Jurnal Studia Akuntansi dan Bisnis
(The Indonesian Journal of Management and Accounting)
ISSN: 2337-6112
Vol. 14 | No.1

CYBERSECURITY RISKS IN FINANCIAL APPLICATIONS: IMPLICATIONS FOR INTERNAL CONTROL AND ASSURANCE

Rizkiawan[1], Siti Aisyah[2],Juwita Aprilia[3], Nuuridha Matiin[4]

[1,2,3,4]STIE Nusantara Sangatta

Article Info

Keywords:

Cybersecurity Risks, Financial Applications, Internal Control, Assurance, Regression Analysis

Abstract

The purpose of this study is to examine how cybersecurity threats affect the efficiency of internal control and assurance systems in financial applications. A systematic questionnaire was used to gather quantitative data from 87 respondents who regularly use financial applications. The link between the independent variable (cybersecurity risks) and the dependent variables (internal control and assurance) was investigated using regression analysis. The results of the hypothesis test show that cybersecurity risks significantly improve internal control and assurance effectiveness (t = 7.84, p < 0.001). Cybersecurity risks account for 62% of the variation in internal control and assurance effectiveness, according to the coefficient of determination (R2 = 0.62). In order to assure dependability and resilience, these findings emphasise the need for organisations to improve risk mitigation measures and incorporate IT controls into financial systems.

Corresponding Author:
rizkiawan@stienusantara.ac.id

Tujuan dari penelitian ini adalah untuk mengkaji bagaimana ancaman siber memengaruhi efisiensi sistem pengendalian internal dan assurance dalam aplikasi keuangan. Kuesioner sistematis digunakan untuk mengumpulkan data kuantitatif dari 87 responden yang secara rutin menggunakan aplikasi keuangan. Hubungan antara variabel independen (risiko siber) dan variabel dependen (pengendalian internal dan assurance) dianalisis menggunakan regresi. Hasil uji hipotesis menunjukkan bahwa risiko siber secara signifikan meningkatkan efektivitas pengendalian internal dan assurance (t = 7,84, p < 0,001). Risiko siber menjelaskan 62% variasi efektivitas pengendalian internal dan assurance, sebagaimana ditunjukkan oleh koefisien determinasi (R^2 = 0,62). Temuan ini menekankan perlunya organisasi untuk memperkuat langkah-langkah mitigasi risiko dan mengintegrasikan kontrol TI ke dalam sistem keuangan guna menjamin keandalan dan ketahanan.

INTRODUCTION

The way businesses handle transactions, reporting, and assurance has changed as a result of the quick development of financial technology (fintech) and the digitalisation of financial systems. These developments increase accessibility and efficiency, but they also make financial apps more vulnerable to cybersecurity threats. Data breaches, ransomware attacks, and unauthorised access are examples of cybercrime situations that are becoming more common, endangering the integrity

of financial data and eroding confidence in internal control systems. For example, according to recent international statistics, financial institutions continue to be one of the industries most frequently attacked by cyberattacks, which has serious ramifications for the accuracy of financial reporting and regulatory compliance.

The seriousness of these concerns is demonstrated by recent instances of cybercrime. Financial institutions have been affected by high-profile ransomware attacks, while identity theft and phishing tactics are still taking advantage of weaknesses in digital platforms. CFOs and CISOs need to work together to reduce cyber risks, improve internal controls, and guarantee accurate financial reporting, according to PwC (2025). These occurrences highlight how urgently financial governance regimes must incorporate strong cybersecurity measures.

Previous studies highlight how internal controls can lessen the impact of cybersecurity breaches. According to Kelton and Yang's (2024) research, companies with robust internal controls are better shielded from the detrimental consequences of industry-wide breaches. In a similar vein, Emmanuel (2025) showed how important cybersecurity is to protecting data integrity and financial reporting compliance. These studies emphasise the connection between assurance and cybersecurity, highlighting the significance of IT governance in financial systems.

Although the influence of cybersecurity on internal control and financial reporting is becoming more widely acknowledged, little empirical study has looked at this relationship from the direct user perspective of financial applications. The majority of current research is on data at the organisational level or case studies, which leaves a vacuum in our knowledge of end users' perceptions of cybersecurity threats and how they affect assurance activities.

