DISCLOSURES OF CYBER EXPOSURE AND AUDIT FEES: EVIDENCE FROM ASEAN-4 BANKING

Etikah Karyani [*], Ana Noveria [**], Taufik Faturohman [**], Raden Aswin Rahadi [**]

[*] *Corresponding author,* Accounting Department, Faculty of Economics and Business, Sebelas Maret University, Surakarta, Indonesia
Contact details: Sebelas Maret University, Jalan Ir. Sutami 36 Kentingan, Jebres, 57126 Surakarta, Jawa Tengah, Indonesia
[**] School of Business and Management, Institute of Technology Bandung, Bandung, Indonesia

OPEN ACCESS

How to cite this paper: Karyani, E., Noveria, A., Faturohman, T., & Rahadi, R. A. (2023). Disclosures of cyber exposure and audit fees: Evidence from ASEAN-4 banking [Special issue]. *Corporate Governance and Organizational Behavior Review, 7*(4), 299–312. https://doi.org/10.22495/cgobrv7i4sip8

ISSN Online: 2521-1889
ISSN Print: 2521-1870

Received: 06.03.2023
Accepted: 04.12.2023

JEL Classification: E50, E58, G21, M41, M42
DOI: 10.22495/cgobrv7i4sip8

Abstract

This study examines how external auditors respond to the disclosure of cyber exposures by commercial banks and how the COVID-19 pandemic period accentuates the effect of voluntary cyber risk disclosures (CRDs) on audit fees. Our study is a preliminary study analysing the CRD of the financial industry in emerging economies in the Association of Southeast Asian Nations (ASEAN). It extends Calderon and Gao's (2021) study one step further with respect to the COVID-19 pandemic and identifies items by using manually collected keywords to extract CRDs. During the period 2015–2020, our samples are 63 listed banks in four ASEAN members (Indonesia, Malaysia, Thailand, and the Philippines — ASEAN-4) and the one-step generalized method of moments (GMM) is used. The study found that audit fees are significantly associated with CRD, including risk causes and impacts. Meanwhile, cyber risk governance disclosures affect audit fees after a one-year lag. This indicates that voluntary CRD is informative. Audit fees are also significantly affected by the interaction between CRD and COVID-19. It suggests that auditors incorporate the nature and content of client CRDs into their fee structure and directly support regulatory reporting requirements in emerging ASEAN countries to include cyber risk factors in annual bank statements.

Keywords: Cyber Risk Governance, Audit Service, Cyber Attack, Generalized Method of Moments

Authors' individual contribution: Conceptualization — E.K., A.N., T.F., and R.A.R.; Methodology — E.K. and A.N.; Formal Analysis — E.K.; Investigation — E.K. and A.N.; Writing — Original Draft — E.K.; Writing — Review & Editing — E.K.; Project Administration — T.F. and R.A.R.

Declaration of conflicting interests: The Authors declare that there is no conflict of interest.

Acknowledgements: This research received a specific grant from the School of Business and Management at the Institute of Technology Bandung (SBM-ITB) Postdoctoral Research Fellowship (Grant No. 280139/27/PL-J/DM/KP/08/2021).

1. INTRODUCTION

The banking world is evolving to become increasingly digital in reporting its financial statements, collecting funds from the public, and investing nationally and internationally. Fitch Ratings (2020) conducted a survey and found that online banking activities throughout the Association of Southeast Asian Nations (ASEAN) region had spiked sharply since the beginning of the pandemic. For example, Bank Rakyat Indonesia (Persero) Tbk. reported growth in internet banking activity of around 88% year on year (YoY) in the first quarter of 2020 (1Q20), and a similar trend occurred in many major banks in the Philippines and Malaysia. In addition to higher digital transactions, Singapore's three major banks reported a significant increase in digital account opening or use of "robo-advisory" financial planning services platforms over the same period. Unfortunately, technological improvements being developed and increasingly implemented in the banking industry have provided new opportunities for cyber fraudsters and hackers since the COVID-19 pandemic began. The Financial Industry Cybersecurity Report (FICR) reported that cybercrime was recognized as the second-highest source of economic abuse in global financial institutions (Uddin et al., 2020). According to Kopp et al. (2017), the financial sector is one of the most targeted sectors related to cybercrime because of its dependence on information and its central role in the credit intermediation process. Therefore, regulators require banks to identify and report their risk profile.

Accounting literature has intensively investigated pricing decisions or audit fees. Previous studies show that accounting firms charge fees to assess client characteristics, including risk, governance, daily operations, and long-term strategic business decisions (Wu, 2012; Rosati et al., 2019; Smith et al., 2019; Yang et al., 2018; Musa et al., 2021). A higher client business risk and potential client litigation risk will require greater auditor involvement by increasing effort or incurring an additional risk premium (Simunic, 1980). Higher client risk is associated with higher audit fees. Furthermore, the Standing Advisory Group (SAG) of the Public Company Accounting Oversight Board (PCAOB) emphasized the potential implications of cybersecurity for financial reporting and auditing (PCAOB, 2014). Financial statement audits are determined by how clients disclose cybersecurity risks and cyberattacks (Institute of Singapore Chartered Accountants [ISCA], 2018; Calderon & Gao, 2021). This raises the question of whether the cybersecurity risks published by companies are relevant to the audit of financial statements and what extent the role of the pandemic (crisis) period influences this relationship.

This study aims to broaden previous studies by associating cyber risk disclosure (CRD) with audit fees. The study is expected to fill the research gap related to the measurement method of risk disclosure and background setting. This research contributes to the literature in two ways. Firstly, our study contributes to the literature on audit fees by explicitly associating CRDs with the audit fees model. Our study extends the work of Calderon and Gao (2021), who examined the association between CRD and audit fees by going one step further during the COVID-19 pandemic. We also modified the CRD measurement based on a rule proposed by the Securities and Exchange Commission (SEC) in March 2022, which requires public companies to disclose cybersecurity[1]. Furthermore, this measurement is implied to an index obtained from the content analysis. Aldasoro et al. (2021) showed that the financial sector has been more frequently affected by cyber-attacks than most other sectors since the COVID-19 pandemic. Phishing attacks, for example, explicitly use uncertainty during COVID-19 to entice users to open fraudulent attachments or give hackers access to networks.

Secondly, to the best of our knowledge, our study is the first to examine the effect of a bank's CRD on audit fees in ASEAN-4 (Indonesia, Malaysia, Thailand, and the Philippines) emerging economies. Previous research linking auditor responses to cyber incidents focuses on the implications of cyber breaches, which imply an increased risk of internal control weaknesses and material misstatements (Rosati et al., 2019; Smith et al., 2019; Li et al., 2020). Audit costs are closely related to client risk characteristics, accounting method selection, day-to-day operational decisions, and long-term strategic business decisions (Bell et al., 2001). In addition, previous research mostly observes the effect of companies disclosing cyber risks on audit fees in developed countries (Moreira, 2019; Calderon & Gao, 2021; Li et al., 2020; Cheong et al., 2021). Meanwhile, this study focuses on ASEAN banks, which are the main targets of cyberattacks (A.T. Kearney, 2018). This is possible due to high digital connectivity, inversely proportional to low cybersecurity awareness, ever-increasing cross-border data transfers, and weak regulations (Hedrich et al., 2017).

