INTERNATIONAL JOURNAL OF SOCIAL SCIENCE, EDUCATIONAL, ECONOMICS, AGRICULTURE RESEARCH AND TECHNOLOGY (IJSET) | ISSN (E): 2827-766X
Website: https://ijset.org/ | Volumes 5 No. 8 (2026)

ESG, CYBER GOVERNANCE, OPERATIONAL RISK IN BANK RESILIENCE: EVIDENCE FROM INDONESIAN BANKS

Trisna Aminwara[1]*, Sudarso Kaderi Wiryono[2], Raden Aswin Rahadi[3]
Institut Teknologi Bandung, Jakarta
E-mail: trisna.aminwara@gmail.com

Received: 02/06/2026 | **Revised** : 11/06/2026 | **Accepted:** 23/06/2026 | **Published** :06/07/2026

Abstract

This study examines how ESG and cyber governance relate to operational risk and bank resilience in Indonesia, with bank stability used as its measurable aspect. Using balanced panel data from 17 KBMI 3 and KBMI 4 banks during 2019–2024, the study applies Fixed Effects regression with robust standard errors and year dummy variables. ESG and cyber governance are measured using disclosure-based indexes from annual and sustainability reports. Bank stability is measured using the natural logarithm of the Z-score, while operational risk is measured by operational risk-weighted assets divided by total risk-weighted assets. The findings show that ESG has no significant direct relationship with bank stability or operational risk. Operational risk is positively related to bank stability, reflecting risk-weighted exposure and capital absorption rather than suggesting that operational failures improve stability. The main finding is that cyber governance negatively moderates the ESG–operational risk relationship, indicating that stronger cyber governance reduces the marginal operational risk association of ESG. Based on these findings, a KRI-Based ESG–Cyber Governance–Operational Risk Monitoring Framework is proposed.

Keywords: bank resilience, bank stability; cyber governance; ESG; operational risk

INTRODUCTION

Banks play important roles in financial intermediation, public confidence, and provision of financial services. In this research, bank stability is considered a measurable indicator of bank resilience since stable banks are usually better able to handle risks and absorb shocks. On the other hand, bank resilience is broader as it encompasses the continuity of operations, responsiveness, and recovery in case of disruptions (BCBS, 2021). Digitalization and sustainability implementation are the key aspects of the current banking environment. Digital banking increases operational efficiency but also adds dependency on IT systems, customer information, third-party IT providers, and service availability. Sustainable finance implementation implies environmental and social screening, portfolio classification, quality data, control of reporting process, and interfunctional cooperation. In Indonesia, according to POJK No. 51/POJK.03/2017, financial organizations must implement sustainable finance and publish sustainability report (OJK, 2017). Such changes create new operational challenges that are not always captured by traditional measures such as capital adequacy, liquidity, and asset quality.

Mixed results on the impact of ESG in banking imply that ESG activities may increase stakeholders' confidence, governance, and risk awareness, but at the same time may impose operational challenges and adjustments when internal capability is lacking (Azmi, Hassan, Houston, & Karim, 2021; Do, Ho, Mai, Nguyen, & Nguyen, 2024; Biswas, Das, Tiwari, & Patro, 2025). The evidence from Indonesia also suggests that ESG risks may have a different impact on bank stability depending on bank-specific features and ownership (Defung, Yudaruddin, Ambarita, Che-Yahya, & Bahrudin, 2024). The notion of operational risk is useful for investigation as ESG practices depend on employees, processes, IT systems, data quality, and third parties. According to the findings of Galletta, Goodell, Mazzù, and Paltrinieri (2023), banks with higher ESG scores exhibit lower operational risk. At the same time, the quality of public ESG practices does not reflect the internal implementation quality. ESG disclosure demonstrates the commitment and legitimacy, while internal controls, risk integration, and support systems are difficult to estimate (Yoo & Managi, 2022). The concept of cyber governance may be relevant in terms of influencing the ESG–operational risk relationship since the ESG processes become more dependent on the use of data and technologies. It includes board oversight, cyber risk integration, incident response, business continuity, and recovery

OPEN ACCESS

capabilities (NIST, 2024; BCBS, 2021). Recent studies investigate the relationship between cybersecurity policy and ESG, operational risk, and bank performance, but mainly focus on cybersecurity as a policy variable and performance determinant (Benthabet, 2025; Bruno, Pistolesi, & Teti, 2025). There is little research devoted to the role of the broad cyber governance in the ESG–operational risk relationship, especially in Indonesian banking sector.

