effect on data availability risk within cloud accounting systems in Jordanian banks.*

2.2.3. Cybersecurity Effectiveness and Data Integrity Risk

Data integrity represents the third foundational pillar of the CIA triad in cloud accounting security, defined as the assurance that financial data remains accurate, consistent, and unaltered across its entire lifecycle—encompassing creation, processing, transmission, and storage—and is particularly vulnerable to both deliberate manipulation through insider

threats or cyberattacks, and unintentional compromise through system errors or flawed data migration processes (Jouini et al., 2014; Tchernykh et al., 2019). Integrity failures carry severe institutional consequences for Jordanian commercial banks, where transactional data accuracy underpins regulatory compliance, financial reporting reliability, and external audit credibility (Central Bank of Jordan, 2021). IT governance theory (Weill & Ross, 2004) frames integrity risk as fundamentally a governance-alignment problem rather than a purely technical one. Because the value of any technical control—file integrity monitoring, a mechanism first formalized through checksum-based checkers such as Tripwire (Kim & Spafford, 1994) and since extended to distributed cloud architectures through blockchain-based verification protocols (Pinheiro et al., 2020)—depends on whether it is embedded within clear decision rights, accountability structures, and continuous oversight, the mere presence of such tools does not guarantee integrity. Cybersecurity effectiveness reduces integrity risk to the extent that these controls are governed, monitored, and enforced consistently across both internal actors and external service providers with privileged access to financial information. Risk management theory (Rausand, 2011) supplies the complementary mechanism, treating integrity as one of three CIA dimensions subject to systematic identification, assessment, treatment, and monitoring—implying that cybersecurity effectiveness reduces integrity risk specifically through continuous detection of unauthorized alteration and swift remediation, rather than through static prevention alone, a distinction that is particularly consequential given the sharp rise in ransomware and data-tampering attacks in Jordan noted earlier (National Cyber Security Center, 2024). This governance-and-detection mechanism remains, however, empirically untested for cloud accounting specifically within Jordanian commercial banks. Accordingly, the following hypothesis is proposed:

H1c. *Cybersecurity effectiveness has a significant negative effect on data integrity risk within cloud accounting systems in Jordanian banks.*

2.3. The Moderating Effect of COBIT-5 on the Relationship Between Cybersecurity Effectiveness and Data Confidentiality Risk

COBIT-5, developed by ISACA, represents a comprehensive IT governance framework that integrates strategic alignment, risk management, and performance monitoring through structured principles and enablers designed to enhance enterprise governance effectiveness (ISACA, 2012; De Haes et al., 2020). IT governance theory (Weill & Ross, 2004) predicts that governance functions as an amplifying condition rather than an additive one: because the value of any security capability depends on whether decision rights, accountability, and monitoring structures are aligned around it, cybersecurity effectiveness should translate into confidentiality-risk reduction more strongly where COBIT-5 institutionalizes clear roles, responsibilities, and access privileges that close the gaps through which insider threats and unauthorized access typically occur (Al-Fatlawi et al., 2021; Okour, 2019). Risk management theory (Rausand, 2011) supplies the moderating mechanism itself: treating confidentiality as a risk subject to continuous identification, assessment, treatment, and monitoring implies that the marginal effectiveness of any security control is conditional on how consistently that cycle is enforced—such that under high governance maturity, the same level of cybersecurity effectiveness yields a materially stronger reduction in confidentiality risk than under weak or informal governance. Existing empirical evidence is directionally consistent with this mechanism but stops short of testing it. Al-Fatlawi et al. (2021) found that COBIT-5-based governance strengthened accounting-information security in an Iraqi commercial bank, though as a direct association rather than a moderation effect; Okour (2019) reported that COBIT-5 significantly reduced cloud-computing risk among Jordanian organizations, but outside the banking sector. van Wyk and Rudman

(2019) supply the underlying risk-assessment and resource-allocation logic through which COBIT-5 for Risk structures technology-risk identification and control, while Al-Tayan et al. (2026) show empirically that higher COBIT-5 maturity in security-management domains (APO13 Manage Security and DSS05 Manage Security Services) corresponds to measurably lower unresolved threat levels, supporting the continuous-monitoring pathway posited above. Al-Gasaymeh et al. (2023) confirm COBIT-5's general positive effect on governance-tool effectiveness within Jordanian commercial banks, closing part of the geographic gap; however, this evidence remains at the level of general institutional governance rather than cybersecurity or cloud accounting specifically, and—like the studies above—evaluates COBIT-5's direct effect rather than its moderating role—consistent with the broader alignment between governance maturity and CIA-wide protection reported in the wider literature (Herath et al., 2023). Taken together, this evidence establishes that COBIT-5 governance improves security outcomes generally and that Jordanian banks are a documented setting for such effects, but has not tested governance maturity as a formal moderator of the cybersecurity-effectiveness–confidentiality-risk relationship—the gap this study addresses. Accordingly, the following hypothesis is proposed:

H2a. *COBIT-5 significantly moderates the relationship between cybersecurity effectiveness and data confidentiality risks within cloud accounting systems in Jordanian banks.*

2.4. The Moderating Effect of COBIT-5 on the Relationship Between Cybersecurity Effectiveness and Data Availability Risk

The COBIT-5 framework operationalizes availability assurance through two specific process areas—DSS04 (Continuity Management) and BAI04 (Availability and Capacity Management)—which formalize business-continuity planning, disaster recovery, and IT capacity oversight as recurring governance obligations rather than discretionary technical practices (Garsoux, 2013; ISACA, 2012). Under this arrangement, availability-related cybersecurity investments—redundancy systems, failover mechanisms, and distributed denial-of-service (DDoS) mitigation tools—are not merely deployed but are continuously tested, escalated, and reviewed against defined resilience targets (Al-Hakim et al., 2021; Oliver & Lainhart, 2012). This distinction matters theoretically: IT governance theory (Weill & Ross, 2004) explains why such continuous oversight—rather than the technical controls alone—is what drives the strengthening of the cybersecurity-availability relationship, since the theory locates security value in the alignment of decision rights and accountability around a control rather than in the control's technical sophistication; and risk management theory (Rausand, 2011) clarifies that this strengthening operates specifically through the treatment and monitoring stages of the risk cycle, meaning the same redundancy or failover investment yields a materially larger reduction in availability risk when DSS04/BAI04-style governance ensures it is actually tested and escalated, compared to when it sits ungoverned and unverified until a disruption occurs. Existing evidence is directionally consistent with this mechanism but does not test it directly: Al-Tayan et al. (2026) link higher COBIT-5 maturity to improved operational stability and reduced downtime in financial institutions, and van Wyk and Rudman (2019) establish COBIT-5's risk-assessment logic for cloud-related availability threats—yet both evaluate COBIT-5's association with availability outcomes on its own, rather than testing governance maturity as a formal moderator of the cybersecurity-effectiveness–availability-risk relationship, leaving unresolved whether COBIT-5 amplifies the protective value of existing cybersecurity investment or produces availability gains independently of it. Accordingly, the following hypothesis is proposed:

H2b. *COBIT-5 significantly moderates the relationship between cybersecurity effectiveness and data availability risk within cloud accounting systems in Jordanian banks.*

2.5. The Moderating Effect of COBIT-5 on the Relationship Between Cybersecurity Effectiveness and Data Integrity Risk

Data integrity—the assurance that financial data remains accurate, consistent, and unaltered across its lifecycle—is threatened either deliberately, through insider manipulation or attacks such as ransomware and data tampering, or inadvertently, through synchronization failures or flawed migration processes, with direct consequences for regulatory compliance and audit credibility in Jordanian commercial banks (Jouini et al., 2014; Tchernykh et al., 2019; Central Bank of Jordan, 2021). COBIT-5 operationalizes integrity assurance through APO12 (Manage Risk) and DSS05 (Manage Security Services), which establish systematic identification, monitoring, and accountability for integrity-related controls such as cryptographic hashing, digital signatures, and file integrity monitoring, and MEA03 (Monitor, Evaluate and Assess Compliance with External Requirements), which enforces the regulatory alignment that prevents integrity breaches from going unreported (Al-Fatlawi et al., 2021; ISACA, 2012; van Wyk & Rudman, 2019). This matters theoretically because IT governance theory (Weill & Ross, 2004) locates a control's protective value not in its technical sophistication but in whether decision rights and accountability are formally assigned around it—precisely what APO12/DSS05/MEA03 supply for integrity—while risk management theory (Rausand, 2011) clarifies that this strengthens the cybersecurity-integrity relationship specifically through the treatment-and-monitoring stages of the risk cycle: the same hashing or file-integrity control yields a materially larger reduction in integrity risk when unauthorized alterations are continuously detected and escalated under mature governance than when it operates unmonitored. Existing evidence supports this mechanism only indirectly: Herath et al. (2023) link stronger security-governance functions to better detection of data-accuracy violations, and Wolden et al. (2015) report that higher COBIT-5 maturity reduces cyberattack exposure—yet both evaluate governance maturity's association with security outcomes on its own, not as a formal moderator of the cybersecurity-effectiveness–integrity-risk relationship, leaving unresolved whether COBIT-5 amplifies existing cybersecurity investment or produces integrity gains independently of it. Accordingly, the following hypothesis is put forward:

H2c. *COBIT-5 significantly moderates the relationship between cybersecurity effectiveness and data integrity risks in cloud accounting systems within Jordanian banks.*

2.6. Conceptual Framework

This study conceptualizes cybersecurity effectiveness as the key independent variable reducing cloud accounting risk across the three CIA dimensions: confidentiality, availability, and integrity (Figure 1). COBIT-5 governance maturity is positioned as a moderating mechanism that strengthens this relationship through formal oversight, accountability, and risk-monitoring structures. COBIT-5, rather than the more recent COBIT 2019, was deliberately selected for four reasons. First, COBIT 2019 is an evolutionary update of COBIT-5 rather than a replacement of its foundations: it retains the distinction between governance and management, the five process domains (Evaluate, Direct and Monitor [EDM]; Align, Plan and Organise [APO]; Build, Acquire and Implement [BAI]; Deliver, Service and Support [DSS]; and Monitor, Evaluate and Assess [MEA]), and the specific objectives on which the arguments of this study rely—APO12, APO13, BAI04, DSS04, DSS05, and MEA03—so the governance mechanisms tested here remain relevant under COBIT 2019 (ISACA, 2019). Second, the Central Bank of Jordan's instructions on the governance and management of information and related technology (Central Bank of Jordan, 2016) were developed on the basis of COBIT-5, which has therefore served as the reference framework through which Jordanian banks implemented, documented, and

audited their IT governance processes; respondents were consequently most familiar with COBIT-5 terminology and structure. Third, the COBIT-5 measurement items used here were adapted from Wolden et al. (2015), whose study examined the COBIT-5 information security framework in supply chain management systems, and were reworded for the banking context (Section 3.3); COBIT-5 is also the framework applied in prior Jordanian studies of IT governance and cloud computing risk (Okour, 2019; Al-Gasaymeh et al., 2023), whereas comparable perception-based measures for COBIT 2019 remain scarce. Fourth, COBIT 2019 replaces the COBIT-5 process capability model with a Capability Maturity Model Integration (CMMI)-based capability and maturity approach that is tailored to each enterprise through design factors and focus areas, which makes standardized measurement across banks through a common survey instrument more difficult. Using COBIT-5 therefore ensured consistency with the regulatory environment, respondents' familiarity with the framework, and the availability of validated measures; the implications of this choice for generalizability are discussed in Section 7. The framework also accounts for the behavioral dimensions of cyber risk—moral hazard and information asymmetry—which mature COBIT-5 governance mitigates through stronger accountability and monitoring of both internal and external exposures. The model is grounded in IT Governance Theory (Weill & Ross, 2004) and Risk Management Theory (Rausand, 2011), which jointly explain how governance structures and systematic risk processes enhance cybersecurity effectiveness and reduce cloud accounting risk, and is further supported empirically by Ali et al. (2020), Al-Tayan et al. (2026), and Yau-Yeung et al. (2020).

