Business Ethics, Internal Control, and Cybersecurity in Foreign Exchange Transactions: Empirical Evidence from Indonesia

Misni Erwati[1*)], Ratih Kusumastuti[2], Rahayu[3], Lutfi[4], Derist Touriano[5], Afriantoni[6]

[1,2,3,4]*Department of Accounting, Universitas Jambi, Jambi, Indonesia*
[5]*Universitas Adiwangsa Jambi, Jambi, Indonesia*
[6]*Universitas Graha Karya Muara Bulian Jambi, Jambi, Indonesia*

ARTICLE INFO

Article history:
Received March 2, 2026
Revised April 16, 2026
Accepted April 28, 2026

JEL Classification:
G21, M14, M41, K22

Key words:
Financial Behavior, Cybersecurity Investment, Business Ethics, Internal Control, Foreign Exchange Transactions,

DOI:
10.14414/tiar.v16i1.5604

Check for updates

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

**) Corresponding author, email: misni_erwati@unja.ac.id*

ABSTRACT

This study examines the relationship between business ethics, internal controls, cybersecurity, and foreign exchange transactions in Indonesia. Cybersecurity is positioned as a mediating mechanism that links governance-related factors to the success of foreign exchange transactions in the banking sector. Using a quantitative survey approach, data were collected from directors and managers of foreign exchange companies affiliated with the Indonesian Foreign Exchange Dealers Association (APVA) that were accessible during the data collection period. A total of 176 questionnaires were distributed, and 121 usable responses were analyzed using path analysis in the SPSS. The results show that business ethics positively and significantly affect cybersecurity, indicating that ethical values, such as integrity, transparency, accountability, and compliance, support stronger cybersecurity practices. Internal control also has a positive and significant effect on cybersecurity, suggesting that control mechanisms contribute to the protection of digital financial transactions. Furthermore, cybersecurity has a positive and significant effect on foreign exchange transactions. However, business ethics and internal controls do not have significant direct effects on foreign exchange transactions, indicating that their contributions operate indirectly through the aspect of cybersecurity. These findings highlight cybersecurity as a strategic governance capability that connects ethical conduct and internal control with transaction reliability, data integrity, and stakeholder trust.

ABSTRAK

Penelitian ini menguji hubungan antara etika bisnis, pengendalian internal, keamanan siber, dan transaksi valuta asing di Indonesia. Keamanan siber diposisikan sebagai mekanisme mediasi yang menghubungkan faktor tata kelola organisasi dengan keberhasilan transaksi valuta asing. Penelitian ini menggunakan pendekatan kuantitatif melalui metode survei. Data diperoleh dari direktur dan manajer perusahaan pedagang valuta asing yang berafiliasi dengan Asosiasi Pedagang Valuta Asing Indonesia (APVA) dan dapat dijangkau selama periode pengumpulan data. Sebanyak 176 kuesioner disebarkan, dan 121 kuesioner yang layak dianalisis menggunakan analisis jalur dengan SPSS. Hasil penelitian menunjukkan bahwa etika bisnis berpengaruh positif dan signifikan terhadap keamanan siber, yang menunjukkan bahwa nilai integritas, transparansi, akuntabilitas, dan kepatuhan mendukung praktik keamanan siber yang lebih kuat. Pengendalian internal juga berpengaruh positif dan signifikan terhadap keamanan siber, yang menunjukkan bahwa mekanisme kontrol berperan dalam melindungi transaksi keuangan digital. Selain itu, keamanan siber berpengaruh positif dan signifikan terhadap transaksi valuta asing. Namun, etika bisnis dan pengendalian internal tidak berpengaruh langsung secara signifikan terhadap transaksi valuta asing, sehingga kontribusinya terjadi secara tidak langsung melalui keamanan siber. Temuan ini menegaskan bahwa keamanan siber merupakan kapabilitas tata kelola strategis yang menghubungkan perilaku etis dan pengendalian internal dengan keandalan transaksi, integritas data, dan kepercayaan pemangku kepentingan.

INTRODUCTION

In recent decades, advances in digital technology have significantly transformed global business activities, particularly through automation, real-time connectivity, and digitalization of financial services (Chyzhevska et al., 2021; Guo & Xu, 2021; Malik et al., 2022). In the financial sector, including foreign exchange transactions, these developments have accelerated transaction speeds, improved operational efficiency, and expanded access to digital financial services. However, the growing dependence on digital infrastructure has also created serious cybersecurity risks, including cyberattacks, data theft, online fraud, unauthorized access, and manipulation of transaction records (Aliyev & Shahverdiyeva, 2022; Luo, 2022; Reshetnikova et al., 2020). These risks are particularly critical in foreign exchange transactions because they involve sensitive financial data, high transaction volumes, regulatory compliance, and stakeholder trust. In Indonesia, the growth of digital financial transactions and the expansion of foreign exchange activities have intensified the need for stronger cybersecurity governance, while many companies still struggle to implement adequate protection against cyber threats (Dudhat & Agarwal, 2023; Mauladi et al., 2022; Munawaroh et al., 2023). Therefore, cybersecurity in foreign exchange transactions should not be viewed solely as a technical issue but also as a governance issue closely related to business ethics and internal control.

Previous studies have examined business ethics, internal controls, cybersecurity, and financial transactions from various perspectives. Studies on business ethics have generally focused on ethical behavior, organizational performance, stakeholder trust, and compliance, while studies on internal control have largely emphasized financial reporting reliability, fraud prevention, audit quality, and governance effectiveness (Aktürk, 2019; Eva & Lucie, 2019; J. Thomas, 2020; Bulau, 2021; Roza et al., 2021; Al-Hawamleh, 2024; Brás et al., 2024). Cybersecurity research has mainly discussed cyber resilience, information system protection, cybersecurity behavior, and organizational readiness in the face of cyber threats (Kumar et al., 2021; Ratmono & Frendy, 2022; Yazdanmehr et al., 2024). Although these studies provide important insights, they tend to examine each issue separately and have not sufficiently explained how business ethics and internal controls jointly contribute to cybersecurity and how cybersecurity influences the success of foreign exchange transactions. More specifically, empirical evidence on cybersecurity as a mediating variable in the relationship between business ethics, internal control, and foreign exchange transaction success remains limited, particularly in Indonesian foreign exchange firms.