This study seeks to address the gap by investigating ESG, cyber governance, operational risk, and bank stability among 17 KBMI 3 and KBMI 4 banks over the period of 2019–2024. ESG-related banking practices and cyber governance will be assessed using disclosure-based indexes, while operational risk will be estimated using operational risk-weighted assets against total risk-weighted assets. By considering bank stability as a measurable aspect of resilience, the paper will connect all the mentioned variables in one framework and convert its findings into the KRI-Based ESG–Cyber Governance–Operational Risk Monitoring Framework.

LITERATURE REVIEW

ESG, Operational Risk, and Bank Stability

The nature of the relationship between ESG and banking outcomes remains ambiguous. ESG practices may positively affect stakeholders' confidence, governance, risk awareness, and stability but simultaneously impose challenges and operational pressures when internal capabilities are weak (Azmi et al., 2021; Do et al., 2024; Biswas et al., 2025). Stakeholder Theory suggests that banks need to take into account the interests of customers, employees, investors, regulators, and society along with the interests of shareholders (Freeman, 1984). Hence, ESG practices may help to implement responsible finance, protect customers, provide transparency, and manage risks properly which, in turn, is expected to increase performance and stability (Donaldson & Preston, 1995).

In empirical literature, there is no agreement on the matter as well. Azmi et al. (2021) find a positive correlation between ESG activities and selected dimensions of banking performance in emerging economies, while Biswas et al. (2025) indicate that ESG practices help to reduce default risk on a longer horizon. In contrast, Do et al. (2024) observe a negative correlation between ESG and bank stability in ASEAN countries. The findings of Defung et al. (2024) also reveal that sovereign ESG risk has a negative impact on bank stability in Indonesia, although their measure is based on sovereign level rather than banks' ESG practices.

Legitimacy Theory is relevant due to the fact that ESG is measured by means of public disclosure. Banks may use information about their ESG-related activities to prove alignment with regulations and social expectations and minimize the level of information asymmetry (Suchman, 1995). However, disclosure may include substantive and symbolic components, so the high level of disclosure does not always mean good internal risk integration and higher stability. Therefore, **H1: ESG has a positive effect on bank stability.**

Operational risk might act as a transmission channel as it emerges due to failure or inadequacy of processes, people, systems, or external events (BCBS, 2026). ESG-related practices require reliable data, portfolio screening, reporting controls, capable employees, and cooperation with third parties. Hence, weak internal integration may increase operational difficulties, mistakes in reporting, compliance issues, and reputational risks.

On the other hand, proper integration is likely to improve internal controls and risk awareness. Galletta et al. (2023) found a negative relationship between ESG scores and operational risk using the global sample of banks and dynamic panel analysis. However, their ESG ratings were external and the country samples were different. Therefore, **H2: ESG has a negative effect on operational risk.**

Operational disruptions may cause financial losses, service disruptions, recovery costs, regulation issues, and reduction of customer confidence resulting in inability of banks to conduct stable operations. Uddin et al. (2023) state that digital transformation may increase operational risk exposure of banks but at the same time may create opportunities for efficiency and growth. Thus, it is expected that operational risk would decrease bank stability. Risk-weighted exposure might also reflect the size of business, technological activity, and capital allocation. Therefore, **H3: Operational risk has a negative effect on bank stability.**

Cyber Governance as a Moderating Capability

Cyber governance is an aspect of bank governance, operational risk management, and operational resilience based on the NIST CSF 2.0 and operational resilience principles of BCBS (NIST, 2024; BCBS, 2021). Banks become more and more dependent on IT systems, customer data, digital services, third-party IT providers, and financial infrastructure. Critical cyber incident may result in service interruption, financial losses, and reduction of public confidence which has implications for the financial stability (IMF, 2024). Consequently, cyber governance needs to be seen not just as a practice of IT security but as organizational capability.

