Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

BLOCKCHAIN USE, CYBER RISK, AND FIRM VALUE: THE MEDIATING ROLE OF INTERNAL CONTROL

Dr. Imran Abdul Aziz [1], Syed Muhammad Shoaib Wasim [2], Yusra Shehzadi [3]

DOI: https://doi.org/10.63544/jbii.v5i7.108

Affiliations:

[1] Visiting Faculty, KSBL/ IoBM, Head of Sales-Spectrum Securities Ltd.
Email: imran.shakir@hotmail.com

[2] Senior Assistant Professor, Business Studies Department, Bahria Business School, Karachi (BBSK)
Email: smshoaib.bukc@bahria.edu.pk

[3] Assistant Professor, Iqra University, Karachi
Email: yshehzadi44@gmail.com

Corresponding Author's Email:

[1] imran.shakir@hotmail.com

Article History:
Received: 24.06.2026
Accepted: 14.07.2026
Published: 24.07.2026

Abstract

This study examines the impact of blockchain use and cyber risk on firm value, with internal control serving as a mediating mechanism, among non-financial firms listed on the Pakistan Stock Exchange. Grounded in agency theory, the research employs a quantitative explanatory design, analysing survey responses from senior financial and assurance professionals alongside secondary financial data using partial least squares structural equation modelling (PLS-SEM). The findings reveal that blockchain use significantly and positively influences internal control effectiveness ($\beta = 0.555$, $p < 0.001$), while cyber risk exerts a significant negative effect on internal control ($\beta = -0.486$, $p < 0.001$). Internal control demonstrates a strong positive relationship with firm value ($\beta = 0.794$, $p < 0.001$) and serves as a significant mediator in both the blockchain use–firm value relationship ($\beta = 0.441$, $p < 0.001$) and the cyber risk–firm value relationship ($\beta = -0.386$, $p < 0.001$). The model exhibits substantial explanatory power, accounting for 66.1% of the variance in internal control and 63.1% of the variance in firm value. These results underscore that the value derived from blockchain technology and the mitigation of cyber risk are contingent upon robust internal control environments. For emerging market firms, effective governance, risk assessment, monitoring procedures, and control activities are essential to translate digital technology investments into tangible firm value. The study extends agency theory by demonstrating how technological conditions—both enabling and threatening—influence economic outcomes through organizational control mechanisms. Practical implications for boards, financial executives, risk managers, auditors, and regulators are discussed.

Keywords: Blockchain Use, Cyber Risk, Internal Control, Firm Value, Agency Theory

1. Introduction

The speed of digitalization of accounting and financial systems had enabled businesses to do things in a different manner that had significantly changed the ways they were recording transactions, securing information, monitoring business activities and reporting on financial performance. The blockchain was one of the many financial technologies that were gaining significant academic and professional interest because of its distributed, traceable, cryptographically secured, and immutable structure, which in contrast to traditional centralized accounting databases, has provided a new way to record transactions. The blockchain-based accounting solution had enabled the validation of transactions to be shared among authorized participants, which helped to minimize re-entry of data, delays in reconciliation, unauthorized changes to

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

transactions, and reliance on a single information custodian. As such, the use of blockchain technology had been linked with real-time accounting, automatic verification, visible audit trails, and enhanced information reliability. Empirical evidence suggested that the use of blockchain had enhanced accrual quality, earnings informativeness, stock liquidity, analyst forecast consensus, and cost of equity, due to the efficiency of blockchain accounting tasks (Liao et al., 2025). However, this increased blockchain use had also introduced challenges in integrating it into their systems, lack of technical expertise, regulatory uncertainty, compatibility with legacy systems, and a lack of understanding regarding the accounting gap blockchain technology could address (Akter et al., 2024).

Cyber risk included the risk of unauthorized access to the Company's information, malicious attacks, loss of information, vulnerabilities of third parties and employees and damage to the confidentiality, integrity, or availability of the Company's information. The repercussions went beyond just the costs of recovery as cyber incidents had impacted operations, undermined customer trust, contributed to litigation and regulatory costs, hurt reputation and caused uncertainty about future cash flows. Capital-market research had revealed that it had created negative investor responses and market value losses from its successful cyberattacks. The analysis of 776 cyber incidents resulted in the finding that the value of the firms involved was significantly reduced following their cyber incident, especially if the attack was severe, novel or widely reported when it was made public (Muktadir-Al-Mukit & Ali, 2025). Other studies had shown that managerial short-termism had raised the risk of data breaches, while the threat of cybersecurity had limited organizational investment decision making and innovation (Chen et al., 2024; Wang et al., 2024). Internal control was the policies, structures, monitoring procedures, authorization practices, risk assessment, communication architecture and corrective actions by which organizations have safeguarded assets, maintained reliable information reporting, ensured compliance and enhanced operational efficiency. Technology risk had not been reduced to zero with strong internal control, it had been translated into organized practices within the organization. In an environment where access rights, data inputs, smart-contract logic, governance duties, and exception-handling routines were not well controlled, blockchain records had not seemed to have added much value. Likewise, when organizations were not receiving effective monitoring, had no response plan, no segregation of duties, no employee accountability, and no continuous assurance, the recognition of cyber risk was also limited.

Previous research had shown that the quality of internal control was more than just a cost to the firm but had real economic implications. These controls helped investors value the corporate resources better, improved the financial reporting quality, made a better payout and investment decision, and helped reduce abnormal cash holding (Chen et al., 2020). Recent studies also indicated that the internal audit's value had increased the corporate value, as its addition had improved the accounting information quality and reduced the agency problem (Han et al., 2025). The literature in the cybersecurity context had been fragmented regarding the developments of internal control weaknesses and how it had affected the resilience of the organizations, and how the quality of controls and the maturity of organizations' information technology had assisted them to survive and recover from cyber incidents (Baatwah et al., 2026). The research on blockchain has focused primarily on adoption intentions, reporting quality, audit transformation or technological implementation. Research into breach disclosure, breach announcements, audit costs, investment reactions, and recovery costs had been focused on cybersecurity research. The research on internal control had been centred on the financial reporting weaknesses, earnings quality, risk management, and audit effectiveness.