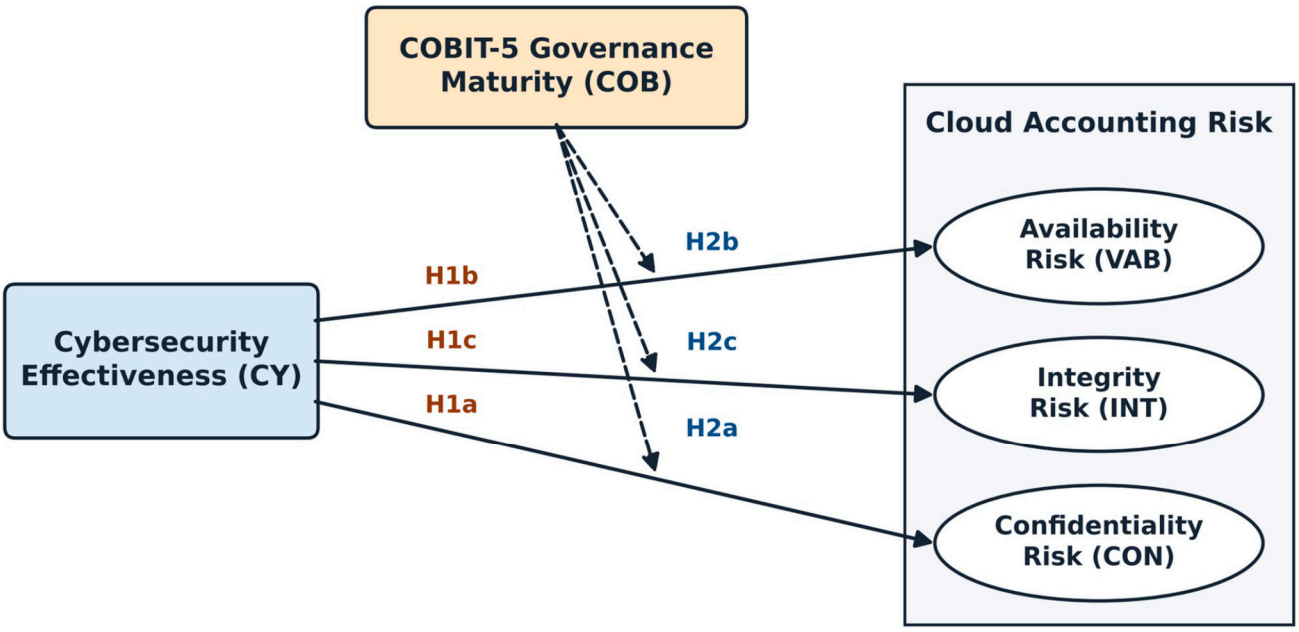


Figure 1. Conceptual framework of the study. Solid arrows denote the hypothesized direct effects of cybersecurity effectiveness (CY) on the three cloud accounting risk dimensions (H1a–H1c); dashed arrows denote the moderating effects of COBIT-5 governance maturity (COB) on these relationships (H2a–H2c).

3. Research Methodology

3.1. Research Design

This study adopts a quantitative, deductive methodology grounded in a positivist epistemology (Creswell, 2009), deriving testable hypotheses from IT governance theory and risk management theory and evaluating them empirically through a cross-sectional survey of purposively selected banking professionals (Bell et al., 2022). A cross-sectional

design is particularly suited to testing the study's moderation hypotheses, which require measuring cybersecurity effectiveness, COBIT-5 governance maturity, and their interaction as they jointly stand within organizations at a single point in time, rather than tracking how governance maturity develops over time—a question left to future longitudinal work (Section 7)—consistent with prior cybersecurity and cloud-accounting-risk studies in banking contexts (Ali et al., 2020; Yau-Yeung et al., 2020). Given this design, the findings should not be interpreted as establishing causal relationships in the strict empirical sense; the hypothesized directions are instead theoretically grounded in IT governance and risk management perspectives, empirically assessed through the estimated structural paths (Shadish, 2002), and partly offset by the out-of-sample predictive tests (PLSpredict and the cross-validated predictive ability test, CVPAT) reported in Section 4.9, which provide evidence of the model's predictive—though not causal—validity.

3.2. Population and Sampling

The target population comprised cybersecurity, IT, network security, and accounting professionals across the 13 commercial banks listed on the Amman Stock Exchange, with a purposive sampling strategy targeting employees demonstrably involved in cloud accounting, cybersecurity, or IT governance and distributed across all four functional specializations and all 13 banks to ensure institutional and functional diversity (Trevena et al., 2013). The minimum required sample size—77 observations per G*Power 3.1 ($f^2 = 0.15$, power = 0.80, $\alpha = 0.05$, three predictors per equation) and 30 observations per the Hair et al. (2017) ten-times rule for the most complex endogenous construct—was substantially exceeded by the final sample of 388 valid responses, confirming adequate statistical power. Common method bias (CMB) was addressed at the design stage through the procedural remedies recommended by Podsakoff et al. (2003): (i) respondents were assured of anonymity and confidentiality and were explicitly informed that there were no right or wrong answers, reducing evaluation apprehension and social-desirability bias; (ii) the predictor items (CY and COB) and the criterion items (CON, VAB, and INT) were placed in separate sections of the questionnaire with distinct instructions, creating psychological separation between them; and (iii) item wording was kept short, specific, and free of double-barrelled phrasing, and was refined during the expert review and pilot test to reduce item ambiguity. CMB was then assessed statistically using Kock's (2015) full-collinearity approach, as detailed in Section 4.4. The final sample (Table 1) was 55.15% male and 44.85% female, predominantly aged 30–50 years (75.26%) and bachelor's-degree holders (62.63%), distributed across cybersecurity (25.26%), accounting (22.68%), network security (21.91%), and IT (20.62%) specializations, with 70.10% reporting 10 or more years of work experience—indicating a relatively experienced and professionally knowledgeable sample.

Participants were identified and selected through a purposive procedure. First, permission to conduct the survey was obtained from the management of each of the 13 banks. Second, the questionnaire was directed only to employees who met two inclusion criteria: (i) holding a position in cybersecurity, information technology, network security, or accounting/finance; and (ii) being directly involved in operating, securing, or overseeing cloud-based accounting systems or related IT-governance processes. Third, the questionnaire was distributed by hand, in paper form, to eligible employees in all 13 banks between 15 January 2026 and 1 March 2026, and completed questionnaires were collected by hand. In total, 400 questionnaires were distributed and 392 were returned, a response rate of 98.0%. Of the returned questionnaires, four were excluded as unusable for analysis, leaving 388 valid responses (an effective response rate of 97.0%). This high response rate reflects the personal, hand-delivered administration and collection of the questionnaire. Because

the questionnaire was anonymous and did not record the respondent's bank, the number of valid responses obtained from each individual bank could not be determined.

Table 1. Demographic Characteristics.

Description (n = 388)	Category	Frequency	Percentage (%)
Gender	Male	214	55.15%
	Female	174	44.85%
Age	Less than 30 years	8	2.06%
	30 to 40 years	153	39.43%
	40 to 50 years	139	35.82%
	Above 50 years	88	22.68%
Education	Others	25	6.44%
	Diploma	44	11.34%
	Bachelor	243	62.63%
	Master	61	15.72%
	Postgraduate	15	3.87%
Position	Cybersecurity	98	25.26%
	Network security	85	21.91%
	Information technology	80	20.62%
	Accounting	88	22.68%
	Other	37	9.54%
Work duration	Less than 5 years	18	4.64%
	5–10 years	98	25.26%
	10–15 years	140	36.08%
	More than 15 years	132	34.02%

3.3. Measurement Instruments

The research instrument is a structured questionnaire in which all constructs are measured on a five-point Likert scale (1 = Strongly Disagree to 5 = Strongly Agree). Cybersecurity Effectiveness (CY) was operationalized using five items adapted from Bulgurcu et al. (2010) and D'Arcy et al. (2009), capturing technical dimensions (encryption, multifactor authentication, intrusion detection/prevention, access control) and organizational dimensions (security training, incident response, continuous monitoring); cloud accounting risks were operationalized through three theoretically grounded sub-scales aligned with the CIA triad—Data Confidentiality Risk (CON1–CON3), drawing on Parsons et al. (2015); Data Availability Risk (VAB1–VAB3), adapted from Ackermann et al. (2012) and Armbrust et al. (2010); and Data Integrity Risk (INT1–INT4), adapted from Ackermann et al. (2012) and Armbrust et al. (2010)—each satisfying the minimum reflective measurement requirement of partial least squares structural equation modeling (PLS-SEM; Hair et al., 2017); and COBIT-5 Governance Maturity (COB) was measured using five items adapted from Wolden et al. (2015), covering governance principles, risk management, accountability, compliance monitoring, and IT-business alignment.

The questionnaire was developed in four stages. In the first stage (item selection and adaptation), all items were drawn from previously validated scales (see the Source column of Table A1 in Appendix A) and adapted to the context of cloud accounting in commercial banks. Adaptation was limited to contextual rewording—for example, replacing generic references to "the organization's information systems" with "the bank's cloud-based accounting system"—while preserving the meaning and structure of the original items; the risk items were worded so that higher scores denote higher perceived risk. The complete questionnaire—the wording of every item as administered, its source, and the

adaptation made to the original item—is provided in Appendix A (Table A1). In the second stage (content validity), the draft instrument was reviewed by six experts—four academics specializing in accounting information systems, cybersecurity, and IT governance, and two professional practitioners—consistent with the recommended range of three to ten reviewers (Lynn, 1986). The experts evaluated each item for relevance, clarity, and representativeness of its construct before the instrument was finalized for the pilot test. In the third stage (translation), the instrument was translated into Arabic and independently back-translated into English following Brislin (1970), and discrepancies were resolved by the research team to ensure semantic equivalence for Jordanian respondents. In the fourth stage (pilot test), the Arabic version was administered to 35 employees who met the same inclusion criteria as the main sample; pilot respondents were not included in the final dataset. The pilot instrument was evaluated against two predefined criteria: (i) clarity and comprehensibility of the items, assessed through respondents' feedback; and (ii) internal-consistency reliability, requiring Cronbach's α of at least 0.70 for each construct (Nunnally & Bernstein, 1994). The pilot results were satisfactory on both criteria, and the instrument required no further modification.

3.4. Statistical Analytical Models

Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed using SmartPLS 4 (Version 4; SmartPLS GmbH, Monheim am Rhein, Germany; Ringle et al., 2024). The technique was selected due to the study's predictive orientation, the presence of a moderating relationship, and the absence of multivariate normality assumptions (Hair et al., 2022). The moderating effect of COBIT-5 was modeled using the two-stage approach (Becker et al., 2018). Specifically, in the first stage the main-effects model (without the interaction term) was estimated to obtain latent variable scores for CY and COB; in the second stage, these scores were standardized, and their product was entered into the structural model as a single-item interaction term (CY $\times$ COB), alongside CY and COB as predictors of each risk dimension. The two-stage approach was preferred over the product-indicator approach because it is recommended when the main aim is to test whether the moderating effect is significant, and because it achieves high statistical power and parameter accuracy (Becker et al., 2018; Hair et al., 2022). Accordingly, no product indicators were generated, and all results reported in Section 4, including the model-fit statistics, refer to this two-stage specification. Because cloud accounting risk comprises three distinct CIA dimensions, a single integrated structural model was specified in which cybersecurity effectiveness (CY), COBIT-5 governance maturity (COB), and their interaction term (CY $\times$ COB) jointly predict three endogenous constructs—confidentiality risk (CON), availability risk (VAB), and integrity risk (INT)—estimated simultaneously within one PLS path model:

$$CON = f(CY, COB, CY \times COB) + \varepsilon_1$$

$$VAB = f(CY, COB, CY \times COB) + \varepsilon_2$$

$$INT = f(CY, COB, CY \times COB) + \varepsilon_3$$

Model assessment followed the two-step procedure of Hair et al. (2022): the measurement model was evaluated first (indicator reliability, internal consistency, convergent and discriminant validity), followed by the structural model (collinearity, R^2, f^2, and bootstrapped path coefficients). All structural paths were estimated with bias-corrected and accelerated (BCa) bootstrapping (5000 subsamples), and the variance inflation factor (VIF), f^2, R^2, and global model fit indices (standardized root mean square residual [SRMR] and normed fit index [NFI]) were reported. Out-of-sample predictive relevance was additionally assessed using PLSpredict (Shmueli et al., 2019) and the cross-validated

predictive ability test (CVPAT; Liengaard et al., 2021). The three risk dimensions were modeled as separate first-order constructs rather than combined into a single higher-order "cloud accounting risk" construct, for two reasons. Theoretically, confidentiality, availability, and integrity are conceptually distinct risk facets that remain empirically correlated (r = 0.60–0.61, Section 4.1) yet discriminant at the latent-construct level, with the highest heterotrait–monotrait (HTMT) ratio (0.733, INT-VAB) still comfortably below the conservative 0.85 threshold (Section 4.3; Henseler et al., 2015)—evidence that the three dimensions are related but not interchangeable manifestations of one risk; collapsing them would obscure the cross-dimensional variation in direct and moderating effects this study aims to detect and later confirms in Section 5.1. Methodologically, the hypotheses (H1a–H2c) are formulated at the level of each CIA dimension. In a higher-order specification, cybersecurity effectiveness and the interaction term would predict the higher-order construct, and the three dimensions would enter the model only as its lower-order components, with their relative contributions captured by the higher-order loadings or weights (Becker et al., 2012; Sarstedt et al., 2019). The dimension-specific direct and moderating paths could then no longer be estimated or tested separately. Modeling the three dimensions as separate first-order endogenous constructs therefore aligns the model with the level at which the hypotheses are stated, consistent with prior CIA-triad-based risk studies (Ackermann et al., 2012; Tchernykh et al., 2019).