OPEN ACCESS

According to the Resource-Based View, organizational success depends on valuable and organized internal resources and capabilities (Barney, 1991). Cyber governance includes governance oversight, cyber risk integration, incident response, continuity, and recovery capabilities. Such capabilities may help banks to manage the operational challenges of ESG-related banking practices, including data management, reporting, portfolio screening, and cooperation with third parties.

Bruno et al. (2025) examined the relationship between cybersecurity policy, ESG, operational risk, and bank performance but mostly considered them as factors affecting the profitability. Benthabet (2025) focused on cybersecurity policy as a moderator of the relationship between ESG and bank performance but used policy adoption as a measure of cyber governance and paid attention to performance. There is little research on the influence of broader cyber governance on the relationship between ESG and operational risk.

This paper attempts to fill the gap by using disclosure-based indexes of bank-level cyber governance, examining operational risk as a transmission channel to bank stability, and considering cyber governance as a moderating capability. The stronger cyber governance may improve data integrity, risk oversight, incident response, continuity, and recovery capabilities which will help banks to deal with the operational challenges of ESG-related practices. Therefore, **H4: Cyber governance negatively moderates the relationship between ESG and operational risk.**

METHOD

Research Design, Population, and Data

This study adopts a quantitative explanatory design using a census of all 17 Indonesian commercial banks classified as KBMI 3 and KBMI 4 as of December 2024. The balanced panel sample comprises four banks classified as KBMI 4 and 13 banks as KBMI 3 for the years 2019–2024, giving 102 bank-year observations. The year 2019 was chosen as the starting point since major financial institutions had reached the mandatory stage of sustainability reporting per POJK No. 51/POJK.03/2017 (OJK, 2017). Secondary data will be used in this research. Financial and risk data will be extracted from bank website, and other official documents issued by OJK and Bank Indonesia. Data on ESG and cyber governance will be collected from annual and sustainability reports. GDP growth of Indonesia will be obtained from the World Development Indicators. The data will be analyzed using STATA.

Variable Measurement

For ESG and cyber governance, we use manual content analysis based on the 0-3 depth-of-disclosure scale adopted from Arfiansyah, Murwaningsari, and Mayangsari (2024). Score 0 means no relevant disclosure, while high scores mean more disclosure. These indexes measure reported practices, but not necessarily their internal quality. The ESG index includes 9 indicators on environmental, social, and governance issues, which can receive a maximum score of 27. The indicators include environmental risk management procedure, screening coverage, climate risk, employee development, consumer protection, discrimination events, fraud disclosure, ESG integration in internal control, and board oversight. The index is developed based on the GRI Standards and financial sector disclosures (GRI, 2021).

The cyber governance index includes 3 indicators, which can receive a maximum score of 9. The indicators include governance oversight of cyber risks, cyber risk integration in enterprise and operational risk management, and cyber event response and operational resilience. The index is based on the governance and resilience concepts of the NIST Cybersecurity Framework and the BCBS operational resilience principles (NIST, 2024; BCBS, 2021). Manual content analysis allows disclosed governance frameworks and cyber practices to be examined in context, similarly to the cybersecurity disclosures studies (Elsayed, Ismail, & Ahmed, 2024). Bank stability will be considered as a measurable aspect of bank resilience and will be measured by the natural logarithm of the Z-score. Operational risk will be measured by Operational Risk-Weighted Assets over Risk-Weighted Assets (ORWA/RWA). ORWA/RWA is an indicator of the share of operational risk in the risk-weighted assets and should not be considered as a measure of actual operational loss. Controls will include bank size, GDP growth, and year dummy variables. As alternatives in the robustness analysis, the Cost-to-Income Ratio will be used as an operational efficiency proxy and gross Non-Performing Loan ratio as asset quality outcomes.