To study the impact of the use of blockchain technology and cyber risk on the value of the company in Pakistan, the impact of blockchain use and cyber risk on the value of the company through the internal control mechanism in Pakistan had been examined. Pakistan provided a relevant setting as the listed companies started to digitize their financial operations in a context of developing technological frameworks, governance and cybersecurity frameworks. The study had truly advanced by bringing together accounting technology, cyber governance, internal control and corporate finance in one single study. It had also extended agency theory to explain how the use of blockchain had reduced information and monitoring issues, how the increased cyber risk had increased agency costs, and how the internal control had passed these on through to firm value. In practice the model had enabled boards, chief financial officers, internal auditors, risk managers,

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

regulators and investors to gain an understanding that the value of digital technologies had not only been dependent upon their adoption, but on the control environment they had passed through.

2. Theoretical Underpinning

The study had been grounded in the agency theory. The theory explains that a separation of ownership and control has led to conflicts between shareholders (as principals) and managers (as agents). Shareholders had been prejudiced by information asymmetry and uncertainty over the extent to which the managers' actions had increased the value of the company, having had more detailed information about the company's operations, technologies, risk exposures, and financial decisions. Managers might have hidden bad choices, fudged the books, not spent enough on cyber security, picked technology for their own benefit, or not reported weaknesses in the digital world. These behaviours had resulted in monitoring, bonding and remaining agency costs (Jensen & Meckling, 1976).

Theory had had a role in blockchain use, as it had changed the information and monitoring context of the agency relationship. Distributed validation, chronological transaction records, limited alteration and traceable audit trails had made managerial discretion over transaction histories more limited and allowed authorized third parties to check economic transactions. So, blockchain had already been a technological monitoring tool that was able to cut verification expenses, enhance timeliness and credibility of accounting information. However, empirical evidence revealed that blockchain-based invoicing led to improved reporting quality and favourable capital-market outcomes had been subject to agency problems, due to managers holding less or more information regarding vulnerabilities, previous incidents, internal security weaknesses, and the possible financial losses of blockchain-based invoicing (Akter et al., 2024; Liao et al., 2025).

If the potential gains of cybersecurity had seemed unclear or if the losses from this investment had been a direct hit to reported profits, managers may have delayed their investment in cybersecurity. If the returns on investing in cybersecurity had been unclear, or if the losses from such an investment had been immediate, it is possible that the managers would have deferred their investment in cybersecurity. They might also have deliberately minimized a cyber incident to avoid damage to their reputation, regulatory investigation, personal liability and/or executive replacement. This information asymmetry had made investors more uncertain about the investments, and the risk that was perceived with the future cash flows. The agency-theoretic argument that there was an absence of strong technological oversight and that it had created material losses for shareholders had been substantiated by evidence of the damage to the firm's reputation and market value caused by cyber incidents (Kamiya et al., 2021; Muktadir-Al-Mukit & Ali, 2025).

Actions taken, risk assessment, monitoring, exchange of information and accountability structures were limited in terms of unauthorized actions and had improved the reliability of managerial reporting. So, the technological conditions had become linked to economic effects in the process of internal control. Where distributed records, automated verification and real-time monitoring of the blockchain were integrated into authorization and assurance processes, this was seen as an improvement in internal control. Cyber risk, on the other hand, had caused the internal control to be weak, as system weaknesses, lack of access, inability to communicate, and inadequate risk measurement had undermined the control environment. Recent studies revealed that despite the adoption of quantitative methods, many organizations were actually managing cyber risk qualitatively, meaning that the cyber-control systems were not as mature as managers believed them to be (Slapničar et al., 2026) and thus, cyber-control systems were not really advanced enough to enable quantitative approaches.

Even when a distributed ledger system had been installed, the use of blockchain didn't necessarily create firm value, and cyber risk had not necessarily destroyed value when technological exposure had existed. Rather, the economic impacts had been based on the success of internal controls in converting technology and risk information into sound reporting, operational continuity, asset protection, managerial accountability and informed decision making. Agency costs had been minimized, resource allocation had been enhanced, expected cash flows were safeguarded, and investor confidence was reinforced. The positive impact of blockchain usage and the negative impact of cyber risk should thus be expected to be passed on via internal control to firm value.

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

3. Hypothesis Development

3.1 Blockchain Use and Internal Control

Blockchain was anticipated to bolster internal control as the technology had enhanced the organizational transactions' traceability, consistency, and verifiability. Historically, accounting solutions involved several parties to keep their own databases and reconcile differences on a periodic basis. Such arrangements have raised the likelihood of duplications, inaccuracies, late verifications, improper adjustments, and discrepancies between counterparties. These shortcomings were mitigated by blockchain systems, which have enabled transactions to be validated and captured in a shared and time-stamped ledger. With the proper authorization of information entered, it would be more difficult and apparent to other network participants to alter information.

The technology had also enabled the internal control via automated rules and continuous monitoring. Smart contracts had enabled preprogrammed controls to be placed within the transactions, so that payments, approvals, transfers or compliance activities had only taken place when certain conditions had been met. This arrangement had helped to do segregation of duties, transaction authorization, exception identification and maintenance of audit-trail. Liao et al. (2025) had discovered that blockchain-invoices increased accounting efficiency, accrual quality, earnings informativeness and decreased error-related restatements. The benefits of technology control, however, have relied on how well the technology was integrated, the technical skills that were required, governance arrangements and compatibility with existing accounting systems (Akter et al., 2024). So, if there were some meaningful applications of blockchain in accounting and financial processes, it was expected that it would improve the design and operation of internal controls.

3.2 Cyber Risk and Internal Control

The cyber risk was identified as expected to impact the internal control due to the direct impact of cyber risk on the reliability and continuity of organizational information systems. Internal controls had relied on reliable communication within the system, timely monitoring, controlled access to the system, reliable system authorizations, and accurate data. Cyberattacks had compromised the security of these foundations by doing things such as hacking into passwords, making changes to information, denying access to the network, encrypting records, exploiting third-party systems, or gaining access to financial applications. Increased cyber exposure had also made it harder to effectively keep the correct segregation of duties and to ensure that transactions were not from "bad guys. The increased cyber exposure had also made it more challenging to maintain proper segregation of duties and to confirm that transactions were from real customers.