The novelty of this study lies in its integrated conceptual and contextual approach. Conceptually, it does not treat business ethics, internal control, and cybersecurity as separate governance issues but instead positions cybersecurity as a mediating mechanism linking ethical and control-based organizational practices to the success of foreign exchange transactions. This approach extends prior studies that have examined ethical governance, internal control, and cybersecurity in separate domains by integrating them into a single empirical framework (Field, (Kumar et al., 2021; Ratmono & Frendy, 2022; Yazdanmehr et al., 2024)). This study focuses on foreign exchange companies in Indonesia, particularly members of the Indonesian Foreign Exchange Dealers Association (APVA), rather than the banking sector or general financial institutions. This context is important because foreign exchange companies operate in a highly sensitive financial environment that depends on transaction security, compliance, data integrity and public trust. Thus, this study offers specific empirical evidence on how non-technical governance factors, namely business ethics and internal control, may indirectly affect the success of foreign exchange transactions through cybersecurity capabilities.

Given the problem and research gap outlined above, this study aims to examine how business ethics and internal controls influence cybersecurity, and how cybersecurity affects the success of foreign exchange transactions in Indonesia. This study also investigates whether cybersecurity mediates the relationship between business ethics and foreign exchange transactions, and between internal control and foreign exchange transactions. This study contributes to the literature on business ethics, internal control, cybersecurity, and foreign exchange transactions by providing empirical evidence of the mediating role of cybersecurity in a digital financial environment. Practically, the findings are expected to help foreign exchange companies strengthen their cybersecurity investments, improve their internal control mechanisms, promote ethical business practices, and enhance stakeholder trust in digital foreign exchange transactions.

Theoretically, this study contributes to the literature by integrating business ethics, internal controls, cybersecurity, and foreign exchange transactions into a single, empirical model. This study extends prior research by treating cybersecurity as a mediator that explains how

governance-related factors influence transaction outcomes in a digital financial environment. In practice, this study offers foreign exchange companies guidance on strengthening cybersecurity as part of their governance and risk management strategies. The findings suggest that ethical values and internal control systems should be translated into concrete cybersecurity practices, including access control, transaction monitoring, incident response, data protection, and regular security evaluations.

THEORETICAL FRAMEWORK AND HYPOTHESES

The theoretical framework of this study explains the relationship between business ethics, internal controls, cybersecurity, and foreign exchange transactions. In digital financial activities, foreign exchange transactions are influenced not only by market factors but also by organizational governance, transaction integrity, data protection, and stakeholder trust. Therefore, business ethics and internal controls are organizational governance factors that may strengthen cybersecurity, and cybersecurity is a strategic mechanism that supports the success of foreign exchange transactions.

Business Ethics and Cybersecurity

Business ethics play an important role in shaping responsible organizational behavior, particularly in financial activities involving sensitive data, regulatory obligations and stakeholder trust. Ethical practices in corporate governance, human resource management, and marketing have been shown to improve organizational performance and decision-making quality. However, unethical practices (Aktürk, 2019; Eva & Lucie, 2019; J. Thomas, 2020).

In the context of financial transactions, ethical principles such as integrity, transparency, fairness, accountability, and legal compliance are essential because they reduce the risk of opportunistic behavior, data manipulation, and misconduct (Aslan et al., 2023; Batten et al., 2022; Corallo et al., 2021; Klimczak et al., 2022; Lee, 2021).

Ethical considerations are also relevant to cybersecurity because cyber risks are not only technical problems but also behavioral and governance issues that require ethical considerations. A strong ethical climate can encourage employees and managers to comply with security procedures, protect confidential data, report suspicious activities, and avoid practices that may expose the organization to cyber threats. Prior studies suggest that ethical frameworks, codes of conduct, and ethical leadership support responsible digital practices and strengthen organizational awareness of cybersecurity risks (Formosa et al., 2021; Saeed et al., 2023; Fleischman et al., 2023).

Additionally, ethical approaches to cybersecurity help organizations balance legal, economic, and organizational interests when addressing cyber-related dilemmas, such as surveillance, privacy, and data protection (Kusumastuti et al., 2016; Formosa et al., 2021; de Souza & de Souza, 2024; Lupton, 2024).

In foreign exchange transactions, business ethics are expected to support cyber security by fostering a culture of compliance, responsibility, and transparency. Companies with stronger ethical standards are more likely to view cybersecurity investments and data protection as part of their moral and organizational responsibilities rather than merely as technical requirements. Therefore, this study proposes the following hypothesis:

H1: Business ethics positively influences cybersecurity.

Internal Control and Cybersecurity

Internal control is a key governance mechanism that helps organizations ensure operational efficiency, reliable financial reporting, asset protection, and regulatory compliance. Previous studies have emphasized the importance of internal control in maintaining the integrity and reliability of financial reporting and in reducing fraud, errors, and weak governance risks (Bulau, 2021; Roza et al., 2021; Al-Hawamleh, 2024; Brás et al., 2024). In financial transactions, including foreign exchange transactions, internal controls support authorization, documentation, monitoring, duty segregation, and compliance with relevant procedures.

The relationship between internal control and cybersecurity is becoming increasingly important in digital financial environments. Strong internal controls can support cybersecurity by ensuring access control, transaction monitoring, audit trails, risk assessment, and timely detection of system vulnerabilities. Internal audits and technology-based monitoring systems can help detect fraud, identify irregular transactions, and reduce operational risks in financial activities (Alshebli, 2022; Feliciano and Quick, 2022; Napitupulu, 2023; Purwanti, 2023). Furthermore, studies on information systems and cybersecurity indicate that robust control mechanisms can strengthen data integrity, prevent unauthorized access, protect organizational assets, and increase accountability (Ashraf, 2022; Malaivongs et al., 2022; Sabillon, 2022; Saeed et al., 2023; Thomas et al., 2022; Villalón-Fonseca, 2022).

Internal control frameworks, including control

activities and risk-based monitoring, are relevant for strengthening cybersecurity readiness. Effective controls help organizations identify cyber risks, classify sensitive data, establish preventive procedures, and respond more effectively to security incidents (Al-Hawamleh, 2024; Blakely et al., 2022; Duggineni, 2023; Kafi & Akter, 2023; Pawar & Palivela, 2022; Rosati et al., 2022). In the foreign exchange sector, where transactions are vulnerable to fraud, money laundering, and data manipulation, internal controls can serve as an organizational foundation for implementing cyber security.