3.5. Ethical Considerations

The study was conducted in accordance with the Declaration of Helsinki and was approved by the Research Ethics Committee, Faculty of Business, Jadara University (Decision No. 3, Ref. EC32025; Session No. 2, 16 November 2025) prior to the commencement of data collection. Permission to distribute the questionnaire was obtained from the management of each participating bank. Before beginning the questionnaire, all participants were presented with an information statement on the cover page explaining the purpose of the study, the voluntary nature of participation, the absence of right or wrong answers, and the strict confidentiality of responses, which were to be used solely for academic research purposes. Informed consent was implied by participants' voluntary completion and return of the questionnaire after reading this statement. No names, employee identifiers, or other personally identifiable information were collected; responses were analysed only in aggregate, individual banks are not identified in the reporting of results, and the data are stored securely and accessible only to the research team.

4. Results

This section reports the empirical results obtained from the integrated PLS-SEM model described in Section 3.4, estimated in SmartPLS 4 on a sample of 388 valid responses. Consistent with the two-step procedure recommended by Hair et al. (2022), the measurement model is assessed first, followed by the structural model, hypothesis testing, and a moderation analysis of the role played by COBIT-5 governance maturity (COB) in the relationship between cybersecurity effectiveness (CY) and the three CIA-based dimensions of cloud accounting risk: confidentiality risk (CON), availability risk (VAB), and integrity risk (INT). All reported statistics are taken verbatim from the SmartPLS 4 output, comprising the PLS-SEM algorithm report and the bootstrapping report (5000 subsamples).

4.1. Descriptive Statistics and Preliminary Correlations

Prior to model estimation, construct-level descriptive statistics and zero-order correlations were computed directly from the raw five-point Likert-scale responses (n = 388) to characterize response patterns and provide a transparent empirical basis for the subsequent

structural results. As shown in Table 2, all five construct means clustered near the scale midpoint (2.99–3.03 on a 1–5 scale)—a pattern that holds across constructs of differing theoretical direction (CY and COB positively framed, CON/VAB/INT risk-framed) and is discussed below—with standard deviations between 0.78 and 0.84, indicating meaningful response variance rather than ceiling/floor effects or uniform agreement bias. Skewness (−0.32 to 0.16) and excess kurtosis (−0.53 to −0.14) were well within the ±2 range conventionally regarded as consistent with approximate normality (Hair et al., 2022); this check is not required for PLS-SEM estimation but is reported as supplementary evidence of data quality ahead of the model comparisons in Section 4.9.

Table 2. Descriptive Statistics and Zero-Order Correlations.

Construct	Mean	SD	Skew.	Kurt.	COB	CY	CON	VAB
COB	2.99	0.81	0.09	−0.17	—			
CY	2.99	0.83	0.16	−0.53	0.376	—		
CON	3.00	0.84	−0.08	−0.14	−0.246	−0.494	—	
VAB	3.03	0.84	−0.32	−0.31	−0.244	−0.414	0.603	—
INT	3.01	0.78	−0.18	−0.29	−0.222	−0.474	0.609	0.608

Note. COB = COBIT-5 governance maturity; CY = cybersecurity effectiveness; CON = confidentiality risk; VAB = availability risk; INT = integrity risk; SD = standard deviation; Skew. = skewness; Kurt. = excess kurtosis. The right-hand panel reports zero-order Pearson correlations computed from the raw Likert-scale responses (n = 388); — denotes the diagonal of the correlation matrix.

The uniformity of these descriptive statistics warrants explicit comment. At the item level, responses were concentrated around the scale midpoint for all 20 items: the neutral option accounted for approximately 40% of responses, the adjacent options (2 and 4) for approximately 24% each, and the extreme options (1 and 5) for approximately 6% each, with very similar distributions across constructs. This is why all construct means lie close to 3.0 and their standard deviations are similar. This degree of uniformity is unusual, particularly because the cybersecurity effectiveness and COBIT-5 items are positively worded whereas the risk items are negatively framed. One possible contributing factor is a midpoint (central-tendency) response style (Baumgartner & Steenkamp, 2001), which may be encouraged when employees are asked to evaluate the security and governance of their own employer, a sensitive topic on which cautious answers are likely. We do not regard this as a complete explanation; the pattern is therefore reported transparently, the anonymized item-level dataset is provided as Supplementary Material File S1, and the pattern is acknowledged as a limitation in Section 7. The midpoint concentration does not, however, imply an absence of systematic covariation: the inter-construct correlations (Table 2) and the measurement and structural results reported below show a clear and theoretically consistent pattern of relationships.

The zero-order Pearson correlations reported in the right-hand panel of Table 2 correspond closely to the latent-variable correlations underlying the Fornell–Larcker matrix reported later in Section 4.3 (e.g., CY-CON = −0.494 raw vs. −0.495 latent; COB-CON = −0.246 in both). Because the latent scores are themselves weighted composites of these same indicators, this correspondence reflects internal consistency between the indicator- and construct-level analyses rather than independent validation; it nonetheless confirms that the pattern of relationships examined in the structural model (Section 4.6) is already visible in the raw indicator data before any latent-variable estimation is applied.

4.2. Measurement Model Assessment

The measurement model was evaluated on four criteria: indicator reliability (outer loadings), internal consistency reliability (Cronbach's α, rho_a, and composite reliability,

CR), convergent validity (Average Variance Extracted, AVE), and indicator-level collinearity (VIF). As shown in Table 3 and Figure 2, all 20 indicator loadings exceeded the 0.70 threshold recommended by Hair et al. (2022), ranging from 0.804 (CY2) to 0.886 (CON2), confirming strong indicator reliability across all five constructs without the need to remove any item. Internal consistency reliability was well established, with Cronbach's α ranging from 0.807 (VAB) to 0.897 (COB), rho_a from 0.812 to 0.899, and CR from 0.886 to 0.924, all comfortably above the 0.70 benchmark. Convergent validity was confirmed for every construct, with AVE values ranging from 0.687 (CY) to 0.757 (CON), all exceeding the 0.50 criterion (Fornell & Larcker, 1981). Indicator-level VIF values ranged from 1.684 to 2.391, well below the conservative threshold of 5.0, indicating no problematic collinearity among the indicators of any construct.

Table 3. Measurement Model: Indicator Loadings, Collinearity, Reliability, and Convergent Validity.

Construct	Item	Loading (λ)	VIF	α	rho_a	CR	AVE	Source
COBIT-5 Governance (COB)	COB1	0.850	2.315	0.897	0.899	0.924	0.709	Wolden et al. (2015)
	COB2	0.845	2.243					
	COB3	0.830	2.209					
	COB4	0.845	2.271					
	COB5	0.840	2.271					
Cybersecurity Effectiveness (CY)	CY1	0.816	1.967	0.886	0.886	0.916	0.687	Bulgurcu et al. (2010); D'Arcy et al. (2009)
	CY2	0.804	1.923					
	CY3	0.833	2.132					
	CY4	0.838	2.244					
	CY5	0.851	2.391					
Confidentiality Risk (CON)	CON1	0.856	1.921	0.840	0.841	0.904	0.757	Parsons et al. (2015)
	CON2	0.886	2.155					
	CON3	0.868	1.923					
Availability Risk (VAB)	VAB1	0.865	1.797	0.807	0.812	0.886	0.721	Ackermann et al. (2012); Armbrust et al. (2010)
	VAB2	0.846	1.684					
	VAB3	0.836	1.784					
Integrity Risk (INT)	INT1	0.815	1.865	0.852	0.854	0.900	0.693	Ackermann et al. (2012); Armbrust et al. (2010)
	INT2	0.840	2.005					
	INT3	0.818	1.801					
	INT4	0.857	2.100					

Note. λ = standardized outer loading; VIF = variance inflation factor; α = Cronbach's alpha; CR = composite reliability; AVE = average variance extracted (reported once per construct). All values meet established thresholds (λ ≥ 0.70; α/rho_a/CR ≥ 0.70; AVE ≥ 0.50; VIF < 5.0; Hair et al., 2022; Fornell & Larcker, 1981).

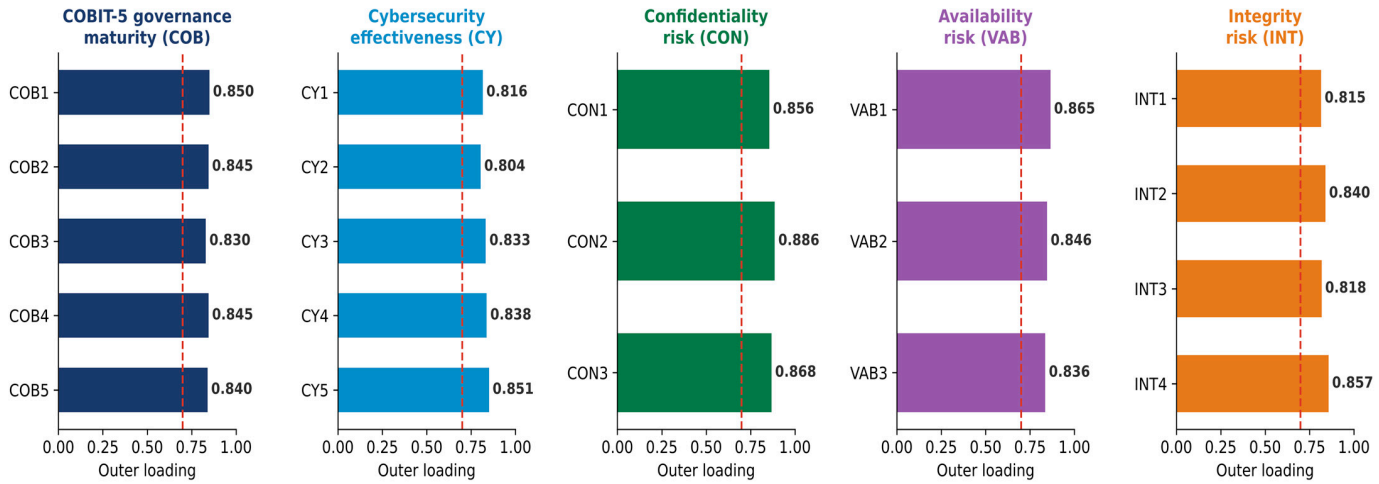


Figure 2. Outer loadings for all indicators, grouped by construct. The dashed reference line marks the 0.70 minimum-loading threshold (Hair et al., 2022); every indicator exceeds it. COB = COBIT-5 governance maturity; CY = cybersecurity effectiveness; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

4.3. Discriminant Validity

Discriminant validity was assessed through two complementary criteria: the traditional Fornell–Larcker criterion and the more diagnostic Heterotrait–Monotrait ratio (HTMT), which Henseler et al. (2015) demonstrated to detect discriminant validity violations that the Fornell–Larcker criterion can fail to identify. As shown in Table 4, the square root of the AVE for every construct (diagonal values, ranging from 0.829 to 0.870) exceeded its correlations with all other constructs, satisfying the Fornell–Larcker criterion. This conclusion is corroborated by the HTMT results in Table 5: every HTMT ratio remained below the conservative 0.85 threshold (Henseler et al., 2015), with the highest value (0.733, between INT and VAB) still comfortably below this cut-off. The convergence of both criteria provides strong evidence that the five constructs are empirically distinct from one another.