Our tests are based on a sample of 63 banks in the 2015–2020 fiscal year. We reviewed disclosure decisions by managers after data breaches and used a more comprehensive keyword list approach to identify CRDs. We found that audit fees are related to the extent of disclosure, indicating that a bank's CRD is informative in determining the level of auditors' judgment. However, the governance of CRD does not significantly affect the audit rate. Therefore, this study examines the effect of this lagged variable on audit fees in an additional analysis. We found that the governance of the bank's CRD in the previous period increased current audit fees. Furthermore, the COVID-19 pandemic lowered audit fees for banks that disclose the total, causes, and impacts of cyber risk. Furthermore, our study adds analysis by replacing audit fees with audit tenure, suggesting that total and individual CRD (risk governance, causes, and impacts) do not affect audit tenure. This means that banks want to be audited by incumbent auditors with a better understanding of the firm's condition.

The remaining parts of the paper are structured as follows. Section 2 reviews the existing literature and develops our hypotheses. Section 3 describes the data and methodology used in this study. Section 4 presents the empirical results. Section 5 summarizes the findings and implications for the literature, regulators, and practitioners.

2. LITERATURE REVIEW AND HYPOTHESES DEVELOPMENT

2.1. Requirement of voluntary CRD and audit fee in ASEAN-4

The term "cyber risk" refers to "operational risks to information and technology assets that have

[1] In response to an increase in high-profile cyberattacks, the SEC is increasing its oversight of corporate cybersecurity risk disclosures and their policies, procedures, and controls to address these risks by issuing *CF Disclosure Guidance: Topic No. 2* (SEC, 2011), which requires companies to disclose the risks of cyber incidents.

consequences affecting the confidentiality, availability, or integrity of information or information systems" (Cebula et al., 2014, p. 2). As a result of the increasing number and severity of cybersecurity incidents since COVID-19, several financial regulators in ASEAN countries have issued guidelines regarding CRDs that public companies must submit to investors. The Financial Services Authority (*Otoritas Jasa Keuangan* — OJK) of Indonesia, has issued regulations comprising cyber incident response and recovery using components similar to those found in the Financial Stability Board (FSB) toolkit through Regulation No. 38/POJK.03/2016 on implementation of information and technology risk management by banks as amended by OJK Regulation No. 13/POJK.03/2020 and OJK Circular Letter No. 21/SEOJK.03/2017. Furthermore, OJK periodically evaluates banks' information technology involving cyber events as part of the operational risk assessment. Unfortunately, their annual reports have no specific requirements for disclosing cybersecurity risks or incidents.

The SEC Philippines requires public companies that have experienced cybersecurity breaches exposed to material cybersecurity risks, but may not have been the target of cyberattacks, must report accurately and promptly. It was regulated in the draft *Guidance for Regulated Entities on Establishing and Maintaining a Cybersecurity Framework*, published in December 2020 (SEC, 2020). Meanwhile, the *Guidelines on Management of Cyber Risk* (SC-GL/2-2016) issued by the Securities Commission (SC) Malaysia on October 31, 2016 (SC Malaysia, 2016), clearly regulates, among other things, the board of directors and senior management's role and responsibilities in building the cyber resilience of capital market entities. In addition, the guidelines regulate the requirements for reporting to SC Malaysia the occurrence of cyber incidents or breaches daily. Furthermore, the Thai Bankers Association (TBA) implemented the personal data protection guidelines for Thai banks (the "Guidelines") to facilitate banking sector operations in conformity with the Personal Data Protection Act 2019 (PDPA). The PDPA was Thailand's first comprehensive data protection law, published in the *Royal Thai Government Gazette* on May 27, 2019, with full implementation planned for June 1, 2022.

As the ASEAN securities markets play an increasingly important role in global investment strategies, the audit function and reliability of audited financial information are becoming increasingly important. Favere-Marchesi (2000) examined the Big Five (Big-5) audit mechanism in seven ASEAN countries. It was stated that audit fees, in addition to audit and client rotation, are mechanisms used by auditors to reduce threats to auditor objectivity. Audit fees refer to remuneration earned by accounting firms and auditors for providing professional services.

Simunic (1980) introduced the theory underlying audit fees; the previous literature on the determinants of audit fees in emerging economies is mixed. Audit fees are determined by the ownership structure (Nelson & Mohamed-Rusdi, 2015), company size (Rusmanto & Waworuntu, 2015; Van et al., 2022), audit complexity, reputation, and risk of audit firms (Van et al., 2022), and the COVID-19 pandemic (Al-Qadasi et al., 2022). Their study results show that audit fees are strongly related to the level of auditor risk (auditor attributes) and client risk (client attributes). Thus, the greater the risk, the more complex the audit procedures that need to be carried out, and the greater the allocation of human and material resources invested. When the necessary human and material resources are unable to reduce audit risk, they may choose to collect a risk premium to avoid claims for damages or compensate for possible future losses.

2.2. Effect of CRD, governance, causes, and impact of cyber risk on audit fees

Previous studies linking auditor responses to cyber incidents focused on the implications of cyber breaches, implying an increased risk of internal control weaknesses and material misstatements being committed (Rosati et al., 2019; Smith et al., 2019; Li et al., 2020). Audit fees are closely correlated with risk characteristics as cybersecurity incidents have increased dramatically (Yang et al., 2018; Smith et al., 2019; Li et al., 2020). The information asymmetry theory suggests that the level of risk disclosure can impact the audit fee, as it can impact the amount of work required by the auditor and the perceived level of risk associated with the company's operations.

Furthermore, the informativeness of corporate textual risk disclosures and cybersecurity incidents indicates a potential failure of internal control over financial reporting (Lawrence et al., 2018). In this case, the company's records may be altered, resulting in financial statement manipulation. Furthermore, more specific cybersecurity disclosures related to companies can improve audit quality, which the auditor responds to by increasing audit effort, ultimately increasing audit fees (Masoud & Al-Utaibi, 2022). Empirical findings show that companies with previous cybersecurity risk disclosures are more likely to experience financial reporting deficiencies, so the higher the audit quality requested, the higher the audit pricing. We also believe that auditors should charge higher fees from riskier clients if they can accurately assess a client's enterprise cybersecurity risks.

H1: CRD has a positive effect on audit fees.

Furthermore, this study divides the level of risk disclosure into three criteria: governance, causes, and impacts of cyber risk. These criteria are based on previous research, surveys, and guidelines. As the threats to cyber risk become more complex, executives need to know whether overall governance decisions on cyber risk management are optimal and what the causes and potential impacts of cyberattacks are on the organization.

Previous studies show a significant relationship between the level of governance and audit fees. On the one hand, the association between governance and audit fees is positive. Governance proxied by the governance structure of the board of directors increases audit fees (Yang, 2015). Khalil et al. (2008) also stated that separating the two forces is positively related to the audit fees of companies listed in Canada. In line with the findings of a study in China, the supervisory authority of the board of directors is eroded if the two powers are consolidated into one. Therefore, the auditor increases the control risk estimate during the audit, which increases the audit fee (Ye, 2020).

On the other hand, Wu (2012) found that better company management will reduce the audit fees the company must incur. Concerning the results of previous studies, we estimated the negative relationship between the governance of CRD and audit fees. This is in line with Bhuiyan et al. (2021), stating that a risk committee determines audit pricing. Furthermore, a risk committee monitors all information to reduce uncertainty and improve the quality of the risk information (Aebi et al., 2012; Karyani et al., 2020). Audit pricing can be lower because of a board that guarantees the effectiveness of cyber risk management. According to agency theory, a higher level of corporate governance can reduce the company's agency costs and audit risk so audit costs are also reduced (Leventis & Dimitropoulos, 2010). Implementing good risk governance indicates strong internal control, which can reduce the scope of audit work, and auditors conduct less testing, resulting in a lower audit fee because they will take a lot of time to complete the audit work. The less audit processing time, the lower the audit fee charged to the company.

H2a: Governance of cyber risk has a negative effect on audit fees.