OPEN ACCESS

Table 1. Operational Definition and Measurement of Variables

Variable	Definition	Measurement
LnZscore	Bank stability	ln[(ROA + equity/total assets) / standard deviation of ROA]
ESGscore	ESG practices	Nine disclosure-based indicators scored 0–3; total range 0–27
CGscore	Cyber governance	Three disclosure-based indicators scored 0–3; total range 0–9
OpsRisk	Operational risk exposure	Operational Risk-Weighted Assets / total Risk-Weighted Assets
LnAsset	Bank size	Natural logarithm of total assets
GDPgrowth	Macroeconomic condition	Indonesia's annual GDP growth
CIR	Alternative operational efficiency proxy	Operating expenses / operating income
NPL	Alternative asset quality proxy	Non-performing loans / total loans

Source: Author's analysis (2026).

Data Analysis and Econometric Model

Before running the regression, LnZscore, OpsRisk, LnAsset, CIR, and NPL will be winsorized at the 5th and 95th percentiles. This ensures that any extreme values do not affect the analysis while including all observations of bank-year data. ESGscore and CGscore will not be winsorized since they are index scores with predetermined upper and lower bounds.

The regression analysis starts with descriptive statistics and then the Pearson Correlation and Variance Inflation Factor for checking multicollinearity. The Hausman test will be used for testing the Fixed Effects and Random Effects models while Modified Wald and Wooldridge will be used to test heteroskedasticity and autocorrelation.

Fixed Effect Model is chosen as the basic model since the research is concerned with changes occurring within individual banks, which requires controlling for time invariant factors such as ownership structure, business models, governance maturity, operational complexity, and risk culture. Robust standard errors and year dummy variable will be used in the main regression. Random Effect Model will be used for robustness analysis.

$$\mathbf{LnZscore_{i,t}} = \boldsymbol{\beta_0} + \boldsymbol{\beta_1}\mathbf{ESGscore_{i,t}} + \boldsymbol{\beta_2}\mathbf{LnAsset_{i,t}} + \boldsymbol{\beta_3}\mathbf{GDPgrowth_t} + \boldsymbol{\gamma}\,\mathbf{Year_t} + \boldsymbol{\varepsilon_{i,t}} \quad (1)$$

$$\mathbf{OpsRisk_{i,t}} = \boldsymbol{\beta_0} + \boldsymbol{\beta_1}\mathbf{ESGscore_{i,t}} + \boldsymbol{\beta_2}\mathbf{LnAsset_{i,t}} + \boldsymbol{\beta_3}\mathbf{GDPgrowth_t} + \boldsymbol{\gamma}\,\mathbf{Year_t} + \boldsymbol{\varepsilon_{i,t}} \quad (2)$$

$$\mathbf{LnZscore_{i,t}} = \boldsymbol{\beta_0} + \boldsymbol{\beta_1}\mathbf{ESGscore_{i,t}} + \boldsymbol{\beta_2}\mathbf{OpsRisk_{i,t}} + \boldsymbol{\beta_3}\mathbf{LnAsset_{i,t}} + \boldsymbol{\beta_4}\mathbf{GDPgrowth_t} + \boldsymbol{\gamma}\,\mathbf{Year_t} + \boldsymbol{\varepsilon_{i,t}} \quad (3)$$

$$\mathbf{OpsRisk_{i,t}} = \boldsymbol{\beta_0} + \boldsymbol{\beta_1}\mathbf{ESGscore_{i,t}} + \boldsymbol{\beta_2}\mathbf{CGscore_{i,t}} + \boldsymbol{\beta_3}(\mathbf{ESGscore_{i,t}} \times \mathbf{CGscore_{i,t}}) + \boldsymbol{\beta_4}\mathbf{LnAsset_{i,t}} + \boldsymbol{\beta_5}\mathbf{GDPgrowth_t} + \boldsymbol{\gamma}\,\mathbf{Year_t} + \boldsymbol{\varepsilon_{i,t}} \quad (4)$$

$$\mathbf{LnZscore_{i,t}} = \boldsymbol{\beta_0} + \boldsymbol{\beta_1}\mathbf{ESGscore_{i,t}} + \boldsymbol{\beta_2}\mathbf{CGscore_{i,t}} + \boldsymbol{\beta_3}\mathbf{OpsRisk_{i,t}} + \boldsymbol{\beta_4}(\mathbf{ESGscore_{i,t}} \times \mathbf{CGscore_{i,t}}) + \boldsymbol{\beta_5}\mathbf{LnAsset_{i,t}} + \boldsymbol{\beta_6}\mathbf{GDPgrowth_t} + \boldsymbol{\gamma}\,\mathbf{Year_t} + \boldsymbol{\varepsilon_{i,t}} \quad (5)$$