Table 4. Discriminant Validity: Fornell–Larcker Criterion.

	COB	CON	CY	INT	VAB
COB	**0.842**				
CON	−0.246	**0.870**			
CY	0.376	−0.495	**0.829**		
INT	−0.222	0.609	−0.475	**0.832**	
VAB	−0.248	0.601	−0.416	0.608	**0.849**

Note. Diagonal elements (bold) are the square roots of AVE; off-diagonal elements are inter-construct correlations. AVE = average variance extracted; CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

Table 5. Discriminant Validity: Heterotrait–Monotrait Ratio (HTMT).

	COB	CON	CY	INT
COB	—			
CON	0.283	—		
CY	0.422	0.573	—	
INT	0.254	0.720	0.545	—
VAB	0.286	0.731	0.490	0.733

Note. All HTMT ratios are below the conservative 0.85 threshold (Henseler et al., 2015), confirming discriminant validity. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

4.4. Structural Model Collinearity and Common Method Bias Assessment

Before interpreting path coefficients, inner (structural) model collinearity was assessed to rule out multicollinearity among the three predictor constructs entering each dependent variable. Inner VIF values were 1.177 for CY, 1.177 for COB, and 1.033 for the interaction term (CY × COB) on every endogenous construct, all far below the conservative 3.3 threshold (Hair et al., 2022), confirming that the structural estimates are not distorted by collinearity.

Common method bias (CMB) was assessed separately, because the inner VIF values above refer only to the predictors of each endogenous construct and therefore do not, by themselves, constitute a test of CMB. Following Kock (2015) and Kock and Lynn (2012), a full-collinearity assessment was conducted in which each latent variable was regressed on all other latent variables in the model, so that vertical and lateral collinearity are evaluated simultaneously; full-collinearity VIF values greater than 3.3 indicate that the model may be contaminated by common method variance. The full-collinearity VIFs, obtained from the latent-variable correlation matrix (Table 4), were 1.179 for COB, 1.548 for CY, 1.959 for CON, 1.944 for INT, and 1.858 for VAB—all well below 3.3. In addition, the highest inter-construct correlation (0.609, Table 4) is far below the 0.90 level that would signal a single dominant common factor (Bagozzi et al., 1991). Taken together with the procedural remedies described in Section 3.2, these results indicate that CMB is unlikely to pose a serious threat to the validity of the findings. Nevertheless, because all constructs were measured through self-reports from the same respondents at a single point in time, CMB cannot be ruled out entirely (see Section 7).

4.5. Coefficient of Determination (R^2) and Effect Size (f^2)

The coefficient of determination (R^2) indicates the proportion of variance in each endogenous construct explained jointly by CY, COB, and the CY × COB interaction term. As reported in Table 6, the model explained 30.6% of the variance in confidentiality risk (R^2 = 0.306, R^2adj = 0.301), 24.4% of the variance in availability risk (R^2 = 0.244, R^2adj = 0.238), and 32.3% of the variance in integrity risk (R^2 = 0.323, R^2adj = 0.318). The interpretation of these values depends on the benchmark adopted. Under Cohen's (1988) guidelines for the behavioral sciences (0.02 = small, 0.13 = medium, 0.26 = large), the R^2 values for confidentiality and integrity risk are large and that for availability risk is medium. Under the more demanding PLS-SEM benchmarks of Chin (1998) (0.19 = weak, 0.33 = moderate, 0.67 = substantial) and Hair et al. (2019) (0.25 = weak, 0.50 = moderate, 0.75 = substantial), however, the model's explanatory power is weak to moderate. We therefore interpret the R^2 values as modest but meaningful, for three reasons. First, the model is deliberately parsimonious: each risk dimension is explained by only two constructs and their interaction, whereas cloud accounting risk is also shaped by factors outside the scope of this study, such as cloud-provider practices, the external threat environment, and employee behavior. Second, the interaction term accounts for a non-trivial share of the explained variance: comparing the R^2 of the model with and without the CY × COB term (derived from the f^2 values reported in Figure 3) shows that the interaction adds approximately 5.7, 6.1, and 9.5 percentage points of explained variance in confidentiality, availability, and integrity risk, respectively. Third, acceptable R^2 levels depend on the research context (Hair et al., 2019), and the positive out-of-sample Q^2predict values (0.224–0.300; Section 4.9) indicate that the explained variance translates into predictive relevance. Accordingly, cybersecurity effectiveness and COBIT-5 governance maturity should be viewed as important, but not exhaustive, correlates of cloud accounting risk.

Table 6. Coefficient of Determination (R^2) for the Endogenous Constructs.

Endogenous Construct	R^2	R^2 Adjusted	Explanatory Power (Cohen, 1988; Hair et al., 2019)
Confidentiality Risk (CON)	0.306	0.301	Large/Weak–moderate
Availability Risk (VAB)	0.244	0.238	Medium/Weak
Integrity Risk (INT)	0.323	0.318	Large/Weak–moderate

Note. Classification under two benchmarks: Cohen (1988): 0.02 = small, 0.13 = medium, 0.26 = large; Hair et al. (2019): 0.25 = weak, 0.50 = moderate, 0.75 = substantial. Incremental R^2 attributable to the CY × COB interaction: CON = 0.057; VAB = 0.061; INT = 0.095. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

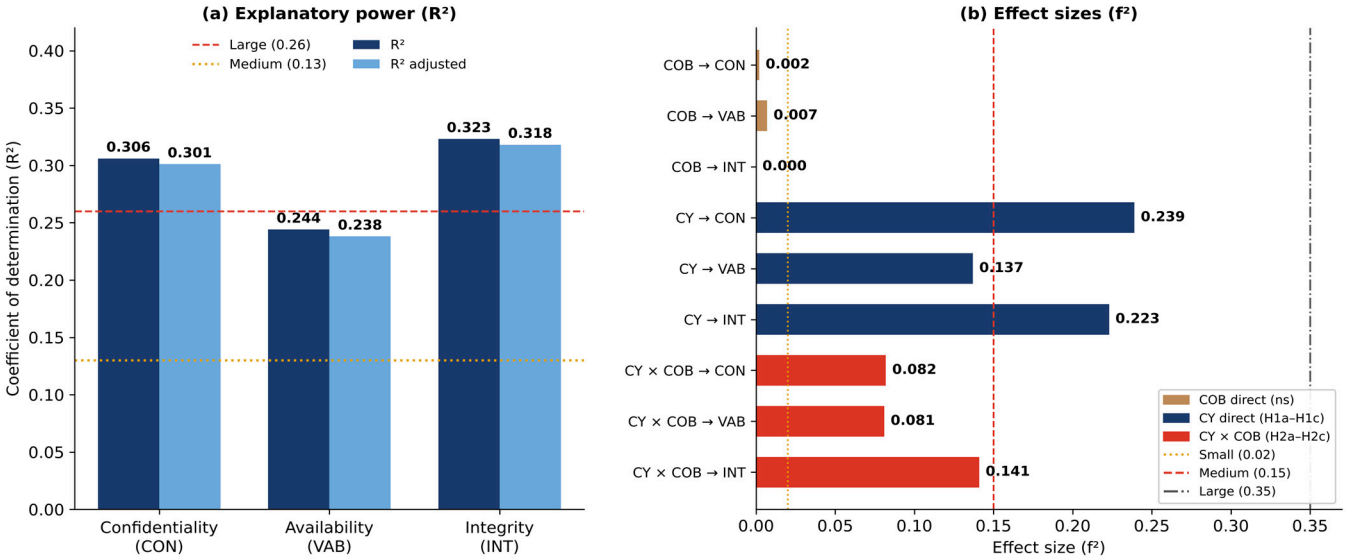


Figure 3. Explanatory power (R^2, R^2 adjusted) and effect sizes (f^2) for all structural paths, with Cohen's (1988) reference thresholds. In panel (**a**), the horizontal lines mark Cohen's medium (0.13) and large (0.26) benchmarks for explained variance; in panel (**b**), the vertical lines mark the small (0.02), medium (0.15), and large (0.35) effect-size benchmarks. ns = not significant; CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

Effect sizes (f^2) were computed for every structural path to assess each predictor's individual contribution to the explained variance of its dependent construct (Figure 3). Following Cohen's (1988) benchmarks (0.02 = small, 0.15 = medium, 0.35 = large), the direct path from cybersecurity effectiveness (CY) produced medium effect sizes for confidentiality and integrity risk (f^2 = 0.239 and 0.223) and a small-to-medium effect size for availability risk (f^2 = 0.137). The CY × COB interaction term produced f^2 values between 0.081 and 0.141, which are small-to-medium by Cohen's general benchmarks but large by the benchmarks proposed specifically for interaction effects (0.005, 0.01, and 0.025; Kenny, 2018). By contrast, the direct effect of COB alone was negligible in every case ($f^2 < 0.01$), consistent with the non-significant COB-only coefficients reported in Section 4.6.

4.6. Structural Model and Hypothesis Testing

Structural paths were tested using bootstrapping with 5000 subsamples, bias-corrected and accelerated (BCa) confidence intervals, and a two-tailed test at $\alpha = 0.05$, following the methodological recommendations of Hair et al. (2019). Figure 4 reproduces the structural model exactly as generated by SmartPLS 4, showing the inner and outer model structure estimated from the study data. Table 7 reports the complete bootstrapping results for the six

hypotheses stated in Section 2—the direct effects of cybersecurity effectiveness (H1a–H1c) and the moderating effects of COBIT-5 governance maturity (H2a–H2c).

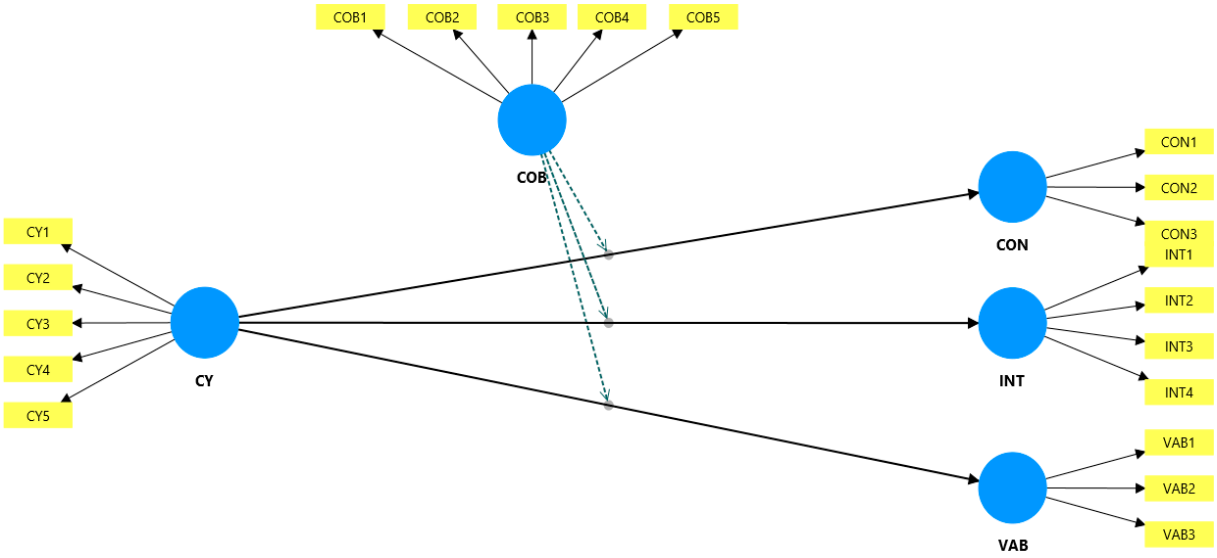


Figure 4. Structural (inner) and measurement (outer) model as generated directly by SmartPLS 4, showing all latent constructs, their indicators, and the estimated structural paths, including the CY × COB interaction term. Blue circles represent the latent constructs and yellow rectangles their indicators; solid arrows denote the measurement and structural paths; dashed green arrows denote the moderating effect of COB on each CY → risk path (the CY × COB interaction), and the grey nodes mark the point at which the moderator acts on each path. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; INT = integrity risk; VAB = availability risk.