When a cyber incident occurs, the auditor must understand its nature and causes (ISCA, 2018). External auditors are also in charge of reviewing their clients' losses, claims, and obligations linked to the incident, as well as the final impact of the financial statements (Center for Audit Quality [CAQ], 2014). According to the risk-based approach theory, audit fees are determined based on the level of risk associated with the company's operations. When companies disclose the causes and consequences of significant cyber risks, such as losses and legal effects, auditors may need to devote more time and resources to assessing and testing the effectiveness of the company's cybersecurity controls. This increased effort and risk may lead to higher audit fees.

Consistent with the findings of Lawrence et al. (2018) that cybersecurity events may indicate weaknesses in internal financial reporting controls. Thus, regardless of their nature, cybersecurity breaches have potential implications for auditors who must assess their clients' cybersecurity risks. We expect increased audit fees because of increased efforts (Rosati et al., 2019; Li et al., 2020). Auditees pay higher fees in response to reports of increased cybersecurity threats.

H2b: Causes of cyber risk have a positive effect on audit fees.

H2c: Impacts of cyber risk have a positive effect on audit fees.

2.3. The moderating effect of the COVID-19 pandemic

The COVID-19 pandemic presents a unique opportunity to study how auditors respond to exogenous shocks in a client's operating environment. Due to the COVID-19 pandemic, auditors were also under pressure from clients to cut audit fees due to the economic slowdown during COVID-19. Krishnan and Zhang (2014) show that audit fees decreased during the global crisis due to negotiations. Similar to the crisis, clients negotiate more stringently during the pandemic, reducing audit fees. The impact of the COVID-19 pandemic has been the toughest challenge for auditors and their clients due to increased financial issues, litigation, and hacking (Albitar et al., 2021). In other words, the potential effect of COVID-19 on the association between CRD and audit fees is unclear. Therefore, the third hypothesis of this study is:

H3: The COVID-19 pandemic affects the relationship between CRD (total and individual) and audit fees.

3. RESEARCH METHODOLOGY

3.1. Sample selection and data collection

The final sample is 352 bank years of 67 commercial banks listed in four ASEAN countries from 2015 to 2020. It consists of 27 Indonesian banks, 5 Malaysian banks, 11 Thailand banks, and 14 Philippines banks. We excluded regional or rural banks because they have less technology infrastructure and fewer cybersecurity risks. Data were collected from the English versions of the annual reports on the bank's official websites and BankFocus (Bureau van Dijk — BvD).

3.2. Variables description

The CRD was measured based on the index proposed by Calderon and Gao (2021) and Li et al. (2018) using the content analysis method to collect CRD data. The questions used to obtain the CRD index are listed in Table 1.

Table 1. CRD index for assessing practices of cyber risk disclosure (Part 1)

Questions	*Keywords*
1. Governance of cyber risks	
1.1. Does the bank's board (board of directors) take ownership of cyber risks?	– Risk board/risk director/cyber-risk oversight committee
1.2. Do they refer to any strategy/policy related to managing cyber risks?	– Cyber risk/cyber risk – Policy/strategy – Cyber risk/IT risk/cyber security/cyber-attack/cyber-thread/IT – Fraud/data-theft/data corruption/cyber insurance/data breach – Management/control
1.3. Does the bank define cyber risk clearly?	– Cyber risk/cyber-attack/cyber thread/cyber security/data-theft/data corruption/data breach is
1.4. Does the bank identify cyber risk as a material item?	– Material/significant/important – Attack/fraud/thread/risk/terrorist/incident/security, cyber-based attack, IT (security/attack), data theft, phishing, data corruption, cyber insurance, data breach, crimeware, ransomware, and keylogger
2. Causes of cyber risks incidents	*A description of the causes of incidents*
2.1. Malware	– Malware
2.2. Phishing/spear phishing	– Phishing/spear phishing
2.3. Spear phishing	– Spear phishing

Table 1. CRD index for assessing practices of cyber risk disclosure (Part 2)

Questions	*Keywords*
2.4. Man in the middle	– Man in the middle
2.5. Trojans	– Trojans
2.6. Ransomware	– Ransomware
2.7. Denial of service attack	– Denial of service attack
2.8. Attacks on IoT devices	– Attacks on IoT devices
2.9. Data breaches	– Data breaches
2.10. Malware on mobile apps	– Malware on mobile apps
3. The impact of cyber risk incidents	*A description of the impact on the bank*
3.1. Damage to the reputation	– Damage/reputation
3.2. Financial losses	– Financial losses/expenses
3.3. Legal actions or implications	– Legal actions/legal implications

Note: The CRD index for each bank year (CRD$_{it}$) uses disclosure indexes. The disclosure is classified into three categories: 1) governance of cyber risk, 2) causes of cyber risk, and 3) impacts of cyber risk. These categories were separated into 17 sub-categories or 17 items or scores. IoT — Internet of things.
Source: Calderon and Gao (2021), Li et al. (2018), Gensler (2022), Duvenhage (2020).

Table 1 explains the three main components of the CRD index, which were then developed into 17 items. In comparison, Calderon and Gao (2020) used a Python program to extract CRD by counting the number of words (*lnWords*). Our study identified items using keywords in a hand-collected manner. The scoring method uses a value of 1 for items that are disclosed and 0 for items that are not disclosed. The disclosure index is assessed using a non-weighted approach to avoid subjective judgments by assuming all items in the checklist are equally important. Thus, the index formula was used to calculate the CRD area index by dividing the number of items disclosed (*n*) by the number of items that should be disclosed (*k*). The more items a bank discloses, the higher the index score it obtains. Banks with higher index scores indicate more comprehensive disclosure. The validity and reliability tests were conducted to determine whether the governance of the cyber risk index was "good" or "adequate" based on Cronbach's alpha value of 0.60–0.70 (Clark & Watson, 1995). The study expects a negative relationship between cyber risk governance and audit fees. Meanwhile, the variables of total risk disclosure and the causes and consequences of risk are expected to be positively correlated with audit fees.

Furthermore, the control variables were used based on previous studies that include the bank's assets size (*SIZE*), leverage (*LEV*), non-performing loans (*NPL*), efficiency ratio (*EFFIC*), securities (*SECUR*), capital ratio (*CAR*), net loss (*NLOSS*), going-concern audit opinion (*GCO*), Big Four auditors (*BIG4*), auditor tenure (*INITIAL*), and gross domestic product growth (*GDPG*). We expected a positive association between audit fees and *SIZE, LEV, NPL, EFFIC, CAR, NLOSS, BIG4, INITIAL*, and *GDPG*. Otherwise, audit fees are expected to negatively correlate with *SECUR* and *GCO*. The impact of control variables on audit fees has been well documented in previous studies (Fields et al., 2004; Calderon & Gao, 2021).

3.3. Empirical models and estimation methods

The following table provides a summary of the research variables used.