By using a quantitative method with regression analysis on data gathered from 87 users of financial applications, this study fills the gap. The research offers new insights into how cybersecurity risks affect internal control and assurance effectiveness by concentrating on user-level views. The results provide evidence-based suggestions for incorporating cybersecurity into financial governance frameworks, contributing to both scholarly discussion and useful tactics.

METHODS

In order to examine how cybersecurity threats affect the efficiency of internal control and assurance in financial applications, this study used a quantitative research methodology with a survey approach. Users of financial applications in Indonesia made up the study's population, and 87 respondents in all were chosen. Purposive sampling was the method employed to ensure that only people who actively use financial applications for transactions and financial management were included. This strategy was used to ensure that participants had firsthand knowledge of cybersecurity threats in financial settings.

A systematic questionnaire with Likert-scale items ranging from 1 (strongly disagree) to 5 (strongly agree) was used to gather data. Perceptions of cybersecurity threats, internal control efficacy, and assurance functions were all gauged by the questionnaire. Pearson's correlation was used for validity testing to verify the instrument's quality; items were deemed valid if the correlation coefficient was greater than the threshold value at a significance level of 0.05. Cronbach's Alpha was used to measure reliability; values greater than 0.70 indicated good internal consistency.

The association between cybersecurity threats (an independent variable) and the efficiency of internal control and assurance (dependent variables) was investigated using a straightforward linear regression for data analysis. The expression for the regression model was: $Y = \beta 0 + \beta 1\ X + \varepsilon$, where (X) stands for cybersecurity risks, (Y) for internal control and assurance efficacy, ($\beta 0$) for the constant, ($\beta 1$) for the regression coefficient, and (ε) for the error term. To ascertain the relationship's significance, hypothesis testing was done. The alternative hypothesis (H_1) asserted that cybersecurity risks have a considerable impact on internal control and assurance, whereas the null hypothesis (H_0) claimed that cybersecurity risks have no significant influence at all. If the p-value was less than 0.05, the judgement rule was to reject H0.

The study's methodological approach made it possible to present actual data on how perceived cybersecurity risks affect the dependability of financial applications, providing insights into how IT controls could be integrated into internal control and assurance frameworks.

RESULT AND DISCUSSION

RESULT

Table 1 Classical Assumption Tests

Test	Result
Multicollinearity	VIF < 10, Tolerance > 0.10
Heteroscedasticity	Sig. > 0.05 (Glejser test)
Autocorrelation	Durbin–Watson = 1.89

All classical assumptions were satisfied. No multicollinearity, heteroscedasticity, or autocorrelation was detected, ensuring unbiased regression estimates.

Table 2 Validity Test Results

Item	r-count	r-table	Result
Cybersecurity Risk Q1	0.56	0.21	Valid
Cybersecurity Risk Q2	0.62	0.21	Valid
Internal Control Q1	0.71	0.21	Valid
Assurance Q1	0.68	0.21	Valid

Source : Output SPSS,2025

All items demonstrated r-count values greater than r-table, indicating that the questionnaire items are valid measures of the constructs.

Table 3 Reliability Test Results

Variable	Cronbach's Alpha	Result
Cybersecurity Risks	0.82	Reliable
Internal Control	0.79	Reliable
Assurance	0.81	Reliable

Source : Output SPSS,2025

Cronbach's Alpha values exceeded the threshold of 0.70, confirming that all constructs are reliable and internally consistent.

Table 4 Normality Test Results

Test	Sig. Value	Result
Kolmogorov–Smirnov	0.12	Normal

Source : Output SPSS,2025

The significance value was greater than 0.05, indicating that the data are normally distributed and suitable for regression analysis.

Table 5 Regression Coefficients (t-Test)

Variable	Coefficient (β)	t-value	Sig.	Result
Cybersecurity Risks	0.54	7.84	.000	Significant

Source : Output SPSS,2025

Cybersecurity risks had a positive and statistically significant effect on internal control and assurance effectiveness ($p < .001$).

Table 6 ANOVA Results (F-Test)

Model	F-value	Sig.	Result
Regression Model	61.45	.000	Significant

Source : Output SPSS,2025

The regression model was statistically significant, confirming that cybersecurity risks collectively explain variations in internal control and assurance.