Table 7. Bootstrapped Path Coefficients and Hypothesis Decisions.

H	Path	β	SD	*t*-Stat	*p*	95% CI	f^2	Decision
H1a	CY → CON	−0.442	0.043	10.312	<0.001	[−0.524,−0.359]	0.239	Supported
H1b	CY → VAB	−0.349	0.048	7.272	<0.001	[−0.439,−0.254]	0.137	Supported
H1c	CY → INT	−0.421	0.046	9.248	<0.001	[−0.511,−0.334]	0.223	Supported
H2a	CY × COB → CON	−0.229	0.038	5.952	<0.001	[−0.300,−0.149]	0.082	Supported
H2b	CY × COB → VAB	−0.237	0.039	6.096	<0.001	[−0.312,−0.159]	0.081	Supported
H2c	CY × COB → INT	−0.296	0.036	8.136	<0.001	[−0.367,−0.223]	0.141	Supported

Note. β = standardized path coefficient; SD = bootstrap standard deviation; *t* = two-tailed *t*-statistic; → = direction of the structural path; 95% CI = bias-corrected and accelerated (BCa) bootstrap confidence interval; f^2 = Cohen's (1988) effect size. All six hypothesized paths are statistically supported. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

For model completeness, the direct (non-hypothesized) path from COBIT-5 governance maturity to each risk dimension, net of the interaction term, was also estimated: none reached statistical significance (CON: β = −0.044, p = 0.389; VAB: β = −0.079, p = 0.117; INT: β = −0.017, p = 0.727). This finding is interpreted in Section 5.3.

4.7. Model Fit and Model Selection Criteria

Table 8 reports global model fit indices. The estimated model produced an SRMR of 0.104, moderately above the conservative 0.08 rule of thumb but which may partly reflect the additional model complexity introduced by the two-stage interaction term (CY × COB) described in Section 3.4; because SRMR thresholds have not been validated for PLS-SEM models that include interaction terms, this value is interpreted with caution

rather than as evidence of acceptable fit (Henseler et al., 2016; Hair et al., 2022). The NFI value of 0.857, while below the traditional 0.90 benchmark, is consistent with typical values observed in PLS-SEM models with a moderate number of indicators and a two-stage interaction term (Hair et al., 2022); absolute fit indices in PLS-SEM are, in any case, regarded as supplementary diagnostics rather than criteria for model acceptance or rejection (Hair et al., 2019).

Table 8. Model Fit Indices.

Index	Saturated Model	Estimated Model
SRMR	0.045	0.104
d_ULS	0.431	2.267
d_G	0.202	0.301
Chi-square	467.087	616.311
NFI	0.892	0.857

Note. SRMR = Standardized Root Mean Square Residual; d_ULS = squared Euclidean distance; d_G = geodesic distance; NFI = Normed Fit Index.

As a supplementary model-selection check, the Bayesian Information Criterion (BIC) was examined (Table 9). Because BIC is a relative criterion, its absolute value—including its sign—carries no meaning on its own, and BIC values cannot be compared across different endogenous constructs; it is informative only when competing models of the same construct are compared, with the lower value indicating the preferred balance between fit and parsimony (P. N. Sharma et al., 2019). We therefore compared the hypothesized model with a competing main-effects model that excludes the CY × COB interaction term. For all three risk dimensions, the model including the interaction term yielded the lower BIC (CON: −118.97 vs. −94.24; VAB: −85.67 vs. −61.37; INT: −128.58 vs. −83.33), with ΔBIC values of 24.3 to 45.3, well above the value of 10 conventionally interpreted as very strong evidence in favor of the model with the lower BIC (Raftery, 1995). This indicates that the improvement in explained variance obtained by adding the moderating term more than compensates for the additional parameter, supporting the specification of COBIT-5 as a moderator rather than only as an additional predictor.

Table 9. Model Selection Criteria (Bayesian Information Criterion).

Endogenous Construct	BIC
Confidentiality Risk (CON)	−118.974
Availability Risk (VAB)	−85.667
Integrity Risk (INT)	−128.582

Note. BIC is a relative criterion: values are comparable only between alternative models of the same endogenous construct, with lower values preferred (P. N. Sharma et al., 2019). BIC of the competing main-effects model (without CY × COB): CON = −94.24; VAB = −61.37; INT = −83.33. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

4.8. Moderation Analysis: Simple Slope Analysis

To further probe the form of the interaction confirmed in H2a–H2c, a simple slope analysis was conducted, estimating the conditional effect of cybersecurity effectiveness (CY) on each risk dimension at three levels of COBIT-5 governance maturity: one standard deviation below the mean (−1 SD, low governance maturity), at the mean, and one standard deviation above the mean (+1 SD, high governance maturity). As shown in Table 10, the risk-reducing effect of cybersecurity effectiveness strengthens monotonically and substantially as COBIT-5 maturity rises across all three risk dimensions. For confidentiality risk, the conditional effect of CY strengthens from $\beta = -0.213$ ($p = 0.0012$) at low governance

maturity to β = −0.671 ($p < 0.001$) at high governance maturity—roughly a three-fold increase in magnitude. The pattern is even more pronounced for availability and integrity risk: the conditional effect of CY on availability risk is not statistically significant at low governance maturity (β = −0.111, $p = 0.107$) but becomes strongly significant at high maturity (β = −0.586, $p < 0.001$); the same pattern holds for integrity risk (β = −0.125, $p = 0.064$, not significant at low maturity, versus β = −0.718, $p < 0.001$, at high maturity).

Table 10. Simple Slope Analysis: Conditional Effects of CY on Cloud Accounting Risk at Three Levels of COB.

Path	COB −1 SD (Low)	COB Mean	COB +1 SD (High)
CY → CON	β = −0.213, $t = 3.24$, $p = 0.0012$	β = −0.442, $t = 10.31$, $p < 0.001$	β = −0.671, $t = 13.94$, $p < 0.001$
CY → VAB	β = −0.111, $t = 1.61$, $p = 0.107$ (ns)	β = −0.349, $t = 7.27$, $p < 0.001$	β = −0.586, $t = 10.96$, $p < 0.001$
CY → INT	β = −0.125, $t = 1.85$, $p = 0.064$ (ns)	β = −0.421, $t = 9.25$, $p < 0.001$	β = −0.718, $t = 15.23$, $p < 0.001$

Note. Conditional (simple slope) effects estimated via SmartPLS 4 at COB −1 SD, mean, and +1 SD. ns = not significant at α = 0.05. SD = standard deviation; CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

This pattern carries a substantively important implication that extends beyond the average interaction effect reported in Table 7: for banks with low COBIT-5 governance maturity, cybersecurity effectiveness is associated with a materially weaker, and for two of the three CIA dimensions statistically undetectable, reduction in cloud accounting risk. The protective value of cybersecurity spending therefore appears to be conditional on—not independent of—the surrounding IT governance infrastructure.

4.9. Predictive Relevance: PLSpredict and CVPAT

Beyond the in-sample explanatory power reported in Section 4.5, the model's out-of-sample predictive relevance was assessed using PLSpredict (Shmueli et al., 2019), a holdout-based k-fold cross-validation procedure (k = 10 folds, 10 repetitions, fixed seed). PLSpredict generates a Q^2predict statistic for each endogenous construct, with values greater than zero indicating that the PLS-SEM model outperforms the most naïve benchmark (the indicator mean). As reported in Table 11, all three endogenous constructs achieved positive Q^2predict values—confidentiality risk (Q^2predict = 0.289), integrity risk (Q^2predict = 0.300), and availability risk (Q^2predict = 0.224)—confirming that the model possesses meaningful predictive relevance for all three risk dimensions. Following the indicator-level comparison rule recommended by Shmueli et al. (2019), the PLS-SEM prediction error, measured by the root mean square error (RMSE), was lower than the linear-model (LM) benchmark for all 10 manifest indicators of the three endogenous constructs (Q^2predict ranging from 0.148 to 0.233 at the item level). Because the conclusion about predictive power rests on this indicator-level comparison, the full results are reported in Appendix B (Table A2) and are discussed here. Following Shmueli et al. (2019), the prediction errors were first inspected; because they were approximately symmetric (skewness between −0.06 and 0.26), RMSE was used as the primary metric, with the mean absolute error (MAE) reported as a robustness check. PLS-SEM produced a lower RMSE than the LM benchmark for all 10 indicators (Δ RMSE ranging from −0.057 to −0.029) and a lower MAE for all 10 indicators. According to the decision rule of Shmueli et al. (2019), this pattern indicates high predictive power. The differences are, however, small in absolute terms, which is expected because the LM benchmark regresses each indicator directly on all exogenous indicators without imposing the measurement model; the predictive advantage of the PLS-SEM model should therefore be interpreted as consistent but modest. Whether

this advantage is statistically significant, rather than merely descriptive, is tested with CVPAT below.

Table 11. PLSpredict Construct-Level Predictive Relevance (k = 10 folds, 10 repetitions).

Endogenous Construct	Q^2predict	PLS-SEM RMSE	PLS-SEM MAE
Confidentiality Risk (CON)	0.289	0.848	0.674
Availability Risk (VAB)	0.224	0.886	0.717
Integrity Risk (INT)	0.300	0.841	0.679

Note. Q^2predict > 0 indicates the model outperforms the indicator-mean benchmark; RMSE = root mean square error; MAE = mean absolute error. Consistent with Shmueli et al. (2019), the PLS-SEM RMSE was lower than the linear-model (LM) benchmark RMSE for all 10 indicators (item-level results are reported in Appendix B, Table A2), confirming high predictive power across the full measurement model. CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

To formally test whether the model's predictive accuracy is statistically superior to competing benchmarks, the cross-validated predictive ability test (CVPAT; Liengaard et al., 2021; P. N. Sharma et al., 2023) was conducted, comparing the PLS-SEM model's average prediction loss against two benchmarks: a naïve indicator-average (IA) model and a linear regression (LM) model. As shown in Table 12, the PLS-SEM model produced a significantly lower prediction loss than both benchmarks for every endogenous construct and overall (all $p < 0.001$ against IA; all $p < 0.01$ against LM), providing rigorous statistical evidence—beyond the descriptive Q^2predict criterion—that the specified structural model possesses genuine out-of-sample predictive ability rather than merely in-sample explanatory fit.

Table 12. Cross-Validated Predictive Ability Test (CVPAT): PLS-SEM vs. Indicator-Average (IA) and Linear-Model (LM) Benchmarks.

Construct	PLS Loss	IA Loss	Diff. (vs. IA)	t (vs. IA)	*p* (vs. IA)	LM Loss	Diff. (vs. LM)	t (vs. LM)	*p* (vs. LM)
CON	0.735	0.940	−0.205	5.549	<0.001	0.797	−0.062	3.682	<0.001
VAB	0.822	0.978	−0.157	4.202	<0.001	0.882	−0.061	3.090	0.002
INT	0.703	0.887	−0.184	5.434	<0.001	0.779	−0.076	4.146	<0.001
Overall	0.748	0.931	−0.182	5.768	<0.001	0.815	−0.067	4.550	<0.001

Note. PLS loss, IA loss, and LM loss are average out-of-sample prediction losses; negative differences indicate PLS-SEM outperforms the benchmark. All differences are statistically significant, confirming the model's superior predictive accuracy over both naïve and conservative benchmarks (Liengaard et al., 2021). CY = cybersecurity effectiveness; COB = COBIT-5 governance maturity; CON = confidentiality risk; VAB = availability risk; INT = integrity risk.

5. Discussion

This study examined how cybersecurity effectiveness (CY) and COBIT-5 governance maturity (COB) are jointly associated with cloud accounting risk across the three CIA dimensions—confidentiality, availability, and integrity—in Jordanian commercial banks. Grounded in IT Governance Theory (Weill & Ross, 2004) and Risk Management Theory (Rausand, 2011), and estimated through a single integrated PLS-SEM model (n = 388), the empirical results support all six hypotheses (H1a–H1c and H2a–H2c).