Table 2. Operationalization of variables

Variables	*Measure*	*References*
Dependent variable		
Audit fee (*AFee*)	Natural logarithm of audit fee	Calderon and Gao (2021)
Independent variables		
Cyber risk disclosure (*CRD*)	*CRD* index = *n/k* * 100%	Calderon and Gao (2021), Li et al. (2018), Duvenhage (2020)
Governance of cyber risk (*GCR*)	*GCR* index = *n/k* * 100%	
Cause of cyber risk (*CAUSE*)	*CAUSE* index = *n/k* * 100%	
Impact of cyber risk (*IMPACT*)	*IMPACT* index = *n/k* * 100%	
Control variables		
Bank's assets size (*SIZE*)	Natural logarithm of total assets	Fields et al. (2004), Calderon and Gao (2021)
Leverage (*LEV*)	Total liabilities/total assets	Calderon and Gao (2021)
Non-performing loans (*NPL*)	Ratio of non-performing loans	Fields et al. (2004)
Efficiency ratio (*EFFIC*)	Total operating expenses/total revenue	Fields et al. (2004)
Securities investment (*SECUR*)	1 - (securities/total assets)	Fields et al. (2004)
Capital ratio (*CAR*)	Total risk-adjusted capital ratio	Fields et al. (2004)
Net loss (*NLOSS*)	Dummy variable equals 1 if the net loss is reported, 0 otherwise	Fields et al. (2004), Calderon and Gao (2021)
Going concern opinion (*GCO*)	Dummy variable equals 1 if the auditor issues a going-concern audit opinion in year *t*, and 0 otherwise	Calderon and Gao (2021)
Big-4 auditor (*BIG4*)	Dummy variable equals 1 if a Big-4 auditor is used, 0 otherwise	Calderon and Gao (2021)
Auditor tenure (*INITIAL*)	Dummy variable equals 1 if auditor tenure ≤ 2 years, 0 otherwise	Calderon and Gao (2020)
GDPG	Gross domestic product annual growth	World Bank (n.d.)

Note: This table reports the operationalization of variables. The first column describes the variables used in this study, and how to measure them is shown in the second column. Meanwhile, the third column explains that the variables to be tested come from prior research.
n — Fulfill item, k — Total item of disclosure.

Following the method used by previous researchers (Calderon & Gao, 2021; Li et al., 2020), we tested the effect of independent variables on dependent variables using the generalized method of moments (GMM). The GMM estimation technique avoids endogeneity problems by using the lag of the dependent variable as an instrument. Therefore, the research is expected to obtain consistent and unbiased results. Furthermore, the specification test of the dynamic panel data regression model consists of the Sargan test and the Arellano-Bond. The Sargan test is conducted to assess the instrument's validity with the criteria if the probability value of the J-statistic > 0.05, it means there is no endogeneity. In contrast, the Arellano-Bond test is used to see if autocorrelation exists in the model instrument used. The $v_{i,t}$ component is an aside assumed to have no autocorrelation, but the estimation in the first difference process is obtained ($v_{i,t}$-$v_{i,t-1}$), so $E(v_{i,t},\ v_{i,t-1})$ does not need to be zero. However, for the next order to see the consistency of the GMM estimator, the assumption $E(v_{i,t},\ v_{i,t-2}) = 0$ or the absence of autocorrelation between $v_{i,t}$ and $v_{i,t-2}$ is still applied.

4. RESULTS AND DISCUSSION

4.1. Cyber risk disclosure (CRD)

The average score and the validity test result used a significance level of 5% with an *r*-table of 0.097 (not tabulated). About 80% of firm-years have disclosures about bank boards taking over cyber risk and referring to any strategy/policy related to cyber risk management. However, almost none of the firm years conveyed information that cyber risk was caused by spear phishing, a man in the middle, trojans, and malware on mobile applications. The greatest cause of cyber risk is the attack on Internet of things (IoT) devices and data breaches. In addition, none of the banks disclosed cyber risks that impacted legal issues. Meanwhile, most cyber risks have implications for bank reputations. This is an important parameter receiving attention from global investors and regulators regarding reputational damage and intellectual property loss resulting from cyber incidents (Li et al., 2018).

The level of CRD in the sample shows an increasing trend from year to year (2015–2020) (not tabulated). This finding complements the study of Hilary et al. (2016), who did not find a significant increase in cybersecurity risk disclosure after a data breach, implying that cybersecurity risk disclosure in the risk factors and management discussion and analysis (MD&A) sections were not informative. Collectively, Malaysian banks performed well, with 48% of them mentioning cyber risk in their annual reports in 2018 and 2019. This was followed by 43% of banks in Thailand in 2020. The highest CRD rates for Indonesian and Philippine banks at approximately 30% were achieved in 2020. Thus, the highest CRD level in ASEAN-4 banking occurred in 2020. Finally, we excluded items that did not have a value or whose value was invalid, and the reliability test results show that Cronbach's coefficient value was 0.675.

4.2. Multivariate analysis

Table 3 reports the descriptive statistics of the sample from 2015 to 2020. It shows that the mean of audit fees was $204,802.22 (corresponding to the natural logarithm value of 12,229). The average of the four CRD measures was 0.2441 (24.41%), 0.5671 (56.71%), 0.0730 (7.3%), and 0.0729 (7.29%) for the total risk disclosure, governance, causes, and effects of cyber risk, respectively. Risk governance (*GCR*) has the highest level of disclosure, which shows the concern of the board of directors or the board of possible cyber risks. However, the board's role was not followed by the disclosure of causes (*CAUSE*) and consequences (*IMPACT*) of corporate risk events.

Table 3. Summary of statistics

Variables	*N*	*Mean*	*Standard deviation*	*Minimum*	*Maximum*
lnAFee	352	12.224	1.203	9.780	15.530
CRD	352	0.244	0.158	0	0.750
GCR	352	0.567	0.301	0	1
CAUSE	352	0.073	0.140	0	0.710
IMPACT	352	0.073	0.200	0	1
lnSIZE	352	22.721	1.795	18.10	25.54
LEV	352	0.814	0.169	0.030	0.950
NPL	352	0.034	0.026	0.002	0.238
EFFIC	352	0.597	0.776	0.140	7.720
SECUR	352	0.913	0.140	0.099	0.999
CAR	352	0.197	0.075	0.080	0.660
NLOSS	352	0.077	0.267	0	1
GCO	352	0.043	0.203	0	1
BIG4	352	0.777	0.417	0	1
INITIAL	352	0.197	0.398	0	1
GDPG	352	0.033	0.041	-0.096	0.072

Note: The table presents the summary statistics of the 352 firm years.

Table A.1 (see Appendix) presents the Pearson correlation between audit fees and various *CRD* measures of CRD. The correlation coefficient between the log of audit fees (*lnAFee*) and the three types of risk disclosure (*CRD, GCR,* and *CAUSE*) is significantly positive. In contrast, the consequences of cyber risk (*IMPACT*) are not significant. Moreover, Table A.1 also proves that it does not contain multicollinearity problems because the correlation value between independent variables was quite low (< 0.85).

Table 4 shows the coefficient value used to examine the association between *lnAFee* and all models indicated in columns 1–4. Panel A of Table 4 explains the model with no *COVID* effect, while Panel B of Table 4 includes the *COVID* variable. In general, the coefficient value of all the main independent variables is positive, which is in accordance with the prediction. Furthermore, the probabilities of the J-stat and *AR*(2) values for all the models are above the significance value (p > 0.05), which means that the equation results do not experience endogenous problems and are valid.