Likewise, cyber risk had been indicative of governance weaknesses, employee knowledge, technological control, and risk assessment. Organizations had underinvested in preventive controls, detection systems and recovery plans, staff training, and independent assurance, as senior management underestimated cyber exposure. Slapničar et al. (2026) have already noted that, in some organizations, the decision-making process was based on qualitative judgments and only "appeared" to be based on quantitative cyber-risk management. There were cyber incidents that were linked to deficiencies in the internal control, delays in audits, reporting issues, and loss of corporate resilience (Baatwah et al., 2026). This would have had a negative effect on the effectiveness of the organization's control environment, risk assessment, control activities, communication and monitoring processes, and therefore, on internal control.

3.3 Internal Control and Firm Value

It was hoped that internal control would add value to the company by safeguarding resources, enhancing the reliability of reporting, minimizing agency costs, and aiding in efficient business decision making. The use of assets for unapproved purposes, managerial behaviour for opportunistic gain, accounting manipulation, operational waste and non-compliance had been held back by strong controls. They also had furnished boards and executives with timely information for investment, financing, working-capital and risk-management decisions. This enabled controlled firms to focus resources on value-creating activities and to steer clear of losses incurred from fraud, incorrect reporting, excess cash holdings, suboptimal investments and regulatory fines.

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

An investor's view of effective internal control was that it had eliminated uncertainty about the reliability of financial statements and sustainability of future cash flows. Less uncertainty would have increased investor confidence and thus decreased the required return on capital. In previous studies, higher internal-control quality was found to lower abnormal cash holdings and to boost the market value of corporate cash, as Chen et al. (2020) demonstrated. Liu et al., (2025) had found that the internal controls had the positive effect on audit quality and Han et al., (2025) had shown that internal auditing increased the value of the companies by improving the accounting information and reducing the agency costs. These results had suggested that value had been added via two channels: operational and informational.

3.4 Blockchain Use and Firm Value

The increased value of a firm was anticipated due to the reduction in transaction costs, improved reporting credibility, faster reconciliation and better interorganizational exchanges enabled by the blockchain. The distributed records had enabled organizations to verify transactions without having to continually depend on manual confirmation and intermediaries. This ability had decreased processing time, administrative expenses and disputes. The transparency and auditability of accounting information had also been enhanced through blockchain, enabling investors, auditors, creditors, suppliers, and regulators to assess the activities of a company more efficiently.

The valuation effect had also occurred due to lower information risk. If the financial information had been "timbler" and more credible, investors would have had less uncertainty and would have required a lower information-risk premium. In Liao et al. (2025), they had observed that blockchain usage led to higher stock liquidity, higher analyst consensus, and lower cost of equity. However, the costs of training, integrating, governing and infrastructure had been incurred by blockchain implementation, and economic benefits had not been established as a result of adoption. Ownership of a firm valued by the use of blockchain in material accounting and financial processes had been expected to positively affect firm value.

3.5 Cyber Risk and Firm Value

The cyber risks were assumed to detract from firm value due to operational disruption, direct losses, reputational damage, legal liability, and uncertainty of future performance. Companies that have been affected by a cyber event had faced investigation, recovery, replacement of systems, compensation to customers, insurance, regulatory, and litigation expenses. Cyberattacks were also reported to have impacted production, sales, procurement and payment systems, and reporting – all of which have led to a loss of revenue and a rise in operating costs. Customers were more vulnerable to customer data or IP being stolen, and customer relationships and competitive advantage had been further eroded.

These impacts had already been priced in by investors as cyber risk had changed their perception of risk and cyber exposure had impacted expected cashflows. Kamiya et al. (2021) have already determined successful cyberattacks adversely affect firm reputation and value to shareholders. We had previously linked disclosure of data breaches with risk of a stock price crash (Cao et al. 2024) and large negative market reactions to publicized data breaches (Muktadir-Al-Mukit and Ali 2025). Governance deficiencies were also found to be associated with higher levels of data-breach exposure, indicating that the negative impacts of cybers exposure had increased due to managerial myopia (Chen et al., 2024). Hence the expectation from investors was that companies with higher cyber risk would have been valued less as they were expected to have higher expenses, higher cash-flow uncertainty and lesser organizational resilience.

3.6 Mediating Role of Internal Control Between Blockchain Use and Firm Value

While blockchain had offered technology, internal control had delivered the benefits of reliable financial and operational outcomes. A blockchain-based system could have ensured that an inaccurate or fraudulently authorized information would have been recorded in an unalterable way, even if the input controls, access management, validation responsibility, and smart-contract governance have been lacking. Hence, the value of the blockchain had been reliant on the control framework around data input, access to permissions, exception management, system changes, and ongoing assurance.

Once the organization had enhanced its internal control through blockchain use, it had seen benefits of increased visibility of transactions, quicker detection of anomalies, increased audit evidence and fewer

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

reconciliation issues. These enhancements had reduced agency costs, safeguarded assets, enhanced the reporting credibility, and fostered investor confidence. So, the internal control was the organizational process through which the use of blockchain has affected the value of the firm. The foreseen mediation did not suggest that all blockchain effects had been occurring via internal control, but that a large part of the valuation impact had been occurring since blockchain had enhanced monitoring and accountability mechanisms.

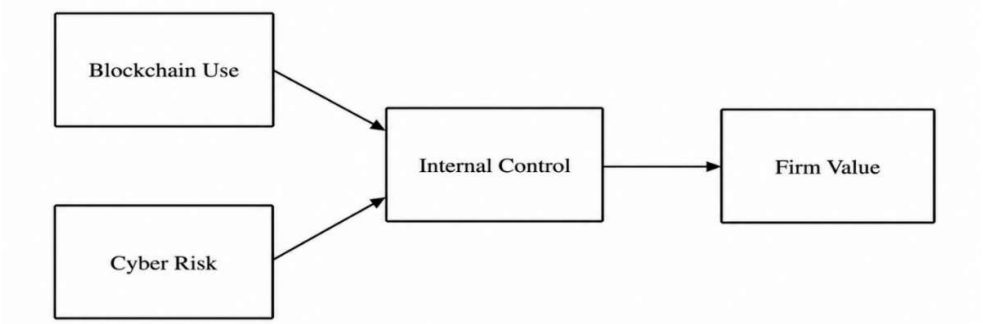
3.7 Mediating Role of Internal Control Between Cyber Risk and Firm Value

The value of the firm had already been directly threatened by cyber risk, but the consequences of cyber risk had also been predicted to be indirect, namely through the deterioration of internal control. The cyber exposure had caused issues with information processing, decreased data reliability, challenges in authorization processes and identified vulnerabilities in risk assessment and monitoring. These control deficiencies had raised the likelihood of financial misstatement, interruption of operations, loss of assets, regulatory non-compliance and ineffective management decisions. This meant that investors had had to deal with increased uncertainty over the company's future cash flows and governance.