Based on this reasoning, this study proposes the following hypothesis:

H2: Internal control has a positive influence on cybersecurity.

Cybersecurity and Foreign Exchange Transactions

Foreign exchange transactions involve buying and selling currencies for liquidity, investment, or profit and are closely linked to international trade, financial stability, and investor behavior (Cespa et al., 2022; Liu & Lee, 2022; Lu et al., 2022; Suhendra et al., 2022). In Indonesia, foreign exchange activities are influenced by regulatory frameworks, monetary policies, exchange rate volatility, international trade, and risk management. Cybersecurity also strengthens stakeholder trust. When companies protect customer data, maintain transaction integrity, and respond effectively to cyber threats, they can increase the confidence of customers, regulators, and partners. Prior studies have shown that effective cybersecurity supports trust, resilience, and continuity in digital financial transactions (Basaran-Brooks, 2022; Krishna et al., 2023; Khalatur et al., 2022). Therefore, cybersecurity is expected to have a direct positive effect on the success of foreign exchange transactions.

Based on this argument, this study proposes the following hypothesis:

H3: Cybersecurity has a positive impact on foreign exchange transactions.

Cybersecurity as a Mediating Variable

Cybersecurity may also function as a mediating mechanism linking business ethics and internal controls to foreign exchange transactions. Business ethics can encourage organizations to prioritize transparency, responsibility, and compliance in digital financial activities, whereas internal controls can provide formal procedures, monitoring systems, and risk mitigation mechanisms. However, these governance factors may not automatically improve foreign exchange transaction success unless they are translated into effective cybersecurity practices.

From the perspective of mediation theory, cybersecurity can bridge organizational governance practices and transaction outcomes by transforming ethical values and control mechanisms into secure digital transaction processes. Previous studies have suggested that cybersecurity supports trust, transparency, and security in digital commerce and financial transactions (D'Hauwers et al., 2020; Farayola al., 2021; Farayola, 2024; Krishna et al., 2023). Cybersecurity also reflects ethical technological investment because organizations are responsible for protecting data, reducing cyber risks, and maintaining stakeholder confidence (Fleischman et al., 2023). In this sense, cybersecurity acts as an operational mechanism through which business ethics and internal controls affect the reliability of transactions.

The mediating role of cybersecurity is also relevant for companies operating in foreign exchange environments. Prior research on foreign exchange risk management indicates that organizational resources, capabilities, and strategic risk responses influence how firms manage foreign exchange exposure and transaction-related uncertainty (Dang & Lindsay, 2022; Pundziene et al., 2022; Martinez, 2023). In the context of this study, cybersecurity capability can be understood as a strategic organizational capability that converts ethical commitment and internal control into safer, more reliable, and trustworthy foreign exchange transactions.

Therefore, this study proposes the following hypothesis:

H4a: Cybersecurity mediates the relationship between business ethics and foreign exchange transactions.

H4b: Cybersecurity mediates the relationship between internal control and foreign exchange transactions.

Based on the reviewed literature, the relationships among business ethics, internal controls, cybersecurity, and foreign exchange transactions can be synthesized into four pathways. First, business ethics is expected to strengthen cybersecurity because ethical practices encourage integrity, transparency, accountability, compliance, and responsible protection of data. Previous studies have shown that ethical governance and leadership support responsible digital practices and cybersecurity awareness (Aktürk, 2019; Eva & Lucie, 2019; J.M. Thomas, 2020; Formosa et al., 2021; Saeed et al., 2023; Fleischman et al., 2023). However, previous research has mostly examined business ethics in relation to organizational performance, compliance, or ethical behavior, while its role in strengthening cybersecurity in foreign exchange

companies is unclear. Therefore, this pathway provides a basis for H1.

Second, internal control is expected to improve cybersecurity because effective control systems support access control, transaction monitoring, audit trails, risk assessment, fraud prevention, and data integrity. Prior studies indicate that internal control contributes to financial reporting reliability, asset protection, fraud prevention, and information system security (Bulau, 2021; Roza et al., 2021; Ashraf, 2022; Malaivongs et al., 2022; Al-Hawamleh, 2024; Brás et al., 2024). Nevertheless, much of the existing literature focuses on internal control in the context of financial reporting, auditing, or general governance, while its specific contribution to cybersecurity in foreign exchange transactions has not been explored. Thus, this pathway provides a basis for the use of H2.

Third, cybersecurity is expected to support the success of foreign exchange transactions by protecting transaction data, maintaining system integrity, preventing cyber fraud, reducing unauthorized access, and strengthening stakeholder trust. Previous studies have emphasized that cybersecurity is essential for the continuity of digital transactions, financial system stability, and trust in digital financial services (Farayola, 2024; Krishna et al., 2023; Perwej et al., 2021; Eling et al., 2023; Basaran-Brooks, 2022). However, empirical evidence on the role of cybersecurity in foreign exchange companies, particularly in Indonesia, is limited. Therefore, this pathway provides a basis for H3.

Fourth, cybersecurity mediates the relationship between governance factors and foreign exchange transaction success. Business ethics foster ethical commitment and responsible behavior, whereas internal controls establish formal monitoring and risk-mitigation procedures. Cybersecurity translates these governance practices into secure, reliable, and trusted transaction processes. Prior studies have indicated that cybersecurity supports trust, transparency, and security in digital commerce and financial transactions (D'Hauwers et al., 2020; Pasiouras et al., 2021; Krishna et al., 2023; Fleischman et al., 2023). However, cybersecurity has rarely been explicitly tested as a mediator between business ethics, internal controls, and foreign exchange transaction success. Accordingly, this pathway provides the basis for H4a and H4b.