Table 4. Result of Models 1, 2, 3, and 4 (GMM model)

Variables	***Predicted sign***	***Panel A***				***Panel B***			
		CRD	***GCR***	***CAUSE***	***IMPACT***	***CRD***	***GCR***	***CAUSE***	***IMPACT***
		(SE)	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***
lnAFee	+	0.5542***	0.5549***	0.5542***	0.7074***	0.0180	0.3640	-0.5687*	0.6271**
		(0.1449)	(0.1804)	(0.1449)	(0.1773)	(03378)	(03377)	(03393)	(0.2732)
CRD	+	0.3352**				0.7580**			
		(0.1708)				(0.2915)			
GCR	-		0.0390				0.0809		
			(0.1158)				(0.1481)		
CAUSE	+			0.2871*				2.1729***	
				(0.1688)				(0.8353)	
IMPACT	+				0.3099***				0.9420***
					(0.1016)				(0.0979)
COVID	+					1.1807**	0.6813*	0.5118	0.2011
						(0.5181)	(0.3731)	(0.3543)	(0.1896)
*CRD * COVID*	+					-3.0570**			
						(1.3428)			
*GCR * COVID*	+						-0.6607		
							(0.4850)		
*CAUSE * COVID*	+							-12.1643***	
								(3.0839)	
*IMPACT * COVID*	+								-0.9462***
									(0.2512)
lnSIZE	+	0.3164***	0.3679***	0.3291***	0.3688***	0.2970***	0.4460***	0.2643	0.2898***
		(0.0672)	(0.0728)	(0.0705)	(0.0798)	(0.0919)	(0.1036)	(0.0825)	(0.0954)
LEV	+	-0.2217	-0.5196	-0.3137	-0.3062	-0.2261	-0.5108	-1.6606	-0.0676
		(0.4713)	(0.4848)	(0.3952)	(0.5143)	(0.4698)	(0.5553)	(1.7385)	(0.4723)
NPL	+	0.3355	0.4430**	0.4465	0.1412	1.1362	0.6922	0.0421	0.1438
		(0.7292)	(0.7618)	(0.7841)	(0.8929)	(0.9803)	(0.9542)	(1.7385)	(0.8392)
EFFIC	-	-0.0046*	-0.0044	-0.0042	-0.0057	0.0042	-0.0012	0.0107	-0.0039
		(0.0025)	(0.0042)	(0.0036)	(0.0038)	(0.0050)	(0.0041)	(0.0083)	(0.0031)
SECUR	-	-0.0001*	-0.0001**	-0.0001	-0.0001	-0.0003	-0.0001**	0.0001	-0.0001
		(0.0003)	(0.0005)	(0.0004)	(0.0004)	(0.0004)	(0.0001)	(0.0001)	(0.0001)
CAR	-	-0.5183*	-0.6280	-0.5265**	-0.5152*	-1.0733**	-0.9077**	-2.5061**	-0.1049**
		(0.2900)	(0.4288)	(0.2451)	(0.2989)	(1.4910)	(0.4147)	(1.1855)	(0.3263)
NLOSS	+	0.1796	0.1622	0.1973	0.1781	0.1069	-0.14277	-0.0581	0.1868
		(0.1345)	(0.1442)	(0.1487)	(0.1509)	(0.1016)	(0.1140)	(0.1394)	(0.1426)
GCO	+	0.0945	0.0998	0.0831	0.1469	0.3931**	0.3135**	0.2899	0.1289
		(0.1370)	(0.1407)	(0.1539)	(0.1259)	(0.1800)	(0.1149)	(0.3405)	(0.1118)
BIG4	+	0.2545	0.2419	0.2569	0.3516**	0.3457**	0.3582**	0.4278**	0.3567*
		(0.1704)	(0.1646)	(0.1737)	(0.1833)	(0.1677)	(0.1387)	(0.2189)	(0.1912)
GDPG	+/-	-0.2017	-0.3755	-0.3467	0.7050	0.5170	1.6310*	-9.1909	1.2565
		(0.4050)	(0.4395)	(0.4419)	(0.5833)	(1.2754)	(0.8769)	(3.7264)	(1.3118)
Number of groups		59	59	59	59	59	59	59	59
Sargant test: Chi-square		14.0420	15.0032	14.9471	11.3619	9.9707	11.4516	2.8774	10.0882
p > chi-square		0.1208	0.0908	0.0923	0.2517	0.1902	0.1201	0.8961	0.1636
AR(2): z-value		-1.0800	-1.2172	-1.1775	-1.2310	0.2608	-0.8519	1.9138	-1.1926
p > chi-square		0.2799	0.2235	0.2390	0.2183	0.7942	0.3942	0.0600	0.2330

*Note: *** p < 0.01, ** p < 0.05, * p < 0.1. Robust standard errors are in parentheses.*

Panel A of Table 4 reports that *lnAfee* is positively and significantly (Cronbach's alpha < 5%) associated with *CRD, CAUSE*, and *IMPACT* with coefficient values of 0.3352, 0.2871, and 0.4250, respectively. Meanwhile, Panel B of Table 4 shows that these three variables have a positive and significant effect on *lnAFee* with coefficient values of 0.7580, 0.0809, and 2.1729, respectively (*H1, H2b*, and *H2c* are rejected). This means there is a significant influence of total disclosure, disclosure of the causes, and the impact of cyber risk on audit fees. On the other hand, the *GCR* coefficient values for both panels are positive and insignificant (*H2a* is accepted), i.e., 0.0390 (Panel A) and 0.0809 (Panel B). Furthermore, the coefficients of the interaction variables *CRD * COVID, CAUSE * COVID*, and *IMPACT * COVID* are significantly negative (at the < 5% level), with values of -3.0570, -2.1643, and -0.9462. However, the coefficient value of *GRC * COVID* is negative and insignificant (p > 0.05).

Turning to the control variables, the regression results for Table 4 are consistent. *lnAFee* is significantly and negatively associated with capital ratio (*CAR*). On the contrary, it is significantly positively associated with bank size (*lnSIZE*) and big auditor (*BIG4*) (at < 5% level). The variables of leverage (*LEV*), efficiency ratio (*EFFIC*), net loss (*NLOSS*), and going concern opinion (*GCO*) are not significant for all the models (see Table 4). Panel A of Table 4 reports that several significant variables are *NPL*, securities investment (*SECUR*), and *BIG4*. In Panel B of Table 4, the p-values for *SECUR, GCO*, and *BIG4* are also significant at the < 5% level.

4.3. Discussion

Our outcomes, shown in Table 4, follow our predictions and support agency theory, information asymmetry theory, and risk-based approach theory. These are due to the coefficients of the main variables (*H1, H2b*, and *H2c*) and the interaction variable being consistently significant. The total *CRD, CAUSE*, and *IMPACT* have a significant effect on audit fees (at the 5% level). Conversely, the *GCR* did not affect audit fees (p > 0.05). In accordance with the risk-based perspective, the auditor responds to the risks disclosed by the client through appropriate adjustments to the audit procedures. Auditors perceiving higher client risk will increase their audit effort, thereby determining higher fees.

Inconsistent with agency theory, the authors found that cyber risk governance did not affect the audit rate. It means that government agencies do not require additional assurance from auditors and are closely scrutinized by regulators. It also implies that auditors reduce their efforts; thus, good risk governance does not affect audit fees. Consistent with previous studies, we suggest two reasons. First, tight supervision by financial regulators (external governance) can partially substitute bank risk governance (internal governance). Strict regulatory oversight reduces audit risk and information asymmetry, potentially reducing the important role of corporate governance players such as the risk committee (Bryan & Klein, 2004; Boo & Sharma, 2008). Second, the board's primary responsibility for monitoring risk management may not be sufficient, in particular, to improve the monitoring of cyber risk (Shakhatreh & Alsmadi, 2021). Otherwise, Qawqzeh et al. (2021) and Al Sharawi (2022) stated that board members play an important role in external audits' high quality and fee levels. Finally, we conducted additional testing to determine whether the absence of this relationship will be different if it is associated with lag or lead effects (see additional tests). According to Simunic (1980), auditors can set the price of audit services based partly on previous audit fees and current information on relevant factors.

Table 4 also reports that *lnAFee* was significantly affected by the interaction between the main variable and COVID-19 as a dummy variable (p > 0.05). Even though the relatively short period of the COVID-19 pandemic has been the representation of numerical data that can be tested, the pandemic has lowered audit fees for companies that disclose the total, causes, and impacts of cyber risk. In line with the results of previous studies, firms negotiate lower prices for audit services during the pandemic (Albitar et al., 2021; International Federation of Accountants [IFAC], 2020). Auditors can reduce their efforts to minimize engagement losses during the COVID-19 social distancing outbreak. Disclosure of cyber risk may have greater complexity and audit effort. Still, prudence and minimizing losses on the engagement make it difficult to perform the engagement under the technical and professional standards applicable to that price. In addition, lower audit operational costs (e.g., personnel salary and utility costs) reduce audit fee offerings. The study conducted by Al-Qadasi et al. (2022) and Harjoto and Laksmana (2022) found the opposite result. It is stated that public health restrictions during COVID-19 led to higher audit costs due to perceived audit risk and additional audit efforts to design new procedures. In addition, the threat of risk, complexity, and legal liability due to the pandemic can be compensated by charging higher audit fees.