In the equations, i represents the bank, t represents the year, β_0 is the constant, β represents the estimated coefficient, μ_i represents the bank-specific fixed effect, γ represents year effects, and ε_{it} is the error term. The ESGscore × CGscore interaction is used to test the moderating role of cyber governance.

Statistical significance is assessed at the 1%, 5%, and 10% levels, with the 10% level interpreted as marginal evidence. Robustness analysis uses NPL and CIR as alternative measures and the Random Effects Model as an alternative estimator. Additional analysis uses lagged ESG and cyber governance variables and compares government-owned and non-government banks.

RESULTS AND DISCUSSION

Descriptive Statistics and Model Diagnostics

Table 2 presents the descriptive statistics for 17 KBMI 3 and KBMI 4 banks during the 2019-2024 period. LnZscore has a mean of 3.601, whereas OpsRisk has a mean of 0.122, meaning that the weight of operational risks is about 12.2% of the overall risk weight of assets. ESGscore averages 23.304 out of 27, and CGscore averages 8.784 out of 9, implying that ESG-related banking practices and cyber governance are disclosed in relatively high levels.

OPEN ACCESS

Table 2. Descriptive Statistics

Variable	N	Mean	SD	Min	Median	Max	Skewness	Kurtosis
LnZscore	102	3.601	0.436	2.965	3.522	4.413	0.258	2.003
ESGscore	102	23.304	2.673	17.000	23.500	27.000	-0.306	2.106
CGscore	102	8.784	0.556	6.000	9.000	9.000	-2.818	10.963
OpsRisk	102	0.122	0.042	0.057	0.121	0.191	0.031	1.830
LnAsset	102	33.346	0.851	32.389	33.012	34.992	0.866	2.301
GDPgrowth	102	0.037	0.026	-0.021	0.050	0.053	-1.644	3.906
CIR	101	0.508	0.104	0.351	0.493	0.715	0.496	2.271
NPL	102	0.025	0.008	0.012	0.026	0.040	-0.052	1.937

Source: STATA Output, Processed Data (2026).

Except for CGscore, most variables have moderate skewness and kurtosis values. CGscore shows the most significant skewness (-2.818) and kurtosis (10.963), implying the presence of a ceiling effect. In other words, the variable is not very variable due to the large number of observations close to the highest value. Negative skewness of GDPgrowth is mainly driven by economic contraction during the pandemic period. The correlation and multicollinearity tests show no signs of any problem. The largest absolute correlation between the variables is 0.4645 between ESGscore and LnAsset. VIF values range from 1.07 to 1.51 (the mean value is 1.27), proving that the problem of multicollinearity does not occur.

The results of the Hausman test imply that the p-value is 0.8273, which means that the Random Effects Model can be considered statistically acceptable. Nonetheless, the Fixed Effects Model serves as the main estimation technique because the analysis aims to reveal within-bank dynamics. The modified Wald and Wooldridge tests identify heteroscedasticity ($p<0.001$) and the presence of first-order autocorrelation ($p=0.0051$). That is why the main models are estimated with robust standard errors and the use of year dummy variables.

Main Regression Results and Discussion

Table 3 presents the results of the five Fixed Effects models with robust standard errors and year dummy variables. The results are discussed according to H1–H4.