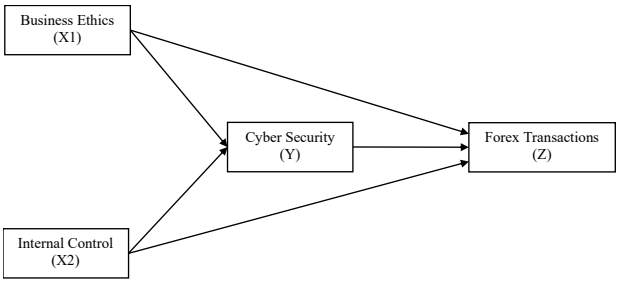


Figure 1. Theoretical Framework

RESEARCH METHOD

This study investigates the impact of cybersecurity on ethical standards and internal controls in foreign

Table 1. Definition of Research Variables and Dimension/

Variable	Dimensions	Operational Definitions
Cybersecurity (Y)	Confidentiality	Ensuring that only authorized parties can access critical information (Al-Hawamleh, 2024; Pawar & Palivela, 2022).
	Authentication	The verification process to ensures the user's identity before granting access (Bandari, 2023; Duggineni, 2023).
	Data Integrity	Ensuring that data is not changed or damaged by unauthorized parties (Pattnaik et al., 2023; Spanov & Alimzhanova, 2023).
	Availability	Ensuring that systems and information are always available to authorized users (Al-Hawamleh, 2024; Pawar & Palivela, 2022).
	Access Control	Settings that determine who can access certain systems or information (Zhou, 2023).
Business Ethics (X1)	Compliance with Law	Ensure business practices comply with applicable regulations and laws (Aslan et al., 2023; Corallo et al., 2021; Lee, 2021).
	Transparency	Providing clear and accurate information to all stakeholders (D'Hauwers et al., 2020).
	Social Responsibility	Taking into account social and environmental impacts in every business decision (Berrah et al., 2021; Kim et al., 2021; Scalzo et al., 2023).
	Integrity	Maintaining the principles of honesty and fairness in business transactions (Batten et al., 2022; Klimczak et al., 2022).
Internal Control (X2)	Financial Control	Ensuring all financial transactions are recorded and reported accurately (Al-Hawamleh, 2024; Al Balushi, 2021; Brás et al., 2024; Villiers, 2022).
	Operational Control	Monitor operational processes to ensure they run efficiently and effectively (Fleischman et al., 2023; Weiss, 2021).
	Compliance Control	Ensuring the organization complies with regulations and internal policies (Duggineni, 2023).
	Risk Management	Identifying and managing risks that affect the achievement of organizational goals (Rosati et al., 2022).
Forex Transactions (Z)	Liquidity	The ability to buy or sell foreign currencies quickly without affecting prices (Benigno et al., 2022).
	Volatility	The level of currency price fluctuations that affect transaction decisions (Liu & Lee, 2022; Suhendra et al., 2022).
	Regulation	Compliance with financial regulations regarding foreign currency transactions (Formosa et al., 2021).
	Exchange Risk	The risk arising from changes in exchange rates can affect transaction results (Della Corte et al., 2022).

exchange transactions in Indonesia. Primary data were collected using a 7-point Likert-scale questionnaire (Table 1) distributed to a simple random sample of Indonesian Foreign Exchange Traders Association (APVA) member companies. Online data collection, facilitated by email and WhatsApp, maximized reach. Data analysis was performed using SPSS version 26 to ensure accurate and comprehensive results.

DATA ANALYSIS AND DISCUSSION

This study used simple random sampling of APVA-affiliated foreign exchange companies accessible during the data collection period. A total of 176 questionnaires were distributed to directors and managers who were considered knowledgeable about business ethics, internal controls, cybersecurity, and foreign exchange transactions. Of these, 153 were returned, and 34 were excluded because of incomplete or inconsistent responses to the questionnaire. Thus, 121 questionnaires were usable for analysis, yielding a response rate of 86.93% and a usable response rate of 68.75% (Table).

Table 2. Questionnaire Distribution

Description	Q	%
Distributed questionnaires	176	100
Unreturned questionnaires	23	13.07
Returned questionnaire	153	86.93
Questionnaires that cannot be processed	34	22.22
Processable questionnaire	121	68.75

Source: Survey data processed by the authors.

Table 3 presents the respondents' profiles based on their position, company size, year of establishment, location, and technology adoption. The respondents were managers (55.37%) and directors (44.63%), indicating that the data were collected from individuals involved in managerial decision-making. The sample was relatively balanced between micro (49.59%) and small (50.41 %) companies and included young (35.54%), mature (35.54%), and legacy companies (28.93%). Respondents were distributed across Java and Bali (26.45%), Sumatra and Riau Islands (21.49%), Sulawesi (19.83%), Kalimantan (16.53%), and Papua (15.70%). Technology adoption varied across low (36.36%), medium (28.93%), and high levels (34.71 %). The chi-square results show that only company size significantly differed in Business Ethics (p = 0.044) and foreign exchange transactions (p = 0.042), while other respondent characteristics showed no significant differences across the main research variables.

Table 3. Respondent Profile

Respondent Characteristics			Cybersecurity (Y)		Chi-Square Test		Business Ethics (X1)		Chi-Square Test		Internal Control (X2)		Chi-Square Test		Forex Transactions (Z)		Chi-Square Test	
	f	%	Σ	x̄	χ²	P-Value	Σ	x̄	χ²	P-Value	Σ	x̄	χ²	P-Value	Σ	x̄	χ²	P-Value
Position																		
Manager	67	55.37	5919	88.34	26.394	0.497	4832	72.12	21.581	0.119	4458	66.54	30.726	0.531	4746	70.84	19.192	0.633
Director	54	44.63	4840	89.63			3924	72.67			3662	67.81			3857	71.43		
Company Size																		
Micro	60	49.59	5303	88.46	30.124	0.309	4324	72.02	25.460	0.044	3980	66.75	26.940	0.721	4258	71.03	34.639	0.042
Small	61	50.41	5456	89.44			4432	72.66			4140	67.87			4345	71.23		
Year Established																		
Young	43	35.54	3788	88.09			3096	72.00			2895	67.33			3023	70.30		
Mature	43	35.54	3836	89.21	68.413	0.090	3109	72.30	24.078	0.768	2847	66.21	68.36	0.332	3026	70.37	37.390	0.749
Legacy	35	28.93	3135	89.57			2551	72.89			2378	67.94			2554	72.97		
Location																		
Sulawesi	24	19.83	2116	88.17			1724	71.83			1590	66.25			1695	70.63		
Sumatra & Riau Islands	26	21.49	2326	89.46	102.656	0.627	1890	72.69	54.653	0.671	1767	67.96	107.20	0.909	1870	71.92	91.272	0.384
Papua	19	15.70	1697	89.32			1362	71.68			1272	66.95			1335	70.26		
Kalimantan	20	16.53	1789	89.45			1466	73.30			1354	67.7			1425	71.25		
Java & Bali	32	26.45	2831	88.47			2314	72.31			2137	66.78			2278	71.19		
Tech. Adoption																		
Low	44	36.36	3926	89.23			3184	72.36			2885	65.57			3159	71.80		
Small	35	28.93	3129	89.40	42.379	0.874	2547	72.77	24.897	0.730	2424	69.26	61.08	0.581	2490	71.14	56.502	0.098
High	42	34.71	3704	88.19			3025	72.02			2811	66.93			2954	70.33		

Source: Survey data, processed by authors.