5.1. Direct Effects of Cybersecurity Effectiveness on CIA Risk Dimensions (H1a–H1c)

H1a–H1c were all supported: cybersecurity effectiveness was significantly and negatively associated with confidentiality, availability, and integrity risk alike (Table 7). Substantively, banks whose employees perceive cybersecurity controls—access management,

encryption, intrusion detection, and identity governance—as more effective report correspondingly lower exposure to unauthorized disclosure of customer data, disruption of cloud accounting service availability, and unauthorized alteration of accounting records. This finding is consistent with Risk Management Theory (Rausand, 2011): cybersecurity effectiveness functions as a risk-treatment capability through which organizations prevent, detect, respond to, and recover from threats to financial information, which would be expected to reduce the likelihood and consequences of cyber risk across all three CIA dimensions; given the cross-sectional design, however, the results document a negative association consistent with this mechanism rather than establishing it causally. The association was strongest for confidentiality risk ($f^2 = 0.239$), followed by integrity risk ($f^2 = 0.223$), and weakest—though still highly significant—for availability risk ($f^2 = 0.137$). One plausible explanation, though this study did not directly measure budget allocation, is that cybersecurity budgets in the Jordanian banking sector may be more heavily weighted toward confidentiality- and integrity-protecting controls (encryption, access privileges, file-integrity monitoring) than toward business-continuity and disaster-recovery capability, which more directly governs availability risk (Endo et al., 2016). This interpretation, however, remains inferred from the effect-size gradient rather than directly evidenced, and warrants confirmation through future research that measures control-specific investment directly.

5.2. The Moderating Role of COBIT-5 Governance Maturity (H2a–H2c)

The confirmation of H2a, H2b, and H2c constitutes this study's central contribution: the CY × COB interaction term was significant and negative across all three dimensions (Table 7). Since both variables were standardized before computing the interaction, this negative sign—layered onto CY's already-negative direct path—indicates that the negative association between cybersecurity effectiveness and risk becomes stronger as COBIT-5 maturity rises. The simple slope analysis (Table 10) clarifies this pattern: the negative association between CY and confidentiality risk roughly triples in magnitude between low and high maturity ($\beta = -0.213$ to -0.671), whereas for availability and integrity risk it is not statistically significant at low maturity ($p = 0.107$ and $p = 0.064$, respectively) and becomes strongly significant at high maturity. This result is consistent with IT Governance Theory (Weill & Ross, 2004), which holds that value from IT investment is realized only when decision rights, accountability structures, and control mechanisms are explicitly governed; cybersecurity spending absent such governance risks being fragmented, poorly prioritized, and consequently less effective at mitigating risk. COBIT-5's governance and management objectives—including APO12 (Manage Risk), DSS05 (Manage Security Services), and MEA03 (Monitor, Evaluate and Assess Compliance with External Requirements)—provide the accountability structures, risk-appetite alignment, and continuous monitoring mechanisms that make cybersecurity investment more targeted, better prioritized, and more auditable, rather than a technically isolated expenditure disconnected from strategic risk decisions (Al-Fatlawi et al., 2021; ISACA, 2012). This interpretation aligns with the regional banking literature: Al-Gasaymeh et al. (2023) found that COBIT-5 improved governance-tool effectiveness in Jordanian commercial banks, and Al-Hakim et al. (2021) reported it reduced credit risk in Islamic banks under a comparable regulatory regime. Al-Tayan et al. (2026) and van Wyk and Rudman (2019) similarly linked higher COBIT-5 maturity to improved operational stability and reduced downtime, supporting the amplification pattern found here for availability risk. This study extends that literature by showing, within one integrated structural model, that COBIT-5 operates as a conditioning mechanism across all three CIA dimensions simultaneously—rarely tested jointly in prior work. This contribution should be stated precisely: the study does not propose a new theory of cybersecurity governance. Its contribution is empirical and theory-refining. It specifies and tests COBIT-5

governance maturity as a boundary condition of the established relationship between cybersecurity effectiveness and cloud accounting risk, and it shows that this boundary condition operates differently across confidentiality, integrity, and availability. The theoretical value of the study therefore lies in clarifying when, and for which CIA dimension, existing IT governance and risk management arguments hold, rather than in replacing them. Notably, the moderating effect of COBIT-5 was not uniform across the three dimensions. In absolute terms, the interaction was strongest for integrity risk ($\beta = -0.296$, $f^2 = 0.141$), whereas it was of similar magnitude for confidentiality risk ($\beta = -0.229$, $f^2 = 0.082$) and availability risk ($\beta = -0.237$, $f^2 = 0.081$). The simple slopes (Table 10), however, show that the practical consequence of governance maturity is most pronounced for availability and integrity risk: in both cases, the association between cybersecurity effectiveness and risk is not statistically significant at low COBIT-5 maturity and becomes strong at high maturity, whereas for confidentiality risk it remains significant even at low maturity. Moreover, relative to its weaker direct path ($\beta = -0.349$), the interaction for availability risk is proportionally larger than that for confidentiality risk, suggesting that governance maturity may be particularly valuable where technical cybersecurity controls appear relatively under-weighted. This is consistent with COBIT-5's DSS04 (Continuity Management) and BAI04 (Availability and Capacity Management) processes, which institutionalize the continuous testing and escalation of resilience-related controls (Section 2.4)—indicating that banks may derive greater marginal benefit from elevating governance maturity precisely in domains where technical controls remain comparatively underdeveloped.

5.3. The Non-Significant Direct Effect of COBIT-5 Governance

A theoretically important finding of this study is that COBIT-5 governance maturity showed no significant direct association with any of the three cloud accounting risk dimensions when estimated independently of its interaction with cybersecurity effectiveness (CON: $\beta = -0.044$, $p = 0.389$; VAB: $\beta = -0.079$, $p = 0.117$; INT: $\beta = -0.017$, $p = 0.727$; Section 4.6). This result should not be read as evidence that COBIT-5 governance is unimportant; rather, it clarifies precisely how COBIT-5 contributes to risk reduction. Consistent with IT Governance Theory (Weill & Ross, 2004), COBIT-5 is, by design, an enabling governance framework rather than a technical control: it does not itself detect intrusions, encrypt data, or restore service continuity. Its value materializes only through the technical and operational mechanisms it governs—chief among them, cybersecurity effectiveness. The statistical signature obtained here—a significant interaction effect combined with a non-significant main effect of the moderator—is the expected pattern for a "pure" moderator variable (S. Sharma et al., 1981) and provides internally consistent evidence that COBIT-5 amplifies cybersecurity's risk-mitigating effect rather than substituting for it or independently reducing risk. This finding should be read as evidence against a detectable independent main effect within the estimated model, not as proof that COBIT-5 cannot influence cloud accounting risk through any other mechanism or non-linear pathway; future research using alternative specifications (e.g., mediation models, non-linear terms) could further probe this possibility. Within the limits of the cross-sectional design, the results therefore suggest that banks adopting COBIT-5 without a commensurate investment in cybersecurity effectiveness may not observe a measurable reduction in cloud accounting risk from governance adoption alone.

6. Conclusions

This study examined the effect of cybersecurity effectiveness on the three CIA-based dimensions of cloud accounting risk—confidentiality, availability, and integrity—in Jordanian commercial banks, and tested the moderating role of COBIT-5 governance maturity in

this relationship. Using an integrated PLS-SEM model on a sample of 388 valid responses, the results show that cybersecurity effectiveness is significantly associated with lower levels of all three risk dimensions, and that this negative association strengthens significantly as COBIT-5 governance maturity increases, while COBIT-5 governance maturity alone shows no statistically detectable direct association with cloud accounting risk. The model's out-of-sample predictive relevance was further confirmed through PLSpredict and the cross-validated predictive ability test (CVPAT), which showed that the specified structural model significantly outperformed both naive and conservative benchmark models in predicting all three risk dimensions. Collectively, and bearing in mind that cross-sectional data identify associations rather than causal effects, these findings are consistent with the view, grounded in IT Governance Theory and Risk Management Theory, that the value of technical IT-governance frameworks lies primarily in their capacity to condition and amplify operational risk controls, not in an independent, stand-alone risk-reduction effect.

6.1. Theoretical Contributions

This study contributes to the literature in three ways. First, it provides a rigorous empirical test of COBIT-5 as a moderating variable within one integrated structural model spanning all three CIA dimensions simultaneously. Second, it demonstrates that IT Governance Theory (Weill & Ross, 2004) and Risk Management Theory (Rausand, 2011) operate complementarily: risk-treatment capability (cybersecurity effectiveness) is associated with lower risk, while governance structure (COBIT-5) conditions the strength of that association. Third, disaggregating cloud accounting risk into its three CIA sub-dimensions reveals that both effects vary meaningfully across dimensions—most notably, availability risk's comparatively weaker direct association ($f^2 = 0.137$), the largest interaction for integrity risk ($f^2 = 0.141$), and the fact that for both availability and integrity risk the association with cybersecurity effectiveness is detectable only at average-to-high governance maturity—opening a more granular research agenda for each dimension individually.

6.2. Practical Implications

The findings carry implications for three stakeholder groups. For bank executives, they reframe cybersecurity and IT governance from two competing budget lines into one interdependent investment: the findings suggest that investment in either alone is associated with a smaller, and sometimes statistically undetectable, reduction in perceived risk; accordingly, cybersecurity initiatives should be integrated within a unified COBIT-5 governance structure, rather than treated as separate technical and administrative functions, guided by formal mechanisms—notably APO12, DSS05, and MEA03. For IT audit and risk-management functions, the uneven protective association across the three CIA dimensions signals where control portfolios are under-weighted; cybersecurity investment should accordingly be rebalanced toward business-continuity and disaster-recovery capability, given availability risk's comparatively weaker protective effect relative to confidentiality and integrity, supported by recurring staff training that links COBIT-5 requirements to day-to-day cybersecurity practice and by periodic—not solely annual—reviews of control effectiveness against governance-maturity indicators, treating both as continuous improvement inputs rather than static compliance exercises. For banking supervisors, including the Central Bank of Jordan, the non-significant direct effect of governance maturity offers an empirical basis for incorporating COBIT-5 (or equivalent) governance-maturity indicators into supervisory risk assessments alongside cybersecurity-specific requirements, regulating the two as complements rather than independently sufficient requirements.

7. Limitations and Future Research

This study has six limitations. First, the purposive sampling strategy across the 13 Jordanian banks limits statistical generalizability, and, although the response rate was high (97.0% valid responses), no complete sampling frame of eligible employees was available against which representativeness could be formally assessed; moreover, because the respondent's bank was not recorded, the representation of individual banks in the sample cannot be verified. Second, because the data are cross-sectional and self-reported, the relationships identified should be interpreted as associations rather than causal effects, and reverse or reciprocal relationships cannot be excluded (for example, banks experiencing lower cloud accounting risk may also perceive their controls as more effective); common method variance likewise cannot be entirely ruled out, notwithstanding the procedural remedies (Section 3.2) and the full-collinearity assessment (Section 4.4). Future studies could address this by using longitudinal or multi-source designs that combine employee perceptions with objective incident data or audit findings. In addition, responses were concentrated around the scale midpoint for all constructs (Section 4.1), which may reflect a central-tendency response style and limits the variance available for detecting relationships; replication with other samples and instruments is therefore needed. Third, the sample was restricted to Jordanian commercial banks, constraining generalizability to other financial subsectors or emerging-market banking systems. Fourth, the estimated model's SRMR (0.104) exceeds the conservative 0.08 guideline, likely reflecting the interaction term's added complexity; this is common in PLS-SEM moderation models but remains a genuine, unresolved caveat for overall model fit. Fifth, cloud accounting risk was operationalized solely through the three CIA-triad dimensions, excluding other relevant dimensions such as accountability or non-repudiation. Sixth, COBIT-5 rather than COBIT 2019 was deliberately used to operationalize governance maturity, for the regulatory, familiarity, and measurement reasons explained in Section 2.6; the findings should be extended to COBIT 2019 or other frameworks only with appropriate caution. Future research should pursue longitudinal designs tracking how COBIT-5 maturity co-evolves with cloud accounting risk; extend the model with mediators such as organizational risk culture; test the moderating pattern's external validity in other emerging markets; and compare alternative governance frameworks (e.g., COBIT 2019, ISO/IEC 27001, NIST) as parallel moderators to determine whether the amplifying pattern is COBIT-5-specific or general to mature IT governance.

Supplementary Materials: The following supporting information can be downloaded at: https://www.mdpi.com/article/10.3390/ijfs14110291/s1, File S1: Anonymized item-level survey dataset (n = 388; Microsoft Excel format).