Table 3. Fixed Effects Regression Results

Variable	M1 LnZscore	M2 OpsRisk	M3 LnZcore	M4 OpsRisk	M5 LnZscore
ESGscore	0.0065 (0.0057)	0.0053 (0.0030)	0.0030 (0.0056)	0.0673* (0.0340)	-0.0100 (0.0594)
CGscore				0.1580* (0.0853)	-0.0555 (0.1597)
ESGscore × CGscore				-0.0070* (0.0038)	0.0012 (0.0071)
OpsRisk			0.6789* (0.3357)		0.7052** (0.3309)
LnAsset	-0.0265 (0.1867)	0.0641 (0.0960)	-0.0698 (0.1279)	0.0848 (0.0971)	-0.1260 (0.1349)
GDPgrowth	-322.5610 (610.7052)	-869.3097*** (271.2443)	267.5956 (572.2281)	-944.6071*** (279.9480)	749.8863 (721.6940)
Year dummy	Yes	Yes	Yes	Yes	Yes
Observations	102	102	102	102	102
Within R-squared	0.1478	0.5904	0.2110	0.6117	0.2393
Prob > F	0.0909	0.0000	0.0098	0.0000	0.0021

Note: Robust standard errors are reported in parentheses. *, **, and *** indicate significance at the 10%, 5%, and 1% levels, respectively.
Source: STATA Output, Processed Data (2026).

OPEN ACCESS

Model 1 shows the insignificant positive coefficient of ESGscore (0.0065). ESGscore is also insignificant in Model 5 after the introduction of CGscore, operational risk, and their interaction term. Thus, H1 is not supported. This means that ESG does not directly explain within-bank changes in stability during the observation period. It is consistent with literature that the effect of ESG depends on the institutional context and quality of implementation (Azmi, Hassan, Houston, & Karim, 2021; Do, Ho, Mai, Nguyen, & Nguyen, 2024). Since ESG score is disclosure-based, the insignificant effect of the variable may be also explained by the difference between reported practices and the real implementation.

Model 2 provides the result of the insignificant positive ESGscore coefficient (0.0053). Hence, H2 is not supported. It is inconsistent with the results obtained by Galletta, Goodell, Mazzù, and Paltrinieri (2023), which prove that better ESG performance is linked to lower operational risk in a global sample of banks. The difference may be caused by the different way of measuring ESG and institutional context. In particular, the previous study uses the external rating of ESG, while this paper develops a disclosure-based index for Indonesian banks. Furthermore, it may take time for the benefits of data collection, screening, reporting, IT development, and cross-functional cooperation to become evident.

In Model 3, OpsRisk has the positive coefficient of 0.6789 and is significant at the 10% level. In Model 5, the coefficient of OpsRisk becomes 0.7052 and is significant at the 5% level. Since the direction of the relationship is opposite to the expected one, H3 is not supported. This result does not prove that operational failures increase bank stability. In this study, OpsRisk is measured using ORWA/RWA, which means the weight of operational risk-weighted assets rather than realized losses. Thus, higher values imply the bigger business scale, digital activities, operational complexity, and capital assigned to operational risk-weighted assets.

Large banks may report bigger operational risk-weighted assets while being in a good capital position and having well-developed controls. The positive coefficient is explained by the risk exposure and capital absorption pattern observed in the KBMI 3 and KBMI 4 segment. This is consistent with findings according to which the digital transformation may create additional operational exposure as well as opportunities for growth (Uddin, Mollah, Islam, & Ali, 2023).

Model 4 presents the key finding of this research. The coefficient of the interaction term ESGscore × CGscore is -0.0070 and is significant at the 10% level. Thus, H4 is supported with some marginally significant evidence. When the model contains an interaction term, ESGscore and CGscore should not be interpreted as the unconditional effects. The marginal effect of ESGscore on OpsRisk is:

Marginal effect of ESGscore = 0.0673 − 0.0070(CGscore)

The marginal effect decreases from approximately 0.0253 when CGscore equals 6 to 0.0043 when CGscore equals 9. It means that the marginal relationship between ESG and operational risk becomes weaker as cyber governance increases. The result does not prove that cyber governance directly lowers realized operational losses. On the contrary, it implies that strong cyber governance may help banks manage the data, systems, processes, and third parties connected to ESG-related banking practices. Board oversight, cyber risk integration, incident response, business continuity, and recovery functions may be considered as the complementary capabilities. The result supports the Resource-Based View theory and is consistent with studies according to which the cybersecurity policy is positively related to ESG-related banking practices (Benthabet, 2025; Bruno, Pistolesi, & Teti, 2025). However, the interaction term is insignificant in Model 5 with the LnZscore as the dependent variable. It means that the moderating effect of cyber governance extends to the ESG – operational risk relationship but not to the ESG – bank stability.