Table 4 presents the overall descriptive statistics for the research variables. Cybersecurity had the highest mean score of 88.92, with a standard deviation of 6.49, indicating that respondents generally perceived cybersecurity practices as well-implemented and consistent across the companies. Business ethics had a mean score of 72.36 and a standard deviation of 3.43, suggesting relatively homogeneous perceptions of ethical practices among the respondents. Foreign exchange transactions had a mean score of 71.10 and a standard deviation of 4.72, indicating a moderate level of perceived effectiveness. In contrast, internal control had a mean score of 67.11 and the highest standard deviation of 7.99, suggesting that the implementation of internal control varied widely across companies. This variation is important

Table 4. Research Variable Descriptives

	N	Min.	Max.	Mean	Std. Deviation
Cybersecurity (Y)	121	71.00	101.00	88,9174	6.48535
Business Ethics (X1)	121	63.00	79.00	72,3636	3.43026
Internal Control (X2)	121	42.00	83.00	67,1074	7.99458
Forex Transactions (Z)	121	60.00	82.00	71,0992	4.71947
Valid N (listwise)	121				

Source: Survey data processed by the authors.

because it indicates that, although foreign exchange companies may share similar ethical perceptions, their formal control systems are not consistently implemented across companies.

Validity and Reliability Test

Validity was assessed using corrected item-total correlations and reliability was assessed using Cronbach's alpha. Items were considered valid when their corrected item-total correlation values exceeded the required threshold, and a construct was considered reliable when Cronbach's alpha was greater than 0.70 (Ghozali, 2018). As shown in Table 5, all corrected item-total correlation values ranged from 0.971 to 0.991, indicating that the items were both valid and reliable. The Cronbach's alpha value of 0.988 also indicates very high internal consistency. However, this value should be interpreted with caution, as an alpha value close to 1.00 may suggest redundancy. Therefore, although the instrument is reliable, future research should refine the questionnaire items to reduce conceptual overlap and minimize potential common method bias.

Table 1. Output Validity and Reliability Test

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted
Cybersecurity (Y)	227.1000	381,197	.975	.990
Business Ethics (X1)	245.8000	469,200	.985	.985
Internal Control (X2)	246.4000	438,041	.991	.979
Forex Transactions (Z)	246.4000	440,524	.971	.984
Cronbach's Alpha		**0.988**		

Source: Author's calculations based on a survey questionnaire using IBM SPSS

Classical Assumption Test

Classical assumption tests were conducted to assess the regression models' feasibility. The normality test using the Normal P-P Plot showed that the residuals were distributed around the diagonal line, indicating that the normality assumption was satisfied (Figure 2)

The multicollinearity test showed that all tolerance values were above 0.10 and all VIF values were below 5, with tolerance ranging from 0.598–0.816 and VIF ranging from 1.226–1.671. These results indicate that there was no serious multicollinearity among the independent variables. The heteroscedasticity test using a scatter plot showed a random distribution of residuals without a clear pattern, indicating that the residual variance was constant (Figure 2). In addition, the

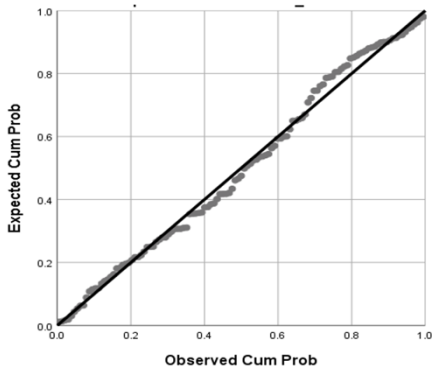


Figure 2. Normal PP Plot of Regression Standardized Residual

Durbin-Watson statistic of 2.071 was close to 2, suggesting that there was no autocorrelation. Overall, the results indicate that the regression models met the classical assumptions and were appropriate for path analysis (Ghozali, 2018).

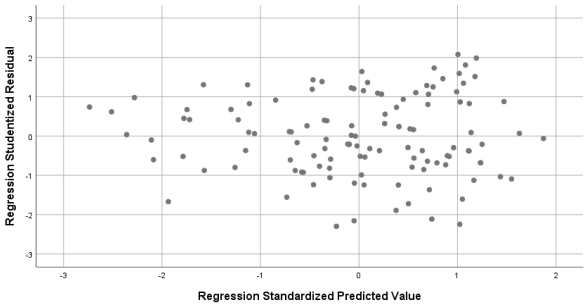


Figure 2. Scatter Plot (Dependent Forex Transactions)

Path Analysis

This study used path analysis to examine the relationships among Business Ethics, Internal Control, Cybersecurity, and Foreign Exchange Transactions. The first regression model assessed the effects of Business Ethics and Internal Control on Cybersecurity.

Table 6. Regression Results for Model 1

Coefficients [a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	11,313	10,374		1.09	0.278		
	Ethics	0.693	0.135	0.367	5,144	0	0.999	1,001
	Control	0.409	0.058	0.504	7,079	0	0.999	1,001

a. Dependent Variable: Cybersecurity

As shown in Table 6, Business Ethics had a positive and significant effect on cybersecurity, with a standardized coefficient of 0.367, a t-value of 5.144, and a significance value of 0.000. Internal Control also had a positive and significant effect on cybersecurity, with a standardized coefficient of 0.504, t-value of 7.079, and significance value of 0.000

(Ghozali, 2018). These findings indicate that both ethical practices and internal control systems contribute to strengthening the cybersecurity capabilities of foreign exchange firms.

The R-squared value of the first model was 0.402, indicating that Business Ethics and Internal Control jointly explained 40.2% of the variation in cybersecurity. The remaining 59.8% was explained by variables not included in the model. This suggests that although business ethics and internal control are important antecedents of cybersecurity, cybersecurity capabilities may also be influenced by other factors, such as IT infrastructure quality, cybersecurity investment, employee digital competence, regulatory pressure, and organizational risk culture (Table 2).