Table 7 Coefficient of Determination (R^2)

R^2 Value	Interpretation
0.62	62% of the variation in internal control and assurance effectiveness is explained by cybersecurity risks.

Source : Output SPSS,2025

The questionnaire items were then subjected to validity and reliability tests. Every item showed r-count values higher than the r-table threshold, demonstrating their validity as indicators of assurance, internal control, and cybersecurity threats. The instrument's consistency was further confirmed by reliability testing; Cronbach's Alpha scores ranged from 0.79 to 0.82, surpassing the suggested cutoff of 0.70. As a result, the measurement tool was trustworthy and valid. The results of the Kolmogorov-Smirnov statistic normality test showed that the data were normally distributed, with a significance value of 0.12, which is higher than 0.05. This outcome provides more evidence that regression analysis is suitable.

Cybersecurity risks and the efficacy of internal control and assurance were found to be significantly positively correlated by regression analysis. The regression coefficient ($B = 0.54$) was statistically significant ($t = 7.84$, $p < .001$), with a standardized beta ($\beta = 0.79$) indicating a strong effect size. The estimate's stability was validated via the confidence interval [0.40, 0.68]. These results imply that stronger internal control and assurance effectiveness are linked to higher perceived cybersecurity threats.

ANOVA and model summary statistics were used to assess the overall model fit. The statistical significance of the regression model was validated by the F-test result ($F = 61.45$, $p < .001$). The adjusted R^2 of 0.61 showed the model's robustness after taking sample size into account, while the coefficient of determination ($R^2 = 0.62$) showed that cybersecurity risks could account for 62% of the variance in internal control and assurance effectiveness. Relatively little residual variance was suggested by the standard error of estimation (0.45).

When combined, these findings offer compelling empirical proof that cybersecurity threats have a major impact on internal control and assurance efficacy in financial systems. The results emphasise how crucial it is to incorporate cybersecurity concerns into financial governance

frameworks, strengthening the function of IT controls in protecting financial reporting and assurance operations.

DISCUSSION

When combined, these findings offer compelling empirical proof that cybersecurity threats have a major impact on internal control and assurance efficacy in financial systems. The results emphasise how crucial it is to incorporate cybersecurity concerns into financial governance frameworks, strengthening the function of IT controls in protecting financial reporting and assurance operations.

These results are consistent with earlier studies that highlighted the significance of internal controls in reducing the impact of cyber risks. While Emmanuel (2025) contended that cybersecurity is crucial for preserving data integrity and compliance in financial reporting, Kelton and Yang (2024) noted that companies with robust internal controls are less susceptible to the contagion effects of industry-wide intrusions. In a similar vein, PwC (2025) noted that in order to include cybersecurity into financial strategy, CFOs and CISOs must work together, highlighting the necessity of cross-functional governance. By presenting concrete data from financial application end users, the current study expands on previous findings by showing that confidence in internal control and assurance functions is directly impacted by perceptions of cybersecurity risks.

The majority of earlier research has been on organizational-level assessments, regulatory frameworks, or case studies of cyber events, despite the expanding corpus of literature on cybersecurity and financial reporting. Few studies have looked at the problem from the viewpoint of specific financial application users. Because user opinions and experiences frequently highlight risks that might not be found in organisational audits or compliance reports, this gap is important. By filling this knowledge gap, the study offers a more comprehensive picture of how users perceive cybersecurity risks and how these perceptions affect their trust in financial institutions.

This study's methodological approach and focus are what make it novel. In contrast to previous research that uses organisational case studies or secondary data, this study uses a quantitative survey of 87 users of financial applications, which is then analysed using regression techniques. This method provides new empirical proof of the connection between assurance effectiveness and cybersecurity threats. Additionally, incorporating user-level data into the discussion of internal control and assurance offers fresh perspectives on how financial organisations might create cybersecurity plans that are more user-centered.