Author Contributions: Conceptualization, M.I.A.; methodology, M.I.A.; software, M.I.A.; validation, M.I.A., I.S.A.-R., R.A., M.A., M.S.A. and A.T.; formal analysis, M.I.A.; investigation, M.I.A.; resources, M.I.A.; data curation, M.I.A.; writing—original draft preparation, M.I.A.; writing—review and editing, I.S.A.-R., R.A., M.A., M.S.A. and A.T.; visualization, M.I.A.; supervision, M.I.A.; project administration, M.I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: The study was conducted in accordance with the Declaration of Helsinki and was approved by the Research Ethics Committee, Faculty of Business, Jadara University (Decision No. 3, Ref. EC32025; Session No. 2, 16 November 2025) prior to the commencement of data collection.

Informed Consent Statement: Informed consent was obtained from all subjects involved in the study.

Data Availability Statement: The anonymized item-level survey data analyzed in this study (n = 388) are provided as Supplementary Material File S1.

Acknowledgments: The authors used Claude Opus 5 (Anthropic PBC, San Francisco, CA, USA) solely for language editing and improving the clarity of the text. The authors reviewed all modifications and take full responsibility for the content of the manuscript.

Conflicts of Interest: The authors declare no conflicts of interest.

Appendix A. Questionnaire Items

Table A1 lists all measurement items in their English version (the questionnaire was administered in Arabic after translation and back-translation; Section 3.3). All items were rated on a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). For the risk constructs, higher scores denote higher perceived risk. The questionnaire also included a cover statement (Section 3.5) and a demographic section (gender, age, education, professional specialization, years of experience, and bank type).

Table A1. Measurement Items, Sources, and Adaptation.

Code	Item (English Version, as Administered)	Source	Adaptation
Cybersecurity Effectiveness (CY)			
CY1	The bank deploys robust encryption protocols to safeguard sensitive financial data stored in and transmitted through cloud accounting systems.	Bulgurcu et al. (2010); D'Arcy et al. (2009)	Adapted from the individual level to the organizational (bank) level
CY2	The bank enforces strict role-based access control (RBAC) policies that restrict cloud accounting data access to authorized personnel only.		
CY3	The bank implements multi-factor authentication (MFA) across all cloud accounting platforms and financial applications.		
CY4	The bank continuously monitors cloud accounting environments using intrusion detection and prevention systems (IDS/IPS).		
CY5	The bank conducts regular security audits and vulnerability assessments of its cloud accounting infrastructure.		
COBIT-5 Governance Maturity (COB)			
COB1	The bank has clearly defined and documented IT governance policies that assign accountability for cybersecurity and cloud accounting risk management.	Wolden et al. (2015)	Adapted to the bank's cloud accounting context
COB2	COBIT-5 governance mechanisms are consistently applied to monitor and enforce compliance with regulatory requirements governing cloud-based financial data.		
COB3	The bank's cybersecurity investments are strategically aligned with organizational risk priorities and business objectives through COBIT-5 governance processes.		

Table A1. *Cont.*

Code	Item (English Version, as Administered)	Source	Adaptation
COB4	The bank employs structured IT risk assessment procedures (consistent with COBIT-5 principles) to systematically identify and mitigate cloud accounting vulnerabilities.		
COB5	COBIT-5 governance frameworks within the bank ensure continuous performance monitoring and systematic evaluation of IT security controls.		
Data Confidentiality Risk (CON)			
CON1	The bank's cloud accounting systems are at significant risk of unauthorized external access to sensitive financial transaction records.	Parsons et al. (2015)	Adapted to the cloud banking context
CON2	The multi-tenant architecture of the bank's cloud environment poses substantial risks of financial data leakage or inadvertent disclosure to unauthorized parties.		
CON3	Transferring financial accounting data to external cloud service providers creates meaningful vulnerabilities to confidentiality breaches and regulatory non-compliance.		
Data Availability Risk (VAB)			
VAB1	Disruptions or outages from the bank's cloud service provider pose a significant risk to the continuity of cloud-based accounting and financial reporting operations.	Ackermann et al. (2012); Armbrust et al. (2010)	Adapted to the cloud banking context
VAB2	Distributed Denial-of-Service (DDoS) attacks targeting the bank's cloud infrastructure present a substantial threat to the availability of accounting systems and financial data.		
VAB3	The bank's reliance on a single external cloud service provider creates critical availability risks due to insufficient redundancy and disaster recovery capabilities.		
Data Integrity Risk (INT)			
INT1	Cloud accounting systems are vulnerable to unauthorized modification of financial records.	Ackermann et al. (2012); Armbrust et al. (2010)	Operationalized within the CIA information security framework
INT2	Cyberattacks may compromise the accuracy and completeness of accounting data stored in cloud environments.		
INT3	The bank faces risks of data corruption that could adversely affect the reliability of financial reporting.		
INT4	Weak change-management controls may allow unauthorized alterations to accounting information.		

Appendix B. Item-Level PLSpredict Results

Table A2. Item-Level PLSpredict Results: PLS-SEM versus Linear-Model (LM) Benchmark (k = 10 folds, 10 repetitions).

Indicator	Q^2predict	PLS-SEM RMSE	LM RMSE	Δ RMSE (PLS − LM)	PLS-SEM MAE	LM MAE
CON1	0.209	0.871	0.910	−0.040	0.681	0.724
CON2	0.229	0.825	0.860	−0.035	0.663	0.695
CON3	0.233	0.869	0.906	−0.037	0.691	0.731
VAB1	0.190	0.885	0.923	−0.038	0.708	0.737
VAB2	0.158	0.914	0.943	−0.029	0.730	0.759
VAB3	0.148	0.911	0.949	−0.038	0.738	0.781
INT1	0.192	0.843	0.887	−0.044	0.662	0.706
INT2	0.214	0.824	0.870	−0.046	0.641	0.701
INT3	0.233	0.810	0.867	−0.057	0.640	0.701
INT4	0.224	0.860	0.906	−0.046	0.685	0.737

Note. Results obtained with PLSpredict (k = 10 folds, 10 repetitions) for the model specified in Section 3.4; because fold assignment is random, values may differ marginally across runs. Negative Δ RMSE values indicate that PLS-SEM predicts the indicator more accurately than the LM benchmark. Following Shmueli et al. (2019), predictive power is high when PLS-SEM outperforms LM for all indicators, medium for the majority, low for a minority, and absent for none.

References

Ackermann, T., Widjaja, T., Benlian, A., & Buxmann, P. (2012, December 16–19). *Perceived IT security risks of cloud computing: Conceptualization and scale development*. 33rd International Conference on Information Systems (ICIS 2012), Orlando, FL, USA. Available online: https://aisel.aisnet.org/icis2012/proceedings/ISSecurity/3/ (accessed on 21 August 2026).

Adrian, F. X., & Wang, G. (2023). Measure the level capability IT governance in effectiveness internal control for cybersecurity using the COBIT 2019 in organization: Banking company. *Journal of Theoretical and Applied Information Technology*, *101*(5), 1710–1723. Available online: http://www.jatit.org/volumes/Vol101No5/9Vol101No5.pdf (accessed on 21 August 2026).

Agarwal, A., Verma, S. B., & Gupta, B. K. (2023). A review of cloud security issues and challenges. *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, *12*, e31459. [CrossRef]

AL-Alawamreh, M. I., Al-alawnh, N. A. K., Thaer, A., Hani, L. Y. B., & Quraan, A. A. (2026). The interactive impact of adopting digital twins and AI on the relationship between cybersecurity and cloud accounting in Jordanian banks. In *Computational intelligence for business analytics and decision systems* (pp. 549–559). Springer. [CrossRef]

Al-Fatlawi, Q. A., Al Farttoosi, D. S., & Almagtome, A. H. (2021). Accounting information security and IT governance under COBIT 5 framework: A case study. *Webology*, *18*(2), 294–310. [CrossRef]

Al-Gasaymeh, A., Qasaimeh, G. M., Alrawashdeh, N., Alsmadi, A. A., & Alzoubi, H. M. (2023). The impact of COBIT 5 on the effectiveness of applying governance tools in Jordanian commercial banks. *Quality—Access to Success*, *24*(194), 377–384. [CrossRef]

Al-Hakim, M. S., Khrais, I., Alsadi, K., & Khasawneh, Y. (2021, December 21–23). *The impact of using information technology governance COBIT5 in reducing banking credit risk in Islamic banks—Case study of Islamic International Arab Bank*. 2021 22nd International Arab Conference on Information Technology (ACIT) (pp. 1–12), Muscat, Oman. [CrossRef]

Ali, O. M., Matarneh, A. J., Almalkawi, A., & Mohamed, H. (2020). The impact of cyber governance in reducing the risk of cloud accounting in Jordanian commercial banks. *Modern Applied Science*, *14*(3), 75–89. [CrossRef]

Al-Khatib, S. F., Ibrahim, Y. Y., & Alnadi, M. (2025). Cybersecurity practices and supply chain performance: The case of Jordanian banks. *Administrative Sciences*, *15*(1), 1. [CrossRef]

Allianz. (2026). *Allianz risk barometer 2026: Identifying the major business risks for 2026*. Allianz Global Corporate & Specialty. Available online: https://commercial.allianz.com/news-and-insights/news/allianz-risk-barometer-2026.html (accessed on 21 August 2026).

Al-Tayan, R., Khatatbeh, I. N., Daradkah, D., Shehadeh, M., & Alzawahreh, H. (2026). Does COBIT framework adoption influence banks' financial stability? Evidence from an emerging country. *Risks*, *14*(6), 138. [CrossRef]

Amer, T. B., & Al-Omar, M. I. A. (2023). The impact of cyber security on preventing and mitigating electronic crimes in the Jordanian banking sector. *International Journal of Advanced Computer Science and Applications*, *14*(8), 371–380. [CrossRef]

Anyanwu, A., Olorunsogo, T., Abrahams, T. O., Akindote, O. J., & Reis, O. (2024). Data confidentiality and integrity: A review of accounting and cybersecurity controls in superannuation organizations. *Computer Science & IT Research Journal*, *5*(1), 237–253. [CrossRef]

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Stoica, I. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. [CrossRef]

Asadi, S., Nilashi, M., Husin, A. R. C., & Yadegaridehkordi, E. (2017). Customers perspectives on adoption of cloud computing in banking sector. *Information Technology and Management*, *18*(4), 305–330. [CrossRef]

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*(3), 421–458. [CrossRef]

Baumgartner, H., & Steenkamp, J.-B. E. M. (2001). Response styles in marketing research: A cross-national investigation. *Journal of Marketing Research*, *38*(2), 143–156. [CrossRef]

Becker, J.-M., Klein, K., & Wetzels, M. (2012). Hierarchical latent variable models in PLS-SEM: Guidelines for using reflective-formative type models. *Long Range Planning*, *45*(5–6), 359–394. [CrossRef]

Becker, J.-M., Ringle, C. M., & Sarstedt, M. (2018). Estimating moderating effects in PLS-SEM and PLSc-SEM: Interaction term generation*data treatment. *Journal of Applied Structural Equation Modeling*, *2*(2), 1–21. Available online: https://papers.ssrn.com/abstract=3223421 (accessed on 21 August 2026). [CrossRef] [PubMed]

Bell, E., Harley, B., & Bryman, A. (2022). *Business research methods* (6th ed.). Oxford University Press. Available online: https://global.oup.com/ukhe/product/business-research-methods-9780198869443 (accessed on 21 August 2026).

Berry, R., & Reisman, M. (2012). Policy challenges of cross-border cloud computing. *Journal of International Commerce and Economics*, *4*, 1–38. Available online: https://www.usitc.gov/journals/Policy_Challenges_of_Cross-border_Cloud_Computing_rev.pdf (accessed on 21 August 2026).

Boston Consulting Group. (2019). *Global wealth 2019: Reigniting radical growth* (p. 22). Boston Consulting Group. Available online: https://www.bcg.com/publications/2019/global-wealth-reigniting-radical-growth (accessed on 21 August 2026).

Brislin, R. W. (1970). Back-translation for cross-cultural research. *Journal of Cross-Cultural Psychology*, *1*(3), 185–216. [CrossRef]

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. [CrossRef]

Central Bank of Jordan. (2016). *Instructions of governance and management of information and related technology* (Circular No. 65/2016). Central Bank of Jordan.