Table 2. Model Summary for Cybersecurity

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.634 [a]	0.402	0.392	5,05872	1,948

a. Predictors: (Constant), Ethics, Control
b. Dependent Variable: Forex

Based on the R-squared value, the residual coefficient for the first model was calculated as follows:

$e1 = \sqrt{(1 - 0.402)} = 0.7733$. Therefore, the first structural model shows that Business Ethics and Internal Control explain part of the variation in cybersecurity, with the remaining variation captured by e1 (Figure 3).

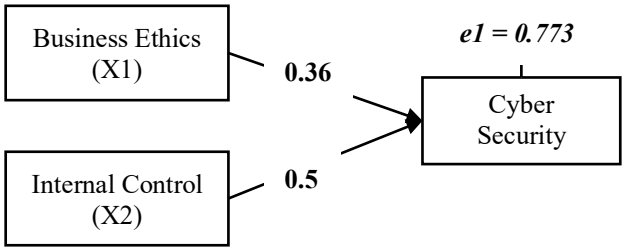


Figure 3. First Structural Path Model Diagram

The second regression model examined the effects of Business Ethics, Internal Control, and Cybersecurity on Foreign Exchange Transactions. As shown in Table 8 cybersecurity has a positive and significant effect on Foreign Exchange Transactions, with a standardized coefficient of 0.449, a t-value of 4.258, and a significance value of 0.000. This finding indicates that cybersecurity capabilities play an important role in supporting the reliability, security, and trustworthiness of foreign exchange transactions.

In contrast, Business Ethics and Internal Control did not have significant direct effects on Foreign Exchange Transactions. Business Ethics had a standardized coefficient of 0.137, a t-value of 1.515, and a significance value of 0.133, while Internal Control had a standardized coefficient of −0.135, a t-value of −1.384, and a significance value of 0.169. These results suggest that business ethics and internal controls do not directly determine foreign exchange transaction outcomes; however, their effects may operate indirectly through the influence of cybersecurity.

Table 3. Regression Results for Model 2

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
		B	Std. Error	Beta			Tolerance	VIF
1	(Constant)	33,771	8,691		3,886	0		
	Cyber	0.327	0.077	0.449	4,258	0	0.598	1,671
	Ethics	0.188	0.124	0.137	1,515	0.133	0.816	1,226
	Control	-0.08	0.058	-0.135	-1,384	0.169	0.701	1,426

Coefficients
a. Dependent Variable: Foreign Exchange Transactions

The R-square value of the second model was 0.222, indicating that Business Ethics, Internal Control, and Cybersecurity explained 22.2% of the variation in Foreign Exchange Transactions. The remaining 77.8% may be influenced by other factors outside the model, such as exchange rate volatility, market liquidity, regulatory compliance, technological infrastructure, service quality, customer trust, and managerial capability. Therefore, the findings should be interpreted as evidence of the importance of cybersecurity, but not as a complete explanation of the success of foreign exchange transactions.

Based on the R-squared value, the residual coefficient for the second model was calculated as follows:

$e1 = \sqrt{(1 - 0.222)} = 0.882.$

Therefore, the second structural model indicates that the unexplained variation in Foreign Exchange Transactions is represented by e2. Thus, the following structural path model diagram Figure 5 was obtained:

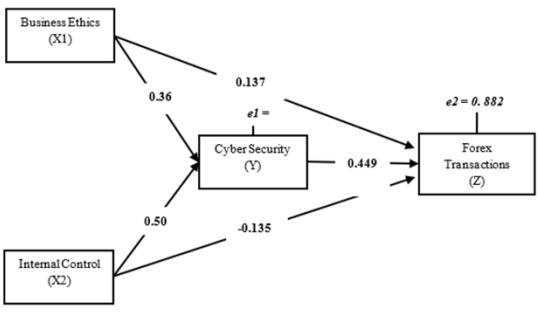


Figure 4. Second Structural Path Model Diagram

The path analysis also indicates indirect effects of Business Ethics and Internal Control on Foreign Exchange Transactions through Cybersecurity. The indirect effect of Business Ethics on Foreign Exchange Transactions through Cybersecurity was calculated by multiplying the coefficient of Business Ethics → Cybersecurity by the coefficient of Cybersecurity → Foreign Exchange Transactions: 0.367 × 0.449 = 0.165. Meanwhile, the indirect effect of Internal Control on Foreign Exchange Transactions through Cybersecurity was calculated as 0.504 × 0.449 = 0.226.

The path analysis also indicates indirect effects of Business Ethics and Internal Control on Foreign Exchange Transactions through Cybersecurity. The indirect effect of Business Ethics on Foreign Exchange Transactions through Cybersecurity was calculated by multiplying the coefficient of Business Ethics → Cybersecurity by the coefficient of Cybersecurity → Foreign Exchange Transactions: 0.367 × 0.449 = 0.165. Meanwhile, the indirect effect of Internal Control on Foreign Exchange Transactions through Cybersecurity was calculated as 0.504 × 0.449 = 0.226.

CONCLUSION, IMPLICATION, SUGGESTION, AND LIMITATIONS

This study examines the relationship between Business Ethics, Internal Control, Cybersecurity, and Foreign Exchange Transactions in Indonesia. The findings show that Business Ethics have a positive and significant effect on cybersecurity, indicating that ethical values such as integrity, transparency, accountability, and compliance support stronger cybersecurity practices. Internal Control also has a positive and significant effect on cybersecurity, suggesting that control mechanisms, such as access authorization, transaction monitoring, audit trails, and risk assessment, are important foundations for protecting digital financial transactions.

Table 9. Hypothesis Testing Summary

Hypothesis	Relationship	Coefficient	t-value	p-value	Result
H1	Business Ethics → Cybersecurity	0.367	5.144	0.000	Supported
H2	Internal Control → Cybersecurity	0.504	7.079	0.000	Supported
H3	Cybersecurity → Foreign Exchange Transactions	0.449	4.258	0.000	Supported
H4a	Business Ethics → Cybersecurity → Foreign Exchange Transactions	0.165	-	-	Indirect effect indicat
H4b	Internal Control → Cybersecurity → Foreign Exchange Transactions	0.226	-	-	Indirect effect indicat

Source: Survey data processed by the authors.