The negative impacts of cyber risk had been mitigated, but not eliminated, through good internal controls. Firms had been able to spot threats earlier and recover better thanks to effective access controls, incident-response procedures, backup systems, employee accountability, constant monitoring and independent assurance. Baatwah et al. (2026) had documented that control weaknesses negatively impacted the survival rate of firms in cyberattack scenarios and IT maturity had bolstered the firms' strategic responses. The effect of cyber risk on the effectiveness of internal control was, therefore, expected to negatively mediate the relationship between cyber risk and firm value.

Figure 1

Conceptual Framework



4. Methodology

4.1 Research Design

The study was quantitative, deductive and explanatory in nature. A quantitative method was chosen because the study had tested the relationships (some theoretical) between blockchain use and cyber risk, between cyber risk and internal control, and between internal control and firm value. The research had taken a positive approach since the variables were operationalized using measurable indicators while the hypothesized relationships were tested statistically. A design of the firm level had been used, and each company listed was a unit of analysis.

A time-separated, dual-source design was preferred over a single-source, cross sectional design. Responses from knowledgeable financial and assurance professionals had been used to measure the use of blockchain and cyber risk and internal control. The market and accounting data of the firms had been acquired using the annual reports and the Pakistan Stock Exchange records which had been used to assess the firm value. This was because the dependent variable was not self-reported by the same individual who assessed the explanatory variables, thereby minimizing the common method bias. Firm size, leverage, profitability, firm age and industry were also controlled for in the study, as they may have affected the level of technology use and market valuation.

4.2 Population, Sample and Sampling Technique

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

The population had included non-financial companies listed on Pakistan Stock Exchange. The PSX had 535 listed companies at the end of 2025, spread over 37 sectors. Financial institutions had been omitted since the banks, insurance companies, investment companies and modarabas were subject to special capital, risk and reporting rules which had led to less comparability with other non-financial enterprises. Firms that had trading suspended, that did not submit annual reports, that did not have market data available or did not have a senior financial or assurance respondent identified had been removed from the sampling frame, which included chief financial officers, finance directors, financial controllers, heads of internal audit, risk managers, information-systems auditors, chief accountants, and senior accounting managers. Participants were expected to have at least three years of professional experience or have a sufficient understanding of the accounting processes, internal controls, protection against cyber threats, and financial processes of their firm. A single senior key informant had been chosen from each company to ensure the company level (unit of analysis) was not lost. If multiple responses had been received from the same firm, the most knowledgeable and senior had been used.

The sampling method used was Proportionate Stratified Random Sampling. Firstly, eligible companies were classified by the industrial sectors they belonged to, in accordance with PSX. That is, the number of firms per sector required had been identified based on the proportion of the eligible population in that sector. Firms were then randomly sampled in each stratum. This technique had led to the lesser chance of having large manufacturing sectors in the sample and the greater representation of technology, energy, pharmaceutical, textile, cement, automobile, food, chemical and service companies.

A priori statistical-power analysis was performed, and minimum sample size of 119 observations was determined to detect a medium effect size (0.15) at a 5% level of significance with a 95% level of statistical power and three predictors of the principal endogenous construct. A minimum target of 250 usable firm-level responses had been set anyway, however, for reasons of non-response, comparisons with other sectors, model complexity, missing information and estimation of mediation effects. The number of firms contacted to obtain the desired number of observations was, therefore, 400 firms that were eligible to be contacted. The actual questionnaires that were distributed, returned, excluded and retained were required to be reported as distributed, returned, excluded and retained when the questionnaires had been completed.

4.3 Measurement Instrument

A questionnaire was developed that was structured according to the literature on accounting-information-systems, cybersecurity, internal-control, and corporate-governance. Each perceptual item had been scored in the range 1-5 where 1 meant “strongly disagree” and 5 meant “strongly agree.” The questionnaire had included an introduction explaining the study, a screening section to determine the eligibility of the respondents, a demographic section, and a specific section for measuring the use of blockchain, cyber risk and internal control.

The six items adapted from Akter et al. (2024) and Liao et al. (2025) were used to measure the use of blockchain reflectively. The items had assessed how much the blockchain or distributed-ledger applications had been adopted to record transactions, to enter digital invoices, to reconcile accounts, to track assets, to handle inter-organizational information exchange, and to maintain verifiable audit trails. The higher the score, the more extensive and substantive the use of blockchain, and not just the intention to use blockchain from management.

Cyber risk was measured reflectively based on six items that were developed from recent research in cybersecurity (Chen et al., 2024; Kamiya et al., 2021; Slapničar et al., 2026). The indicators had been the following: perceived exposure to unauthorized use of their system, data breaches, service impact, third party vulnerabilities, financial impact, and reputational impact. Each threat had been scored on how material a threat it was to the firm. The higher values had signified that exposure to cyber risk is greater than the cyber security capability.

The internal control was being realized as a hierarchical structure consistent with the framework of the Committee of Sponsoring Organizations. The five dimensions of the control environment, risk assessment, control activities, information and communication, and monitoring had been represented. Three reflective

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

items were used in measuring each dimension, which resulted in 15 indicators of internal control. After the five dimensions were taken, they had been capable of confirming the second-order internal-control construct with the PLS procedure. The items had evaluated management accountability, risk identification procedures, authorization procedures, segregation of duties, information reliability, communication of control responsibilities, continuous monitoring, and the timely remediation of identified weaknesses.