Robustness and Additional Analysis

The Random Effects results confirm the main moderation finding. The interaction term ESGscore × CGscore remains negative and becomes significant at the 5% level ($\beta = -0.0061$), while OpsRisk maintains the positive relationship with bank stability in the full model ($\beta = 0.7007$, $p < 0.10$). It means that the results of this study are not confined to the Fixed Effects approach. The interaction term is insignificant when NPL is used as the alternative dependent variable, implying that the moderating effect is more related to operational risk exposure than to asset quality. CIR has the negative and significant relationship with LnZscore ($\beta = -0.4843$, $p < 0.05$), meaning that lower operational efficiency is associated with lower bank stability. The lagged specification shows the positive and significant interaction between prior-year ESG and cyber governance in the explanation of bank stability ($\beta = 0.0188$, $p < 0.01$). It implies that the financial implications of ESG and cyber governance may take time to appear. However, the result is considered as the supplementary evidence. Ownership analysis proves that the positive OpsRisk-stability

OPEN ACCESS

relationship is significant in government-owned banks ($\beta = 1.0673$, $p < 0.01$), while the relationship is insignificant in non-government banks.

Practical Implications

It may be concluded that ESG-related banking practices, cyber governance, and operational risks should not be managed separately as reporting and compliance areas. Since cyber governance moderates the ESG-Operational risk relationship, the operational effects of ESG may partly depend on supporting governance, systems, and controls. Thus, this paper proposes the KRI-Based ESG-Cyber Governance-Operational Risk Monitoring Framework. The framework unites some selected ESG, cyber governance, and operational resilience indicators in one monitoring view. It complements Risk and Control Self-Assessment and loss event data. While RCSA is used for risk identification and control assessment, loss event data is helpful in getting the feedback from actual incidents. Finally, KRIs are responsible for continuous monitoring and providing early warnings.

Table 4. Illustrative Integrated KRI Monitoring Areas

Monitoring Area	Illustrative KRIs	Purpose
ESG-related operational risk	ESG data corrections or restatements; percentage of new products assessed for ESG and operational risk; ESG initiatives reviewed for cyber and privacy risk	Monitor data quality and process integration
Cyber governance and digital resilience	Overdue high-risk cyber findings; customer-impacting cyber, IT, or privacy incidents; critical vendors assessed for cyber and BCP/DRP risk	Monitor digital and third-party exposure
Integrated operational resilience	BCP/DRP test completion; operational loss events related to IT, cyber, reporting, or process failure; overdue corrective actions	Support early warning, escalation, and recovery readiness

Source: Author's analysis (2026).

Implementation of the framework may start from the mapping of existing indicators and assigning each KRI with a clear definition, data source, owner, reporting frequency, threshold, and escalation procedure. The indicators may be discussed in existing risk and management committees depending on the bank size, business model, risk profile, risk appetite, and available data.

CONCLUSION

This research uses balanced panel data from 17 KBMI 3 and KBMI 4 banks in Indonesia during 2019–2024 to examine ESG, cyber governance, operational risk, and bank resilience, with bank stability used as its measurable aspect. The results show no significant relationship between ESG and either bank stability or operational risk. Operational risk is positively related to bank stability, reflecting risk exposure and capital absorption rather than implying that operational problems improve stability. The main finding is that cyber governance negatively moderates the relationship between ESG and operational risk. Stronger cyber governance reduces the marginal association between ESG and operational risk, although the interaction does not directly explain bank stability.

This study contributes by integrating these variables within a broader bank resilience perspective and proposing a KRI-Based ESG–Cyber Governance–Operational Risk Monitoring Framework. Its limitations include reliance on public disclosure, a six-year period, and a sample limited to large Indonesian banks. Future research may include other bank groups and longer observation periods to test whether the findings remain consistent across different banking conditions. It may also use internal governance data, cyber incidents, or realized operational losses to better capture implementation quality and actual operational risk exposure.