Central Bank of Jordan. (2021). *Cybersecurity framework for Jordan financial sector* (pp. 1–143). Central Bank of Jordan. Available online: https://www.cbj.gov.jo/EBV4.0/Root_Storage/EN/CSF4JFSv1-0.pdf (accessed on 21 August 2026).

Cheng, M., Qu, Y., Jiang, C., & Zhao, C. (2022). Is cloud computing the digital solution to the future of banking? *Journal of Financial Stability*, *63*, 101073. [CrossRef]

Chin, W. W. (1998). The partial least squares approach to structural equation modeling. In G. A. Marcoulides (Ed.), *Modern methods for business research* (pp. 295–336). Lawrence Erlbaum Associates.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates.

Cram, W. A., Wang, T., & Yuan, J. (2023). Cybersecurity research in accounting information systems: A review and framework. *Journal of Emerging Technologies in Accounting*, *20*(1), 15–38. [CrossRef]

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.

Cybersecurity Ventures. (2020, November 13). *Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine*. Available online: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/ (accessed on 21 August 2026).

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, *20*(1), 79–98. [CrossRef]

De Haes, S., Van Grembergen, W., & Debreceny, R. S. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324. [CrossRef]

De Haes, S., Van Grembergen, W., Joshi, A., & Huygh, T. (2020). *Enterprise governance of information technology: Achieving alignment and value in digital organizations* (3rd ed.). Springer. [CrossRef]

Eldalabeeh, A. R., Al-Shbail, M. O., Almuiet, M. Z., Bany Baker, M., & E'leimat, D. (2021). Cloud-based accounting adoption in Jordanian financial sector. *The Journal of Asian Finance, Economics and Business*, *8*(2), 833–849. [CrossRef]

Endo, P. T., Rodrigues, M., Gonçalves, G. E., Kelner, J., Sadok, D. H., & Curescu, C. (2016). High availability in clouds: Systematic review and research challenges. *Journal of Cloud Computing*, *5*(1), 16. [CrossRef]

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50. [CrossRef]

Garsoux, M. (2013). *COBIT 5: ISACA's new framework for IT governance, risk, security and auditing* (pp. 1–39). ISACA Whitepapers. Available online: https://www.academia.edu/25367454/COBIT_5_ISACA_COBIT_5_ISACAs_new_framework_for_IT_Governance_Risk_Security_and_Auditing_An_overview (accessed on 21 August 2026).

Gartner. (2024). *Gartner forecasts global information security spending to grow 15% in 2025*. Gartner Press Release. Available online: https://www.gartner.com/en/newsroom/press-releases/2024-08-28-gartner-forecasts-global-information-security-spending-to-grow-15-percent-in-2025 (accessed on 21 August 2026).

Gawande, M. R., & Kapse, A. S. (2014). Analysis of data confidentiality techniques in cloud computing. *International Journal of Computer Science and Mobile Computing*, *3*(3), 169–175. Available online: https://ijcsmc.com/docs/papers/March2014/V3I3201433.pdf (accessed on 21 August 2026).

Gupta, V., Rashdi, P. T., Surahio, K. S., & Nadeem, R. (2024). Digital accounting and management: Transforming financial processes in the digital era. *The Critical Review of Social Sciences Studies*, *2*(2), 1671–1677. [CrossRef]

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2022). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications. Available online: https://books.google.jo/books?id=y8JyzgEACAAJ&redir_esc=y (accessed on 21 August 2026).

Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107–123. [CrossRef]

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2–24. [CrossRef]

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20. [CrossRef]

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135. [CrossRef]

Herath, T. C., Herath, H. S. B., & Cullum, D. (2023). An information security performance measurement tool for senior managers: Balanced scorecard integration for security governance and control frameworks. *Information Systems Frontiers*, *25*(2), 681–721. [CrossRef]

Héroux, S., & Fortin, A. (2025). How the three lines of defense can contribute to public firms' cybersecurity effectiveness. *International Journal of Disclosure and Governance*, *22*(2), 377–396. [CrossRef]

Hon, W. K., & Millard, C. (2018). Banking in the cloud: Part 1—Banks' use of cloud services. *Computer Law & Security Review*, *34*(1), 4–24. [CrossRef]

Idensohn, C. J., & Flowerday, S. (2025). Financial insider threats: A cybersecurity STRIDE analysis. *Issues in Information Systems*, *26*(1), 94–109. [CrossRef]

International Organization for Standardization & International Electrotechnical Commission [ISO/IEC]. (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems—Requirements*. International Organization for Standardization. Available online: https://www.iso.org/standard/27001 (accessed on 21 August 2026).

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. ISACA.

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA. Available online: https://www.isaca.org/store2/product/WCB19FGM (accessed on 21 August 2026).

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489–496. [CrossRef]

Kankanhalli, A., Teo, H.-H., Tan, B. C. Y., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154. [CrossRef]

Kenny, D. A. (2018). *Moderation*. Available online: http://davidakenny.net/cm/moderation.htm (accessed on 21 August 2026).

Kim, G. H., & Spafford, E. H. (1994). The design and implementation of Tripwire: A file system integrity checker. In *Proceedings of the 2nd ACM conference on computer and communications security* (pp. 18–29). Association for Computing Machinery. [CrossRef]

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), 1–10. [CrossRef]

Kock, N., & Lynn, G. S. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems*, *13*(7), 546–580. [CrossRef]

Koh, T. Y., & Prenio, J. (2023). *Managing cloud risk—Some considerations for the oversight of critical cloud service providers in the financial sector* (FSI Insights on Policy Implementation, No. 53). Bank for International Settlements, Financial Stability Institute. Available online: https://www.bis.org/fsi/publ/insights53.htm (accessed on 21 August 2026).

Kul, G., & Upadhyaya, S. (2015). Towards a cyber ontology for insider threats in the financial sector. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *6*(4), 64–85. [CrossRef]

Lee, I. (2021). Cybersecurity: Risk management framework and investment cost analysis. *Business Horizons*, *64*(5), 659–671. [CrossRef]

Liengaard, B. D., Sharma, P. N., Hult, G. T. M., Jensen, M. B., Sarstedt, M., Hair, J. F., & Ringle, C. M. (2021). Prediction: Coveted, yet forsaken? Introducing a cross-validated predictive ability test in partial least squares path modeling. *Decision Sciences*, *52*(2), 362–392. [CrossRef]

Liu, C., & Babar, M. A. (2026). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. *Australian Journal of Management*, *51*(1), 62–92. [CrossRef]

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research*, *35*(6), 382–385. [CrossRef]

Mather, T., Kumaraswamy, S., & Latif, S. (2009). *Cloud security and privacy: An enterprise perspective on risks and compliance*. O'Reilly Media. Available online: https://archive.org/details/cloudsecuritypri0000math (accessed on 21 August 2026).

Maurer, T., & Nelson, A. (2021). The global cyber threat to financial systems. *Finance & Development*, *58*(1), 24–27. Available online: https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf (accessed on 21 August 2026).

Morshed, A., & Khrais, L. T. (2025). Cybersecurity in digital accounting systems: Challenges and solutions in the Arab Gulf region. *Journal of Risk and Financial Management*, *18*(1), 41. [CrossRef]

National Cyber Security Center. (2024). *Annual cybersecurity report 2024*. National Cyber Security Center. Available online: https://www.ncsc.jo/Ar/NewsDetails/ncsc_Annual_Report_2024 (accessed on 21 August 2026).

National Institute of Standards and Technology [NIST]. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST Cybersecurity White Paper No. 29). National Institute of Standards and Technology. [CrossRef]

Novianti, I. D., & Dewayanto, T. (2025). The role of accounting technology in preventing cyberfraud: A systematic literature review. *Asia Pacific Fraud Journal*, *10*(2), 209–226. [CrossRef]

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Okour, S. (2019). The impact of the application of IT governance according to (COBIT 5) framework in reduce cloud computing risks. *Modern Applied Science*, *13*(7), 25–37. [CrossRef]

Oliver, D., & Lainhart, J. (2012). COBIT 5: Adding value through effective GEIT. *EDPACS*, *46*(3), 1–12. [CrossRef]

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2015). The design of phishing studies: Challenges for researchers. *Computers & Security*, *52*, 194–206. [CrossRef]

Petcu, D., & Crăciun, C. (2014). Towards a security SLA-based cloud monitoring service. In *Proceedings of the 4th international conference on cloud computing and services science (CLOSER 2014)* (pp. 598–603). SciTePress. [CrossRef]

Pinheiro, A., Canedo, E. D., de Sousa, R. T., Jr., & de Oliveira Albuquerque, R. (2020). Monitoring file integrity using blockchain and smart contracts. *IEEE Access*, *8*, 198548–198579. [CrossRef]

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903. [CrossRef] [PubMed]

Raftery, A. E. (1995). Bayesian model selection in social research. *Sociological Methodology*, *25*, 111–163. [CrossRef] [PubMed]

Rausand, M. (2011). *Risk assessment: Theory, methods, and applications*. John Wiley & Sons. [CrossRef]

Ringle, C. M., Wende, S., & Becker, J.-M. (2024). *SmartPLS 4 (Version 4)*. SmartPLS GmbH. Available online: https://www.smartpls.com (accessed on 21 August 2026).

Sarstedt, M., Hair, J. F., Cheah, J.-H., Becker, J.-M., & Ringle, C. M. (2019). How to specify, estimate, and validate higher-order constructs in PLS-SEM. *Australasian Marketing Journal*, *27*(3), 197–211. [CrossRef]

Shadish, W. R. (2002). Revisiting field experimentation: Field notes for the future. *Psychological Methods*, *7*(1), 3–18. [CrossRef] [PubMed]

Sharma, P. N., Liengaard, B. D., Hair, J. F., Sarstedt, M., & Ringle, C. M. (2023). Predictive model assessment and selection in composite-based modeling using PLS-SEM: Extensions and guidelines for using CVPAT. *European Journal of Marketing*, *57*(6), 1662–1677. [CrossRef]

Sharma, P. N., Sarstedt, M., Shmueli, G., Kim, K. H., & Thiele, K. O. (2019). PLS-based model selection: The role of alternative explanations in information systems research. *Journal of the Association for Information Systems*, *20*(4), 346–397. [CrossRef]

Sharma, S., Durand, R. M., & Gur-Arie, O. (1981). Identification and analysis of moderator variables. *Journal of Marketing Research*, *18*(3), 291–300. [CrossRef]

Shmueli, G., Sarstedt, M., Hair, J. F., Cheah, J.-H., Ting, H., Vaithilingam, S., & Ringle, C. M. (2019). Predictive model assessment in PLS-SEM: Guidelines for using PLSpredict. *European Journal of Marketing*, *53*(11), 2322–2347. [CrossRef]

Statista. (2026). *Cloud computing—Worldwide*. Available online: https://www.statista.com/outlook/tmo/cloud-computing/worldwide/ (accessed on 22 August 2026).

Tchernykh, A., Schwiegelshohn, U., Talbi, E.-G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581. [CrossRef]

Thales. (2025). *2025 Thales cloud security study: Global edition*. Thales Group. Available online: https://cpl.thalesgroup.com/about-us/newsroom/thales-2025-cloud-security-study-reveals-ai-tool-sprawl-security-gap (accessed on 21 August 2026).

Trevena, L., Zikmund-Fisher, B. J., Edwards, A., Gaissmaier, W., Galesic, M., Han, P. K., & Woloshin, S. (2013). Presenting quantitative information about decision outcomes: A risk communication primer for patient decision aid developers. *BMC Medical Informatics and Decision Making*, *13*(Suppl. S2), S7. [CrossRef] [PubMed]

van Wyk, J., & Rudman, R. (2019). COBIT 5 compliance: Best practices cognitive computing risk assessment and control checklist. *Meditari Accountancy Research*, *27*(5), 761–788. [CrossRef]

Weill, P., & Ross, J. W. (2004). *IT governance: How top performers manage IT decision rights for superior results*. Harvard Business School Press.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, *48*(3), 1846–1852. [CrossRef]

Yau-Yeung, D., Yigitbasioglu, O., & Green, P. (2020). Cloud accounting risks and mitigation strategies: Evidence from Australia. *Accounting Forum*, *44*(4), 421–446. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.