Firm value had been determined from secondary data which was not from the questionnaire. A formative valuation construct had been developed comprised of Tobin's Q and market-to-book ratio. In previous times, Tobin's Q was defined as the ratio of the market value of equity and book value of liabilities to the book value of total assets. Previously, the ratio of the market value of equity to the book value of equity of the shareholders had been used. All of the market information was derived from PSX records, and the accounting values were taken from the audited annual reports. To minimize the effect of outliers, the first and ninety-ninth percentiles were minorized for extreme observations in the financial observations.

The questionnaire had undergone content and face validity by accounting professors, internal auditors, finance professionals, and information-systems experts. About 30 eligible professionals who were not involved in the principal survey had participated in a pilot test. Their input had been incorporated into changes to the wording, to eliminate ambiguities, to lessen the technical jargon, and to test the timing for completion. Full data collection had yet to begin, and preliminary reliability coefficients had to be greater than 0.70.

4.4 Data Collection

Data was collected using personally delivered and secure online questionnaires. Communication was made with the Company secretaries, Finance departments and internal-audit functions to find out eligible respondents. An information sheet was given to each participant that explained the academic purpose of the study, that the study participants were welcome to participate, that there would be no report to which the study participants could be identified, and that participants would be kept confidential. The respondents had been told that they would not be identified and that the results would only be given in aggregate.

To enhance response rates, reminders were sent after every two weeks. The financial data of firms was linked to the survey responses by means of confidential identification codes. To consider possible non-response bias, comparisons were made between early and late respondents on the key variables. To minimize evaluation apprehension and common-method variance, procedural remedies had been employed such as respondent anonymity, neutral wording, separation of predictor sections, and the use of objective firm-value data.

4.5 Data Analysis Techniques

Data were initially checked for missing values, response patterns, duplicate observations, respondents who were not engaged with the questions, and extreme outliers using SPSS. Descriptive statistics of the respondents, firms and industries and the study variables were computed. Data that were missing had been dealt with on the basis of the amount and nature of the missing data and firms for which certain information was not available had been eliminated. Multicollinearity has been preliminarily assessed by analysing correlation analysis and variance-inflation factors.

Partial least squares structural equation modelling has been carried out based on the presence of mediators, hierarchical measurement, reflective indicators, formative valuation measures and an emphasis on prediction in the framework. The two-stage strategy had been used to estimate the higher-order internal-control construct. The reflective measurement model was assessed using indicators loadings, Cronbach's alpha, composite reliability, rho_A, average variance extracted and the heterotrait-monotrait ratio. Indicator loadings needed to be greater than 0.708, reliabilities needed to be between 0.70 and 0.95, the AVE needed to be greater than 0.50 and the HTMT needed to be less than 0.85 or less than 0.90.

Indicators of collinearity, significance, and relevance of outer weights, and theoretical contribution of Tobin's Q and the market-to-book value had been evaluated as part of the formative construct assessment of the firm value. Previously, values of variance-inflation factors below 3 had been preferred and values below 5 had been considered acceptable. Prior to interpreting the relationships, structural-model collinearity had been assessed.

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

The hypothesized paths were tested for with 10,000 bootstrap resamples and bias-corrected confidence intervals. Path coefficients, t-statistics, p-values and confidence intervals had been reported. Coefficients of determination had been used to assess the explanatory power, and the effect size measured by f^2. The predictive relevance had been assessed by the Q^2 and out-of-sample predictive performance had been investigated by the PLSpredict.

The specific indirect effects of the use of blockchain and internal control on cyber risk and firm value had been evaluated using mediation. An indirect effect had been considered significant when its bootstrapped confidence interval had excluded zero. The direct effects had been included in the model so as to be able to detect complementary, competitive, indirect-only or partial mediation effects. As controls, firm size, leverage, profitability, age and industry had been incorporated. Robustness tests were run by estimating Tobin's Q and the market-to-book value individually and by comparing the two estimates between the high-technology and traditional sectors.

5. Finding and Analysis

5.1 Measurement Model

All items in the measurement model are highly reliable, convergent valid, and have acceptable collinearity between constructs. The loadings for Business Uncertainty (BU) had a range of 0.819 to 0.857 and for Corporate Risk (CR) were 0.795 to 0.846. These values were above the suggested cut-off of 0.70, thus indicating that the indicators were representative of their underlying constructs. The indicators of the Internal Control (IC) had loadings between 0.888 and 0.922, and Firm Value (FV) had loadings of 0.956 and 0.952, which were very strong indicator reliability. The internal consistency results were also good. Cronbach's alpha scores ranged from 0.902 to 0.948, and composite reliability scores ranged from 0.925 to 0.960. All values were above 0.70, which indicated excellent reliability of the constructs. For BU, CR, and FV, the composite reliability score was below the critical score of 0.95, indicating item similarity, but still good consistency; IC had a score of 0.960, with good consistency. Convergent validity was assessed by the average variance extracted values which ranged from 0.673 to 0.911, all of which met the minimum criterion of 0.50.

The VIF values ranged from 1.967 to 4.261. There were no problems with multicollinearity with all values less than the conservative range of 5.00. The larger VIF values for IC_CA and IC_RA indicated good inter item correlation without being problematic. The overall results of the measurement model fulfilled the reliability and validity criteria, as well as the collinearity criterion, and was appropriate for the subsequent assessment of the structural model. The results offer confidence that the constructs were measured consistently and that the estimated relationships are statistically credible overall, empirically.