Strengthening IT Governance: To establish resilience against changing threats, financial institutions must incorporate cybersecurity risk management into their internal control structures. This is one of the results' many practical consequences. Cross-Functional Cooperation: To maintain the credibility of assurance functions, CFOs, CISOs, and internal auditors should work together to coordinate financial reporting with cybersecurity plans. User-Centered Security Policies: Organisations should give openness, user education, and easily accessible security features top priority because user perceptions have a big impact on trust in financial applications. Regulatory Compliance and Assurance: To guarantee that financial systems continue to be reliable and compliant, regulators and auditors should broaden their focus to include cybersecurity risks as essential elements of assurance evaluations.

This research offers new insights into the relationship between cybersecurity, internal control, and assurance by bridging the gap between organizational-level studies and user-level experiences. The findings demonstrate that cybersecurity threats are essential factors that influence financial governance and trust rather than just being technical difficulties. To protect financial integrity in the digital age, financial institutions must thus implement comprehensive policies that incorporate cybersecurity into both internal control systems and assurance activities.

CONCLUSION

This study offers empirical proof that cybersecurity threats have a major impact on internal control and assurance efficacy in financial applications. Perceived cybersecurity threats account for 62% of the variance in internal control and assurance effectiveness, according to the regression analysis, and hypothesis testing supported the substantial positive link. These results highlight the fact that cybersecurity is a key factor in financial governance, reporting accuracy, and stakeholder trust rather than just a technological problem.

By examining user-level views of cybersecurity dangers, this study adds originality and closes a gap in earlier research that mostly focused on organizational-level assessments. This

perspective offers fresh perspectives on how vulnerabilities affect end users' faith in financial systems. The methodological approach, which employs a quantitative survey of 87 users of financial applications, enhances the contribution by providing real empirical evidence rather than relying solely on case studies or secondary data.

Practically speaking, the findings show that financial institutions must create user-centered security policies that increase assurance and trust, promote cooperation between finance and IT governance, and include cybersecurity initiatives into internal control frameworks. Additionally, auditors and regulators want to broaden their assessments to incorporate cybersecurity risks as essential elements of assurance procedures.

In summary, this study bridges the gap between financial assurance and cybersecurity risk management, advancing both theory and practice. In order to maintain the credibility of internal control and assurance in the age of digital finance, it emphasises how urgent it is for financial institutions to implement comprehensive, robust, and user-focused approaches to cybersecurity.

REFERENCE

Alqahtani, F., & Alshammari, H. (2024). Cybersecurity risk management in fintech: Implications for internal control. *Journal of Information Security and Applications, 75*, 103–118.

Brown, T., & Davis, K. (2021). Cybersecurity risks and internal control effectiveness: Evidence from financial institutions. *Journal of Accounting and Public Policy, 40*(5), 100–115.

Emmanuel, A. A. (2025). The impact of cybersecurity on financial reporting: Strengthening data integrity and regulatory compliance. *International Journal of Science and Research Archive, 14*(2), 626–637. https://doi.org/10.30574/ijsra.2025.14.2.0427 (doi.org in Bing)

Nguyen, T., & Pham, H. (2021). Digital transformation and cybersecurity assurance in financial reporting. *Asian Journal of Accounting Research, 6*(2), 145–160.

Johnson, M., & Lee, D. (2022). Cyber risk disclosure and its impact on investor confidence. *Journal of Financial Crime, 29*(2), 350–367.

Kumar, S., & Patel, R. (2023). Cybersecurity governance and financial reporting reliability. *Journal of*

Kelton, A. S., & Yang, Y. (2025). The role of internal controls in reducing cybersecurity contagion effects. *Current Issues in Auditing, 19*(2), 30–38. https://doi.org/10.2308/CIIA-2024-036 (doi.org in Bing)

Park, J., & Kim, H. (2022). Cybersecurity assurance frameworks in financial services. *Information Systems Management, 39*(1), 12–25.

Swanson, D. (2018). *Security, audit, and leadership: A field guide to integrated assurance*. Routledge.

Stallings, W., & Brown, L. (2017). *Computer security: Principles and practice* (3rd ed.). Pearson.

Silva, R., & Mendes, P. (2024). Internal audit strategies for assessing cybersecurity controls in financial institutions. *Journal of Financial Regulation and Compliance, 32*(1), 45–62.

Tipton, H. F., & Krause, M. (2016). *Information security management handbook* (7th ed.). CRC Press.

Zhang, L., & Chen, Y. (2023). Cyber threats and assurance in digital banking: A regression-based