The results further show that cyber security has a positive and significant effect on foreign exchange transactions. This finding confirms that cybersecurity is not merely a technical function but a strategic capability that supports transaction reliability, data integrity, fraud prevention and stakeholder trust. However, business ethics and internal controls do not have significant direct effects on foreign exchange transactions. This indicates that ethical values and control systems may not directly improve transaction outcomes unless translated into effective cybersecurity practices. Therefore, cybersecurity serves as an important mechanism that links governance quality to the success of foreign exchange transactions.

The practical implication of this study is that foreign exchange companies should treat cybersecurity investment not as a separate technical expense but as part of corporate governance and risk management. Companies must strengthen cybersecurity policies, improve internal controls, enhance employee awareness of cyber risks, and build an ethical culture that supports responsible data protection. For managers, the findings imply that ethical conduct and internal control must be operationalized through concrete cybersecurity practices, including access controls, system monitoring, incident response procedures, and regular security evaluations.

Theoretically, this study contributes to the literature by integrating Business Ethics, Internal Control, and Cybersecurity into a single model of Foreign Exchange Transactions. These findings suggest that cybersecurity helps explain how governance-related factors influence transaction outcomes in a digital financial environment. This provides a more specific understanding of the role of cybersecurity as a bridge between organizational governance and transaction success, particularly in the context of foreign exchange companies in Indonesia.

This study had several limitations. First, the research used cross-sectional survey data; therefore, the findings cannot fully capture changes in cybersecurity practices and transaction performance

over time. Second, the study relied on self-reported questionnaire data, which may have been affected by respondent perceptions and common method bias. Third, the sample was limited to APVA-affiliated foreign exchange companies accessible during the data collection period; therefore, the findings should be interpreted within that context. Fourth, the mediation effect was identified through path coefficient analysis; however, future studies should use Sobel tests, bootstrapping, or structural equation modeling to provide stronger evidence of mediation.

Future research should include additional variables, such as IT infrastructure quality, cybersecurity investment, organizational risk culture, regulatory pressure, digital competence, and customer trust. Future studies may also use longitudinal or mixed-method approaches to better explain how ethical values and internal control systems are transformed into cybersecurity capabilities. In addition, expanding the sample to include other financial institutions or comparing foreign exchange companies across regions would provide broader evidence of cybersecurity governance in digital financial transactions.

ACKNOWLEDGMENT

We would like to express our deepest appreciation to the Research and Community Service Institution (LPPM) Universitas Jambi for the generous research funding provided under the 2024 Applied Research Grant Program

REFERENCES

Aktürk, E. B. (2019). Perception Regarding Ethical Rules Implemented in the context of corporate governance: A study in banking sector. *European Journal of Science and Technology*, *17*, 1347–1356.

Al-Hawamleh, A. (2024). Cyber resilience framework: Strengthening defenses and enhancing continuity in business security. *International Journal of Computing and Digital Systems*, *15*(1), 1315–1331.

Aliyev, A. G., & Shahverdiyeva, R. (2022). Scientific and methodological bases of complex assessment of threats and damage to information systems of the digital economy. *International Journal of Information Engineering and Electronic Business*, *2*, 23–38.

Alshebli, A. R. (2022). Internal Audit under Corporate Governance Regulations: A Comparison between Kuwait and New York Stock Exchanges. *Journal of the Gulf & Arabian Peninsula Studies*, *48*, 186.

Arauz, T., Chanfreut, P., & Maestre, J. M. (2022). Cybersecurity in networked and distributed model predictive control. *Annual Reviews in Control*, *53*, 338–355.

Arogundade, O. R. (2023). Network security concepts, dangers, and defense best practical. *Computer Engineering and Intelligent Systems*, *14*(2), 25–38.

Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, *97*(2), 1–24.

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks and solutions. *Electronics*, *12*(6), 1333.

Basaran-Brooks, B. (2022). Money laundering and financial stability: Does adverse publicity matter? *Journal of Financial Regulation and Compliance*, *30*(2), 196–214.

Batten, J. A., LonČarski, I., & Szilagyi, P. G. (2022). Financial Market Manipulation, Whistleblowing, and the Common Good: Evidence from the LIBOR Scandal. *Abacus*, *58*(1), 1–23.

Blakely, B., Kurtenbach, J., & Nowak, L. (2022). Exploring the information content of cyber breach reports and the relationship to internal controls. *International Journal of Accounting Information Systems*, *46*, 100568.

Bulau, V. (2021). Ways of maintaining the quality of financial audit in the context of validating financial statements. *Journal of Public Administration, Finance and Law*, *20*, 181–188.

Cespa, G., Gargano, A., Riddiough, S. J., & Sarno, L. (2022). Foreign exchange volume. *The Review of Financial Studies*, *35*(5), 2386–2427.

Chyzhevska, L., Voloschuk, L., Shatskova, L., & L., S. (2021). Digitalization as a vector of information system development and accounting system modernization. *Studia Universitatis Economic Series*, *31*(4), 18–39.

Corallo, A., Lazoi, M., Lezzi, M., & Pontrandolfo, P. (2021). Cybersecurity challenges for manufacturing systems 4.0: assessment of the business impact level. *IEEE Transactions on Engineering Management*, *70*(11), 3745–3765.

D'Hauwers, R., Van Der Bank, J., & Montakhabi, M. (2020). Trust, transparency and security in the sharing economy: What is the Government's role? *Technology Innovation Management Review*, *10*(5), 6–18.

Dang, V. H., & Lindsay, V. (2022). Determinants of hedging strategy in foreign exchange risk management by exporting small and medium-

sized enterprises: The mediating role of resources. *Journal of General Management*, *48*(1), 3–13.

Dudhat, A., & Agarwal, V. (2023). Indonesia's digital economy's development. *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, *4*(2), 109–118.

Duggineni, S. (2023). (2023). Impact of Controls on Data Integrity and Information Systems. *Science and Technology*, *13*(2), 29–35.

Eling, M., Elvedi, M., & Falco, G. (2023). The economic impact of extreme cyber risk scenarios. *North American Actuarial Journal*, *27*(3), 429–443.

Eva, T., & Lucie, K. (2019). Do environmental and ethical aspects of interfunctional coordination lead to smaller business performance. *Technological and Economic Development of Economy*, *25*(6), 1282–1292.

Farayola, O. A. (2024). Revolutionizing banking security: integrating artificial intelligence, blockchain, and business intelligence for enhanced cybersecurity. *Finance & Accounting Research Journal*, *6*(4), 501–514.