Table 1

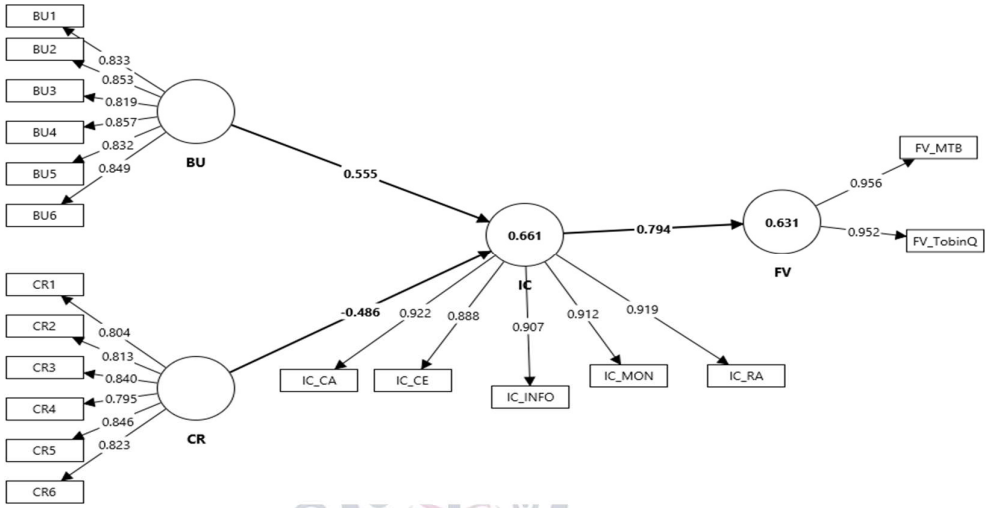
Reliability and Validity

Construct	Indicator	Outer Loading	Cronbach's Alpha	Composite Reliability	AVE	VIF
BU	BU1	0.833	0.917	0.935	0.707	2.355
	BU2	0.853				2.630
	BU3	0.819				2.240
	BU4	0.857				2.575
	BU5	0.832				2.370
	BU6	0.849				2.499
CR	CR1	0.804	0.903	0.925	0.673	2.116
	CR2	0.813				2.215
	CR3	0.840				2.354
	CR4	0.795				1.967
	CR5	0.846				2.519
	CR6	0.823				2.261
FV	FV_MTB	0.956	0.902	0.953	0.911	3.078
	FV_TobinQ	0.952				3.078

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

IC	IC_CA	0.922	0.948	0.960	0.827	4.261
	IC_CE	0.888				3.197
	IC_INFO	0.907				3.722
	IC_MON	0.912				3.840
	IC_RA	0.919				4.173

Figure 2
Measurement Model



5.1.1 Discriminant validity. The discriminant validity results suggest that all construct pairs are empirically different. The values of inter-construct ranges between 0.232 to 0.858, which is still below the widely accepted value of 0.90 for HTMT. The strongest association is found between BU and RR (0.683), while the weakest is seen between BU and CR (0.232), which indicates a high conceptual gap. There are moderate relationships between CR and FV (0.603) and between CR and IC (0.652) and between BU and IC (0.705). There is a strong BU–FV correlation (r = 0.753) and the strongest correlation is found between FV and IC (r = 0.858). Although this is more associated, it is still within the acceptable range. Hence, the measurement model overall is validated with regard to discriminant validity.

Table 2
HTMT Criteria

Construct	BU	CR	FV
BU	—	—	—
CR	0.232	—	—
FV	0.753	0.603	—
IC	0.705	0.652	0.858

5.2 Structural Model

All relationships were statistically significant with a p-value less than 0.001 and a t-value significantly greater than 1.96, which was the case in the structural model results. BU showed a significant positive effect on IC (β = 0.555, t = 14.175), with an increase in BU resulting in an increase in IC. On the other hand, the negative effect of CR on IC was statistically significant (β = −0.486, t = 12.563), indicating that higher CR levels decreased IC. The direct effect of IC was the highest, with β = 0.794 and t = 35.497 which indicated that IC has substantial role in improving firm value. The mediation outcomes proved to be important as well. The results showed that the relationship between BU and FV was positively mediated by IC (β = 0.441, t = 12.171), but the relationship between CR and FV was negatively mediated by IC (β = −0.386, t = 12.378). As

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

such, all direct and mediation hypotheses were confirmed. In general, IC was identified as an important pathway by which BU and CR impacted FV.

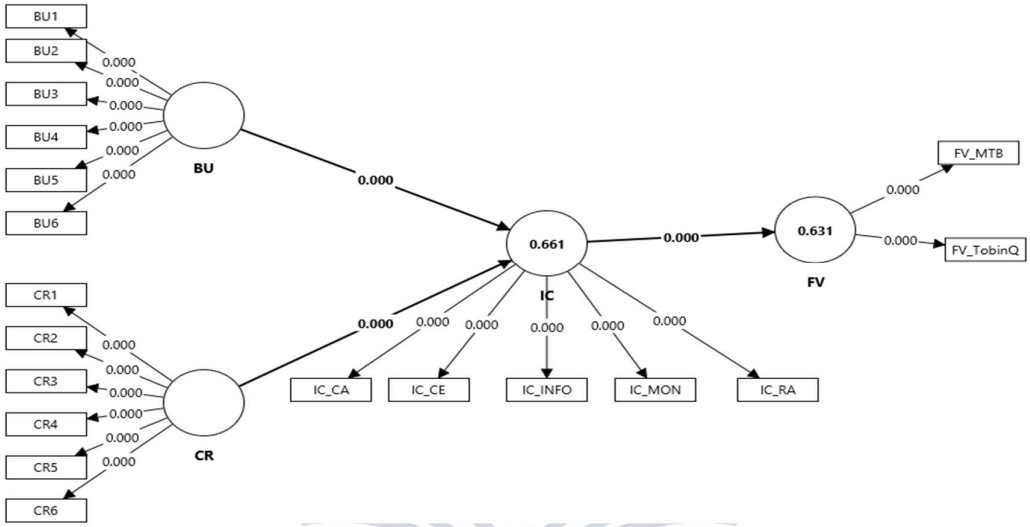
Table 3

Path Coefficient

Relationship	Original Sample (O)	STDEV	T Value	P Value
BU → IC	0.555	0.039	14.175	0.000
CR → IC	-0.486	0.039	12.563	0.000
IC → FV	0.794	0.022	35.497	0.000
BU → IC → FV	0.441	0.036	12.171	0.000
CR → IC → FV	-0.386	0.031	12.378	0.000

Figure 3

Structural Model



5.2.1 explanatory power, effect size, and Predictive relevance. The structural model had a high explanatory and predictive value. The value of R-square for firm value (FV) was 0.631, which means that internal control (IC) explains 63.1% of the variance in firm value (FV). Likewise, the BU and CR together accounted for 66.1% of the variation in IC and had an R-square value of 0.661. The adjusted R-square values of 0.629 and 0.658 were not far off from the respective R-square values, thus indicating the stability of the model. The results of the effect size analysis indicated that BU had a large effect size on IC ($f^2 = 0.867$) and CR had a large effect size on IC ($f^2 = 0.664$). IC had an extremely significant impact on FV ($f^2 = 1.707$) and was therefore a very important variable in explaining firm value. In addition, the out-of-sample predictive relevance was high with Q^2 values of 0.570 and 0.542 for the FV and IC, respectively. In general, the model was able to predict the accuracy of the explanation, the effect size and the predictive value of the model was very good.