Our regression results show those audit fees are significantly related to bank size, *NPL*, auditor size (*BIG4*), and going concern opinion. Audit fees are positively influenced by the firm and auditor size. Audit fees are higher for large banks due to greater audit complexity (Fields et al., 2004) and agency fees (Lyubimov, 2019). Banks audited by big auditors (*BIG4*) are charged higher fees due to premium audit services (Francis, 2004) as well as a higher reputation and audit market (Lyubimov, 2019).

According to Boo and Sharma (2008), banks that receive a going concern opinion (*GCO*) will pay higher fees to demonstrate a high-quality audit. Credit quality is the most widely owned asset by banks. The high level of non-performing loans owned by banks requires greater audit efforts and fees because the risk of default is higher than current loans. Conversely, banks need to maintain adequate capital levels (*CAR*) to fund their investments, fulfill depositor and lender obligations, and meet regulatory requirements set by regulators. A low capital ratio increases auditor effort, resulting in greater audit costs. However, proxies for clients' ability to pay (*NLOSS*), bank leverage (*LEV*), bank efficiency, and *GDPG* are insignificant.

4.4. Additional test

Additional tests were performed to provide some additional evidence regarding our results. Firstly, we re-estimated all equations with lagged variables because of the lack of a dominant significant result for the cyber risk governance variable. Previous studies were proven to support the idea that audit fees are related to current and past events (Hribar et al., 2014), the potential lag or lead effects of cyber-security incidents (Rosati et al., 2019), and prior cybersecurity risks disclosure (Calderon & Gao, 2021). Table 5 shows that *lnAFee* was significantly affected by *GCR* lag and significantly negative *GCR * COVID* interactions. This means that the governance of the bank's CRD in the previous period increased the current audit fees. This audit fee was lower during the pandemic than during the non-pandemic period. We suggest that the governance of the bank's CRD requires additional assurance from the auditor based on a demand-based perspective. Hay et al. (2004) argue that the demand effect may cause risk committees to demand more audits to fulfill their responsibilities and protect their reputations against the dubious cyber risk reported by management.

Finally, we replaced audit fees with audit tenure. Although audit tenure and fees are related to audit quality, they measure different aspects of the audit process. Audit tenure indicates the length of working relationships between companies or issuers that use audit services at the same public accountant within a certain period of time. The longer audit engagement gives the auditor a deeper understanding of the company's operations, business risks, and systems, resulting in a more efficient audit process (Lee et al., 2009). Previous research also shows that informed company risk is very likely to be a factor in changing auditors (Nasser et al., 2006; Junaidi et al., 2016).

Different from the results of previous studies, our study found that total and individual CRDs (risk governance, causes, and impacts) did not affect audit tenure, as indicated in Table 6. During the COVID-19 pandemic, we failed to prove the effectiveness of this relationship. These findings are in-line study against auditor turnover which states that companies at high risk, as indicated by the information submitted, want to be audited by the same auditor because incumbent auditors have a better understanding of the company's condition (Sinason et al., 2009; Fairchild, 2008; Hategan et al., 2022).

Table 5. Result of Models 1, 2, 3, and 4 (Lagged-GMM model)

Variables	***Predicted sign***	***Panel A***				***Panel B***			
		CRD	***GCR***	***CAUSE***	***IMPACT***	***CRD***	***GCR***	***CAUSE***	***IMPACT***
		(SE)	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***
L.lnAFee	+	0.6016***	0.5814***	0.5831***	0.7401***	0.2127	0.3548	0.1225	0.5701**
		(0.1250)	(0.1493)	(0.1350)	(0.1804)	(0.1858)	(0.2416)	(0.2425)	(0.1595)
L.CRD	+	0.2400				1.4127***			
		(0.1498)				(0.5078)			
L.GCR	-		0.2212***				0.3014***		
			(0.0680)				(0.0932)		
L.CAUSE	+			-0.4969				2.7808***	
				(0.4616)				(0.9079)	
L.IMPACT	+				0.4250***				-0.2825
					(0.1751)				(0.1753)
L.COVID	+					0.6681***	0.6245***	0.3051*	0.0794
						(0.1817)	(0.1852)	(0.1714)	(0.1387)
*L.CRD * COVID*	+					-2.0513***			
						(0.6022)			
*L.GCR * COVID*	+						-0.6717**		
							(0.2736)		
*L.CAUSE * COVID*	+							-4.8697***	
								(1.4375)	
*L.IMPACT * COVID*	+								0.2190
									(0.1420)
lnSIZE	+	0.2956***	0.2601***	0.4186***	0.3598***	0.1495	0.2969***	0.0309	0.4649***
		(0.0745)	(0.0700)	(0.1120)	(0.0775)	(0.1342)	(0.1048)	(0.1906)	(0.0850)
LEV	+	-0.2699	-0.3056	-1.0645	-0.3989	0.8385	-0.1644	2.2013	-0.5893
		(0.5001)	(0.3827)	(0.6262)	(0.5254)	(0.6708)	(0.4080)	(1.2018)	(0.5670)
NPL	+	0.4829	0.1946	0.2751	0.0517	1.4870	0.7346	1.9610	0.2510
		(0.7583)	(0.7923)	(0.7273)	(0.9149)	(1.0211)	(0.9076)	(1.2007)	(0.7102)
EFFIC	-	-0.0035	-0.0052	-0.0074	-0.0065	-0.0011	-0.0046**	0.0085	-0.0052
		(0.0026)	(0.0037)	(0.0036)	(0.0036)	(0.0030)	(0.0038)	(0.0057)	(0.0026)
SECUR	-	-0.0001	-0.0007	-0.0004	-0.0001***	-0.0006	-0.0007	0.0006	-0.0008**
		(0.0004)	(0.0004)	(0.0004)	(0.0004)	(0.0004)	(0.0004)	(0.0008)	(0.0004)
CAR	-	-0.4445	-0.4624	-0.9375**	-0.4749*	-2.2999	-0.6975**	0.1802	-0.7062**
		(0.3210)	(0.2731)	(0.4730)	(0.3104)	(0.4429)	(0.3102)	(0.7414)	(0.3283)
NLOSS	+	0.1969	0.1990	0.1621	0.1598	0.1313	1.1849	0.0172	0.1489
		(0.1325)	(0.1462)	(0.1413)	(0.1532)	(0.0955)	(0.1122)	(0.1137)	(0.1098)
GCO	+	0.1013	0.0728	0.1178	0.2034	0.3931**	0.3036**	0.1297	0.1605
		(0.1333)	(0.1532)	(0.1608)	(0.1233)	(0.1598)	(0.1485)	(0.2013)	(0.1277)
BIG4	+	0.2812*	0.2587	0.2769	0.4098**	0.3457**	0.3815**	0.3321*	0.3191*
		(0.1699)	(0.1731)	(0.1833)	(0.1757)	(0.1638)	(0.1363)	(0.1830)	(0.1690)
GDPG	+/-	-0.1574	-0.1559	-0.5081	0.9465	1.0323	1.6317**	-2.1786	0.8914
		(0.3777)	(0.4197)	(0.5741)	(0.6624)	(1.2401)	(0.8309)	(2.1447)	(0.9052)
Number of groups		59	59	59	59	59	59	59	59
Sargant test: Chi-square		14.5034	13.2315	15.5778	10.5431	7.7138	7.3319	4.9558	13.2755
p > chi-square		0.1055	0.1524	0.0762	0.3083	0.3584	0.3951	0.7622	0.2086
AR(2): z-value		-1.3426	-1.5587	-1.2229	-1.2866	-1.8117	-0.8519	-1.2994	-1.3391
p > chi-square		0.1794	0.1191	0.2214	0.1982	0.1070	0.3942	0.1938	0.1805