REFERENCES

Arfiansyah, Z., Murwaningsari, E., & Mayangsari, S. (2024). Financial report quality, ESG disclosure, risk disclosure, audit quality and idiosyncratic risk: Evidence from Indonesian companies. Journal of Research Administration, 6(1), 4839–4864.

Azmi, W., Hassan, M. K., Houston, R., & Karim, M. S. (2021). ESG activities and banking performance: International evidence from emerging economies. Journal of International Financial Markets, Institutions and Money, 70, 101277. https://doi.org/10.1016/j.intfin.2020.101277

OPEN ACCESS

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

Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.

Basel Committee on Banking Supervision. (2026). The Basel Framework. Bank for International Settlements.

Benthabet, S. (2025). When ESG meets cybersecurity: The moderating effect of digital protection on bank performance in MENAT countries. International Journal of Economics and Financial Issues, 15(6), 356–370. https://doi.org/10.32479/ijefi.21354

Biswas, A., Das, A., Tiwari, A. K., & Patro, A. (2025). Do environmental, social, and governance (ESG) practices help mitigate bank default risk? Journal of Environmental Management, 380, 124762. https://doi.org/10.1016/j.jenvman.2025.124762

Bruno, E., Pistolesi, F., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. International Review of Economics & Finance, 99, 104053. https://doi.org/10.1016/j.iref.2025.104053

Deegan, C. (2002). Introduction: The legitimising effect of social and environmental disclosures—A theoretical foundation. Accounting, Auditing & Accountability Journal, 15(3), 282–311. https://doi.org/10.1108/09513570210435852

Defung, F., Yudaruddin, R., Ambarita, N. P., Che-Yahya, N., & Bahrudin, N. Z. (2024). The impact of ESG risks on bank stability in Indonesia. Banks and Bank Systems, 19(4), 194–204. https://doi.org/10.21511/bbs.19(4).2024.15

Do, H. L., Ho, H. H., Mai, T. C., Nguyen, T. N., & Nguyen, T. S. (2024). Does ESG really matter to the bank's stability in ASEAN countries? Cogent Economics & Finance, 12(1), 2420218. https://doi.org/10.1080/23322039.2024.2420218

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. Academy of Management Review, 20(1), 65–91. https://doi.org/10.2307/258887

Elsayed, D. H., Ismail, T. H., & Ahmed, E. A. (2024). The impact of cybersecurity disclosure on banks' performance: The moderating role of corporate governance in the MENA region. Future Business Journal, 10, 115. https://doi.org/10.1186/s43093-024-00402-9

Freeman, R. E. (1984). Strategic management: A stakeholder approach. Pitman.

Galletta, S., Goodell, J. W., Mazzù, S., & Paltrinieri, A. (2023). Bank reputation and operational risk: The impact of ESG. Finance Research Letters, 51, 103494. https://doi.org/10.1016/j.frl.2022.103494

Global Reporting Initiative. (2021). GRI 1: Foundation 2021.

International Monetary Fund. (2024). Cyber risk: A growing concern for macrofinancial stability. In Global financial stability report, April 2024: The last mile—Financial vulnerabilities and risks.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). U.S. Department of Commerce.

Otoritas Jasa Keuangan. (2017). Peraturan Otoritas Jasa Keuangan Nomor 51/POJK.03/2017 tentang penerapan keuangan berkelanjutan bagi lembaga jasa keuangan, emiten, dan perusahaan publik.

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. Academy of Management Review, 20(3), 571–610. https://doi.org/10.2307/258788

Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? Technological Forecasting and Social Change, 197, 122919. https://doi.org/10.1016/j.techfore.2023.122919

World Bank. (n.d.). GDP growth (annual %)—Indonesia [Data set]. World Development Indicators. Retrieved January 31, 2026, from https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=ID

Yoo, S., & Managi, S. (2022). Disclosure or action: Evaluating ESG behavior towards financial performance. Finance Research Letters, 44, 102108. https://doi.org/10.1016/j.frl.2021.102108

OPEN ACCESS