Table 4

R- Square, f- Square, Q- Square

Assessment	Construct / Relationship	R-square	R-square Adjusted	f-square	SSO	SSE	Q^2
Explanatory Power	FV	0.631	0.629	—	500.000	214.819	0.570
Explanatory Power	IC	0.661	0.658	—	1250.000	572.795	0.542
Effect Size	BU → IC	—	—	0.867	—	—	—
Effect Size	CR → IC	—	—	0.664	—	—	—
Effect Size	IC → FV	—	—	1.707	—	—	—

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

6. Discussion

The conclusions validate asset-light hybrid sukuk as an institutional-market innovation and not just structuring option. Global Practices had the biggest influence on Market Development, suggesting that investor-protection mechanisms, disclosure requirements, asset-substitution arrangements and documentation that had been tested globally helped to lower uncertainty and speed up the domestic market acceptance. The result here transcends DoI, as it demonstrates that the influence of observability and perceived relative advantage does not take effect until foreign practices are modified in order to address local legal, Shariah, and market conditions. The outcome is also in line with numerous studies that indicate that sukuk markets offer diversification advantages but are vulnerable to institutional quality and out-of-country risks (Billah et al., 2024).

Regulatory Readiness also made a significant contribution to Market Development, reinforcing the fact that legal enforceability, tax neutrality, ownership clarity, Shariah consistency and credible distress-resolution arrangements are essential for market development. The discovery is significant as hybrid sukuk combine several contractual elements that may cause confusion for regulators, which can be worse than in conventional sukuk. It backs the argument of Zaheer and van Wijnbergen (2025) that ambiguous ownership and investor-recourse clauses make restructuring difficult and dampen investors' confidence.

Market Development significantly improved Riba Transformation and was a mediator of the effects of both Global Practices and Regulatory Readiness. Hence, international learning and regulatory reform were not a one-shot deal as they created transformation through deeper issuance, wider investor participation, better liquidity, more tenors and better access to Shariah-compliant instruments. This mechanism is expected to be consistent with previous studies that found a connection between the process of sukuk market development and economic growth, stability of Islamic banks, and Islamic financial deepening (Smaoui & Nechi, 2017; Ledhem, 2022; Baita et al., 2026).

Last but not least, Institutional Support enhanced the Market Development – Riba Transformation relationship. This moderation effect is applicable to illustrate that systemic substitution occurs in the market with the market expansion only when there is co-ordination of issuance, liquidity management, Shariah governance and investor confidence by public institutions. In general, the results indicate that to be able to transform the economy of Pakistan into riba-free, simultaneous innovation diffusion, its market deepening, and its institutional commitment are needed.

6.1 Theoretical Implications

This study extends the Diffusion of Innovation Theory by showing how international financial innovation can be transformative when it gets institutionalized in the domestic market. Global Practices had a direct and indirect impact on Riba Transformation, demonstrating that market-level translation of relative advantage and observability is needed. In addition, the study further develops Institutional Theory by differentiating Regulatory Readiness and Institutional Support. Regulatory Readiness provided legitimacy, enforceability and normative acceptance, while Institutional Support facilitated the systemic financial transformation of market development. Based on those findings, the conclusion is that the diffusion and institutional perspectives are brought together in a sequential manner to explain the path of asset-light hybrid sukuk from imported innovation to institutionalized riba free financial infrastructure.

6.2 Practical Implications

Pakistan needs to have a sequenced implementation approach for asset light hybrid sukuk. International templates must be tailored to the requirements of the property, taxation, insolvency and Shariah regimes as well as the requirements in terms of public debt of the domestic market. Documentation, beneficial ownership, asset substitution and disclosure requirements, investors' rights of recourse and approval protocols should then be harmonized. Beyond pilots, policy measures should include regular sovereign and corporate issuance calendars, diverse maturities, tradable liquidity instruments, and wider institutional-investor participation. A clear national asset register and a uniform hybrid-sukuk protocol will lower transaction costs and time to approval. These would advance liquidity, boost investor confidence, and enhance the ability of sukuk to supplant interest-based financial products and instruments.

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

6.3 Managerial Implications

Islamic banks, investment institutions, advisory firms and public-debt offices managers should view asset-light hybrid sukuk as one in a suite of approaches to building an Islamic banking ecosystem, not just a financing product. To overcome the complexity of contracts and to ensure alignment to Sharia, cross-functional teams of Shariah, legal, treasury, taxation, risk and capital-market experts should be set up. International mechanisms should be carefully selected but tailored to the institutional framework of Pakistan. There should be coordination by the managers with the regulators, exchanges, rating agencies, market makers and Shariah boards for consistency of issuance and for better secondary market liquidity. Building trust and retaining market participation should continue to be the focus of investor education, credible disclosure, transparent asset management, and strong governance.

6.4 Limitations and Suggestions for Future Work

The findings of the study could not be used to make causal and temporal inferences because of its cross-sectional study design, and the lack of statistical generalizability due to purposive sampling. Also, reliance on self-reported professional perceptions resulted in potential common-method and social-desirability biases. The analysis was limited to the experiences of Pakistan and thus may not be applicable to jurisdictions that have varying legal, tax and shariah-governance frameworks. Further studies are required using the longitudinal and multi-country designs to study the market development before and after the hybrid-sukuk reforms. Scholars should consider using objective measures such as volume of issuance, spreads, bid to cover ratios, liquidity, the composition of investors, and default experience, and test other moderators, such as trust in the market, digital issuance, and harmonization of Shariah.