*Note: *** p < 0.01, ** p < 0.05, * p < 0.1. Robust standard errors are in parentheses.*

Table 6. Result of Models 1, 2, 3, and 4 (Audit tenure as the dependent variable — GMM model) (Part 1)

Variables	***Predicted sign***	***Panel A***				***Panel B***			
		CRD	***GCR***	***CAUSE***	***IMPACT***	***CRD***	***GCR***	***CAUSE***	***IMPACT***
		(SE)	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***	***(SE)***
L.lnAFee	+	0.9789***	1.0078***	0.9737***	1.0254***	1.0656***	1.0979***	1.0242***	1.0065***
		(0.0893)	(0.0834)	(0.0876)	(0.0847)	(0.0808)	(0.780)	(0.1521)	(0..1628)
CRD	+	1.1278				0.8541			
		(0.7458)				(0.8558)			
GCR	-		0.1624				-0.1098		
			(0.0300)				(0.3591)		
CAUSE	+			1.2611				1.1235	
				(0.6098)				(0.6939)	
IMPACT	+				-0.11996				-0.9801
					(0.5061)				(2.6612)
COVID	+					0.3009	0.1957	0.1699	-0.3047
						(0.5736)	(0.3592)	(0.9183)	(1.5356)
*CRD * COVID*	+					0.9536			
						(1.3058)			
*GCR * COVID*	+						0.6842		
							(0.6344)		

Table 6. Result of Models 1, 2, 3, and 4 (Audit tenure as the dependent variable — GMM model) (Part 2)

Variables	*Predicted sign*	*Panel A*				*Panel B*			
		CRD	*GCR*	*CAUSE*	*IMPACT*	*CRD*	*GCR*	*CAUSE*	*IMPACT*
		(SE)	*(SE)*	*(SE)*	*(SE)*	*(SE)*	*(SE)*	*(SE)*	*(SE)*
*CAUSE * COVID*	+							0.5290	
								(4.0856)	
*IMPACT * COVID*	+								1.5472
									(3.7365)
lnSIZE	+	-0.5119	-0.3819	-0.4667	-0.1996	-0.8564	-0.7626	-0.7095	-0.4040
		(0.6456)	(0.6274)	(0.6383)	(0.5061)	(0.7555)	(0.7489)	(0.8259)	(0.8844)
LEV	+	-0.8877	-0.6302	-0.9008	-0.3416	-1.0065	-1.1392	-1.3436	-1.0063
		(1.6825)	(1.7164)	(1.6536)	(0.6318)	(2.1157)	(2.1825)	(1.9420)	(1.9584)
NPL	+	-8.8749	-7.6192	-7.7855	-0.6587	-9.7864*	-8.0702	-7.6506	-6.4571
		(5.5789)	(5.6272)	(5.5353)	(1.7248)	(5.5738)	(5.4083)	(5.9018)	(6.0481)
EFFIC	-	-0.0125*	-0.0089	-0.0112*	-7.6743	-0.0180**	-0.0144**	-0.0153	-0.0132
		(0.0067)	(0.0039)	(0.0060)	(5.5428)	(0.0075)	(0.0038)	(0.0105)	(0.0107)
SECUR	-	0.0004	0.0006	-0.0005	-0.0075	0.0007*	0.0068*	0.0007*	0.0007
		(0.0004)	(0.0004)	(0.0004)	(0.0066)	(0.0004)	(0.0004)	(0.0003)	(0.0004)
CAR	-	-4.1148*	-3.9049*	-4.4676*	-3.7923*	-3.6607	-3.4359	-3.8701	-3.9168
		(2.2764)	(2.2468)	(2.3766)	(2.2780)	(2.2954)	(2.2880)	(2.3908)	(2.4105)
NLOSS	+	0.3913	0.248	0.4705	0.2210	0.2444	0.1372	0.2469	0.1159
		(0.4384)	(0.4580)	(0.4511)	(0.4585)	(0.4430)	(0.4554)	(0.4542)	(0.5589)
GCO	+	-1.2553*	-1.0888	1.5665	-1.1842	-1.2354*	-1.2469	-1.6508**	-1.3863*
		(0.6742)	(0.6956)	(0.6701)	(0.6643)	(0.7479)	(0.7745)	(0.8041)	(0.7821)
BIG4	+	-0.0408	-0.2324	-0.0617	-0.3589	0.4644	0.1284	0.3321	0.1241
		(1.5139)	(1.5927)	(1.4453)	(1.6041)	(1.5665)	(1.5822)	(1.5529)	(1.7289)
GDPG	+/-	-2.1241*	-1.8685	-2.8588	-2.1145	3.2394	3.6224	-0.7884	-3.294
		(1.2402)	(1.2345)	(1.3699)	(1.5963)	(3.0006)	(3.1072)	(9.5257)	(10.8542)
Number of groups		68	68	68	68	68	68	68	68
Sargant test: Chi-square		9.3239	10.0658	9.6090	9.7525	8.3136	8.1163	6.7842	5.9905
p > chi-square		0.4079	0.3451	03830	0.3708	0.5028	0.5224	0.4516	0.5408
AR(2): z-value		0.6333	0.8616	0.4120	0.8697	0.6041	0.8093	0.4100	0.7922
p > chi-square		0.5265	0.3889	0.6803	0.3844	0.5457	0.4183	0.6817	0.4282

*Note: *** p < 0.01, ** p < 0.05, * p < 0.1. Robust standard errors are in parentheses.*

5. CONCLUSION

This study investigates whether companies with cyber risk disclosure are charged higher audit fees. The study also examines whether the COVID-19 pandemic affected the association between cyber risk disclosure with audit fees. Cyber risk disclosure is proxied by total cyber risk disclosure, cyber risk governance, cyber risk causes, and cyber risk impacts. The results show that disclosure of total, causes, and impacts of cyber risk was significantly and positively associated with audit fees. In contrast, the governance of cyber risk disclosure affected audit fees after the lagged variable. This means that this type of disclosure affects audit fees in the following year. Further analysis shows that this audit fee was decreased during the COVID-19 pandemic. The results of another additional analysis examining the effects of cyber risk disclosure on audit tenure cannot be proved.