Feliciano, C., & Quick, R. (2022). Innovative information technology in auditing: auditors' perceptions of future importance and current auditor expertise. *Accounting in Europe*, *19*(2), 311–331. https://doi.org/10.1080/17449480.2022.2046283

Fleischman, G. M., Valentine, S. R., Curtis, M. B., & Mohapatra, P. S. (2023). The influence of ethical beliefs and attitudes, norms, and prior outcomes on cybersecurity investment decisions. *Business & Society*, *62*(3), 488–529.

Formosa, P., Wilson, M., & Richards, D. (2021). A principlist framework for cybersecurity ethics. *Computers & Security*, *109*, 102382.

Ghozali, I. (2018). *Aplikasi Analisis Multivariate Dengan Program IBM SPSS 25* (9th ed.). Universitas Diponegoro.

Guo, L., & Xu, L. (2021). The effectsof digital transformation on firm Performance: Evidence from China's manufacturing sector. *Sustainability*, *13*, 2–18.

Hudaya, A., & Firmansyah, F. (2023). Financial stability in the Indonesian monetary policy analysis. *Cogent Economics & Finance*, *11*(1), 2174637.

Kafi, M. A., & Akter, N. (2023). Securing financial information in the digital realm: case studies in cybersecurity for accounting data protection. *American Journal of Trade and Policy*, *10*(1), 15–26.

Klimczak, K. M., Sison, A. J. G., Prats, M., & Torres, M. B. (2022). How to deter financial misconduct if crime pays? *Journal of Business Ethics*, *179*(1), 205–222.

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective. *Information Systems Frontiers*, *25*(5), 1713–1741.

Kumar, S., Biswas, B., Bhatia, M. S., & Dora, M. (2021). Antecedents for enhanced level of cyber-security in organisations. *Journal of Enterprise Information Management*, *34*(6), 1597–1629. https://doi.org/10.1108/JEIM-06-2020-0240

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

Liu, T. Y., & Lee, C. C. (2022). Exchange rate fluctuations and interest rate policy. *International Journal of Finance & Economics*, *27*(3), 3531–3549.

Luo, Y. (2022). A general framework of digitization risks in international business. *Journal of International Business Studies*, *53*(2), 344–361.

Malaivongs, S., Kiattisin, S., & Chatjuthamard, P. (2022). Cyber trust index: A framework for rating and improving cybersecurity performance. *Applied Sciences*, *12*(21), 11174.

Malik, H., Chaudhary, G., & Srivastava, S. (2022). Digital transformation through advances in artificial intelligence and machine learning. *Journal of Intelligent & Fuzzy Systems*, *42*(2), 1–8.

Martinez, J. (2023). Financial Risk Management in International Markets. *Center for Management Science Research*, *1*(2), 1–11.

Mauladi, K. F., Laut Mertha Jaya, I. M., & Esquivias, M. A. (2023). Exploring the link between cashless society and cybercrime in Indonesia. *Journal of Telecommunications and the Digital Economy*, *10*(3), 58–76.

Mulyawan, C., & Latifah, E. (2019). Indonesian monetary regulation regarding Chinese electronic payment in Indonesia. *Jambe Law Journal*, *2*(1), 45–60.

Munawaroh, F., Widodo, P., & Azhari, Y. (2023). Efforts to strengthen cyber defense and cyber security of the Indonesian government in maintaining national security. *JETISH: Journal of Education Technology Information Social Sciences and Health*, *2*(1), 166–172.

Napitupulu, I. H. (2023). Internal control, manager's competency, management accounting information systems and good corporate governance: Evidence from rural banks in Indonesia. *Global Business Review*, *24*(3), 563–

585.

Pasiouras, F., Bouri, E., Roubaud, D., & Galariotis, E. (2021). Culture and multiple firm–bank relationships: a matter of secrecy and trust? *Journal of Business Ethics*, *174*, 221–249.

Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). *International Journal of Information Management Data Insights*, *2*(1), 100080.

Perwej, Y., Abbas, S. Q., Dixit, J. P., Akhtar, N., & Jaiswal, A. K. (2021). A systematic literature review on the cyber security. *International Journal of Scientific Research and Management*, *9*(12), 669–710.

Purwanti, D. (2023). The Strategic Imperative of Treasury and Financial Risk Management in a Volatile Economic Landscape. *Advances in Management & Financial Reporting*, *1*(3), 119–128.

Ratmono, D., & Frendy. (2022). Examining the fraud diamond theory through ethical culture variables: A study of regional development banks in Indonesia. *Cogent Business & Management*, *9*(1), 2117161.

Reshetnikova, N., Magomedov, M., & Buklanov, D. (2020). Digital finance technologies: Threats and challenges to the global and national financial security. *International Science and Technology Conference "Earth Science."* https://doi.org/10.1088/1755-1315/666/6/062139

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060.

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

Roza, M., Ramdhani, H. E. J., & Eny, S. (2021). The effect of corporate governance, audit quality, and auditor industry specialization on the integrity of financial statements. *Journal of Applied Business, Taxation and Economics Research*, *1*(2), 231–242.

Sabillon, R. (2022). The cybersecurity audit model (CSAM). In *Research Anthology on Business Aspects of Cybersecurity* (pp. 77–139). IGI global.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666.

Sihotang, J., Purba, M. L., Nopeline, N., & Ujung, M. S. (2023). Indonesia's Foreign currency reserves: An Analysis of the Influencing Factors. *Indonesian Journal of Business Analytics*, *3*(2), 183–196.

Thomas, J. (2020). Ethics in Organization and Management: The Application of Contemporary Theories of Ethical Decision-Making in Global Conditions. *International Journal of Business Strategy and Automation*, *1*(3), 67–74.

Thomas, L., Gondal, I., Oseni, T., & Firmin, S. S. (2022). A framework for data privacy and security accountability in data breach communications. *Computers & Security*, *116*, 102657.

Vargas, P., & Tien, I. (2023). Impacts of 5G on cyber-physical risks for interdependent connected smart critical infrastructure systems. *International Journal of Critical Infrastructure Protection*, *42*, 100617.

Villalón-Fonseca, R. (2022). The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity. *Computers & Security*, *120*, 102805.

Yazdanmehr, A., Jawad, M., Benbunan-Fich, R., & Wang, J. (2024). The role of ethical climates in employee information security policy violations. *Decision Support Systems*, *177*, 114086.