7. Conclusion

The study finds that with the inclusion of financial innovation in regulatory, market, and institutional frameworks, asset-light hybrid sukuk can play a significant role in the economic transition of Pakistan towards a riba-free economy. Global Practices and Regulatory Readiness played a major role in enhancing Market Development, and also directly supported Riba Transformation. Both effects were conveyed by Market Development, and it shows that structural innovation can only have impact through the depth and liquidity of the offerings, investor interest and diversity of products. Institutional Support reinforced the importance of market development in bringing about systemic change. Therefore, the move towards transition in Pakistan should focus on standardized structures, enforceable ownership, coordinated governance, frequent issuance, maturities spread across various horizons and credible investor protection. For sustainable financial transformation, it is therefore crucial that there is trust and liquidity in the sukuk ecosystem.

Contribution of Authors

All the authors participated in the ideation, development, and final approval of the manuscript, making significant contributions to the work reported.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Data Availability

The datasets generated during and analysed during the current study are available from the corresponding author on reasonable request.

References

Akter, M., Kummer, T.-F., & Yigitbasioglu, O. (2024). Looking beyond the hype: The challenges of blockchain adoption in accounting. *International Journal of Accounting Information Systems, 53*, Article 100681. https://doi.org/10.1016/j.accinf.2024.100681

Baatwah, S. R., Asiri, M., Bajaher, M. S., Alyafai, A., & Baajajah, S. (2026). Thriving post-cyberattacks: The power of control, disclosure, and IT maturity. *Electronic Commerce Research, 26*, 1705–1743. https://doi.org/10.1007/s10660-025-09958-2

Baita, A. J., Umar, U. H., & Masyita, D. (2026). Sukuk, banking attributes and Islamic financial development. *International Journal of Social Economics, 53*(7), 1122–1135. https://doi.org/10.1108/IJSE-12-2024-0998

Billah, M., Hadhri, S., Balli, F., & Sahabuddin, M. (2024). Exploring the dynamic links and implications for hedging and investment strategies between sukuk and commodity-market volatility: Evidence from country-level

Journal of Business Insight and Innovation
Volume 5 Issue 7, 2026
ISSN-p: 3006-2284, ISSN-e: 3006-0982
https://insightfuljournals.com/

analysis. *International Review of Economics & Finance, 93*, 350–371. https://doi.org/10.1016/j.iref.2024.03.011

Cao, H., Phan, H. V., & Silveri, S. (2024). Data breach disclosures and stock price crash risk: Evidence from data breach notification laws. *International Review of Financial Analysis, 93*, Article 103164. https://doi.org/10.1016/j.irfa.2024.103164

Chen, H., Yang, D., Zhang, J. H., & Zhou, H. (2020). Internal controls, risk management, and cash holdings. *Journal of Corporate Finance, 64*, Article 101695. https://doi.org/10.1016/j.jcorpfin.2020.101695

Chen, W., Li, X., Wu, H., & Zhang, L. (2024). The impact of managerial myopia on cybersecurity: Evidence from data breaches. *Journal of Banking & Finance, 166*, Article 107254. https://doi.org/10.1016/j.jbankfin.2024.107254

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework*. COSO.

Demek, K. C., & Kaplan, S. E. (2023). Cybersecurity breaches and investors' interest in the firm as an investment. *International Journal of Accounting Information Systems, 49*, Article 100616. https://doi.org/10.1016/j.accinf.2023.100616

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.

Han, S., Mei, J., & Deng, J. (2025). Does internal compliance auditing increase corporate value? The influence of accounting information quality and agency problems. *Finance Research Letters, 86*, Article 108897. https://doi.org/10.1016/j.frl.2025.108897

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. https://doi.org/10.1007/s11747-014-0403-8

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behaviour, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 139*(3), 719–749. https://doi.org/10.1016/j.jfineco.2019.05.019

Le, A.-T., Huang, H. H., & Do, T. K. (2024). Navigating through cyberattacks: The role of tax aggressiveness. *Journal of Corporate Finance, 88*, Article 102649. https://doi.org/10.1016/j.jcorpfin.2024.102649

Ledhem, M. A. (2022). The financial stability of Islamic banks and sukuk market development: Is the effect complementary or competitive? *Borsa Istanbul Review, 22*(Suppl. 1), S79–S91. https://doi.org/10.1016/j.bir.2022.09.009

Liao, K., Lin, L., & Sun, Y. (2025). Blockchain adoption and corporate financial reporting quality. *Journal of Accounting and Public Policy, 49*, Article 107265. https://doi.org/10.1016/j.jaccpubpol.2024.107265

Liu, Y., Liu, Q., & Wei, Y. (2025). Digital finance, internal control, and audit quality. *Finance Research Letters, 76*, Article 107033. https://doi.org/10.1016/j.frl.2025.107033

Muktadir-Al-Mukit, D., & Ali, M. H. (2025). The dynamics of stock market responses following cyberattack news: Evidence from an event study. *Information Systems Frontiers*. Advance online publication. https://doi.org/10.1007/s10796-025-10639-6

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioural research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879

Rosati, P., Gogolin, F., & Lynn, T. (2022). Cyber-security incidents and audit quality. *European Accounting Review, 31*(3), 701–728. https://doi.org/10.1080/09638180.2021.1904575

Slapničar, S., Axelsen, M., & Eulerich, M. (2026). Cyber risk management: An illusion of a risk-based approach. *Journal of Management Control, 37*, 359–394. https://doi.org/10.1007/s00187-025-00401-z

Smaoui, H., & Nechi, S. (2017). Does sukuk market development spur economic growth? *Research in International Business and Finance, 41*, 136–147. https://doi.org/10.1016/j.ribaf.2017.04.018

Wang, J., Ho, C. Y., & Shan, Y. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis, 91*, Article 103028. https://doi.org/10.1016/j.irfa.2024.103028

Zaheer, S., & van Wijnbergen, S. (2025). Sukuk defaults: On distress resolution in Islamic finance. *Qualitative Research in Financial Markets, 17*(2), 292–311. https://doi.org/10.1108/QRFM-08-2023-0203