Some limitations in this study must be overcome in future research. First, we focused on the role of boards in cyber risk management and oversight as representatives of cyber risk governance. This proxy is considered less comprehensive because it focuses too much on several aspects that can increase the potential for bias (Pan, 2008). Second, using content analysis to explain cyber risk disclosure may not be comprehensive or sufficient. Experimental or interview-based studies may better explain

REFERENCES

1. A.T. Kearney. (2018). *Cybersecurity in ASEAN: An urgent call to action.* https://www.southeast-asia.kearney.com/documents/1781738/1782318/Cybersecurity+in+ASEAN%E2%80%94An+Urgent+Call+to+Action.pdf/80a880c4-8b70-3c99-335f-c57e6ded5d34
2. Aebi, V., Sabato, G., & Schmid, M. (2012). Risk management, corporate governance, and bank performance in the financial crisis. *Journal of Banking & Finance, 36*(12), 3213–3226. https://doi.org/10.1016/j.jbankfin.2011.10.020
3. Al Sharawi, H. H. M. (2022). The impact of ownership structure on external audit quality: A comparative study between Egypt and Saudi Arabia. *Investment Management and Financial Innovations*, *19*(2), 81–94. http://doi.org/10.21511/imfi.19(2).2022.07
4. Albitar, K., Gerged, A. M., Kikhia, H., & Hussainey, K. (2021). Auditing in times of social distancing: The effect of COVID-19 on auditing quality. *International Journal of Accounting & Information Management, 29*(1), 169–178. https://doi.org/10.1108/IJAIM-08-2020-0128
5. Aldasoro, I., Frost, J., Gambacorta, L., & Whyte, D. (2021). COVID-19 and cyber risk in the financial sector. *BIS Bulletin, 37*. https://www.bis.org/publ/bisbull37.htm
6. Aldasoro, I., Gambacorta, L., Giudici, P., & Leach, T. (2020). *Operational and cyber risks in the financial sector* (BIS Working Papers No. 840). Bank of International Settlements (BIS). https://www.bis.org/publ/work840.pdf
7. Al-Qadasi, A., Baatwah, S. R., & Omer, W. K. (2022). Audit fees under the COVID-19 pandemic: Evidence from Oman. *Journal of Accounting in Emerging Economies, 13*(4), 806–824. https://doi.org/10.1108/JAEE-08-2021-0269
8. Bell, T. B., Landsman, W. R., & Shackelford, D. A. (2001). Auditors' perceived business risk and audit fees: Analysis and evidence. *Journal of Accounting Research*, *39*(1), 35–43. https://doi.org/10.1111/1475-679X.00002

9. Bhuiyan, M. B. U., Cheema, M. A., & Man, Y. (2021). Risk committee, corporate risk-taking and firm value. *Managerial Finance*, *47*(3), 285–309. https://doi.org/10.1108/MF-07-2019-0322
10. Board of Commissioners of the Financial Services Authority. (2020). *Perubahan atas Peraturan Otoritas Jasa Keuangan No. 38/POJK.03/2016 tentang penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum* [Amendment of Financial Services Authority Regulation No. 38/POJK.03/2016 concerning the application of risk management in the use of information technology by commercial banks]. https://www.ojk.go.id/id/regulasi/Documents/Pages/tentang-Penerapan-Manajemen-Risiko-dalam-Penggunaan-Teknologi-Informasi-oleh-Bank-Umum/pojk%2013-2020.pdf
11. Boo, E., & Sharma, D. (2008). The association between corporate governance and audit fees of bank holding companies. *Corporate Governance*, *8*(1), 28–45. https://doi.org/10.1108/14720700810853383
12. Bryan, S., & Klein, A. (2004). *Non-management director options, board characteristics, and future firm investments and performance* (Working Paper No. 04-009). New York University. http://doi.org/10.2139/ssrn.550506
13. Calderon, T. G., & Gao, L. (2021). Cybersecurity risks disclosure and implied audit risks: Evidence from audit fees. *International Journal of Audit*, *25*, 24–39. https://doi.org/10.1111/ijau.12209
14. Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). *A taxonomy of operational cyber security risks: Version 2* (Technical Note No. CMU/SEI-2010-TN-028). Software Engineering Institute. https://resources.sei.cmu.edu/asset_files/technicalnote/2014_004_001_91026.pdf
15. Center for Audit Quality (CAQ). (2014). *CAQ member alert: Cybersecurity and the external audit.* https://thecaqprod.wpenginepowered.com/wp-content/uploads/2019/03/caqalert_2014_03.pdf
16. Cheong, A., Yoon, K., Cho, S., & Gyun, N. W. (2021). Classifying the contents of cybersecurity risk disclosure through textual analysis and factor analysis. *Journal of Information Systems*, *35*(2), 179–194. https://doi.org/10.2308/ISYS-2020-031
17. Clark, L. A., & Watson, D. (1995). Constructing validity: Basic issues in objective scale development. *Psychological Assessment*, *7*(3), 309–319. https://doi.org/10.1037/1040-3590.7.3.309
18. Duvenhage, F. J. (2020). *A comparison of cyber risk disclosure in the banking sector between South Africa and China* [Master's project, North-West University]. https://repository.nwu.ac.za/bitstream/handle/10394/36655/Duvenhage_FJ.pdf?sequence=1
19. Fairchild, R. (2008). Auditor tenure, managerial fraud, and report qualification: A game theoretic approach. *ICFAI Journal of Audit Practice*, *5*(2), 42–54.
20. Favere-Marchesi, M. (2000). Audit quality in ASEAN. *The International Journal of Accounting*, *35*(1), 121–149. https://doi.org/10.1016/S0020-7063(99)00049-7
21. Fields, L. P., Fraser, D. R., & Wilkins, M. S. (2004). An investigation of the pricing of audit services for financial institutions. *Journal of Accounting and Public Policy, 23*(1), 53–77. https://doi.org/10.1016/j.jaccpubpol.2003.11.003
22. Financial Services Authority (OJK). (2017). *Surat Edaran Otoritas Jasa Keuangan No. 21/SEOJK.03/2017* [Circular letter of the Financial Services Authority No. 21/SEOJK.03/2017]. https://ojk.go.id/id/kanal/perbankan/regulasi/surat-edaran-ojk/Pages/Surat-Edaran-Otoritas-Jasa-Keuangan-Nomor-21-SEOJK.03-2017.aspx
23. Fitch Ratings. (2020). *Digital banks in South-East Asia.* https://www.fitchratings.com/research/banks/digital-banks-in-south-east-asia-19-08-2020
24. Francis, J. R. (2004). What do we know about audit quality? *The British Accounting Review*, *36*(4), 345–368. https://doi.org/10.1016/j.bar.2004.09.003
25. Gensler, G. (2022, March 9). *Statement on proposal for mandatory cybersecurity disclosures.* Securities and Exchange Commission. https://www.sec.gov/news/statement/gensler-cybersecurity-20220309
26. Gensler, G. (2022, March 9). *Statement on proposal for mandatory cybersecurity disclosures.* Securities and Exchange Commission (SEC). https://www.sec.gov/news/statement/gensler-cybersecurity-20220309
27. Harjoto, M. A., & Laksmana, I. (2022). The impact of COVID-19 lockdown on audit fees and audit delay: International evidence. *International Journal of Accounting & Information Management*, *30*(4), 526–545. https://doi.org/10.1108/IJAIM-02-2022-0030
28. Hategan, C.-D., Pitorac, R.-I., & Crucean, A. C. (2022). Impact of COVID-19 pandemic on auditors' responsibility: Evidence from European listed companies on key audit matters. *Managerial Auditing Journal*, *37*(7), 886–907. https://doi.org/10.1108/MAJ-07-2021-3261
29. Hay, D., Knechel, W. R., & Wong, N. (2004). *Audit fees: A meta-analysis of the effect of supply and demand attributes.* http://doi.org/10.2139/ssrn.512642
30. Hedrich, W., Wong, G., & Yeo, J. (2017). *Cyber risk in Asia Pacific: The case for greater transparency.* Marsh & McLennan Companies. https://www.marsh.com/content/dam/marsh/Documents/PDF/asia/en_asia/Cyber%20Risk%20in%20Asia%20Pacific%20-%20The%20Case%20for%20Greater%20Transparency.pdf
31. Hilary, G., Segal, B., & Zhang, M. H. (2016). *Cyber-risk disclosure: Who cares?* (Research Paper No. 2852519). Georgetown University. http://doi.org/10.2139/ssrn.2852519
32. Hribar, P., Kravet, T., & Wilson, R. (2014). A new measure of accounting quality. *Review of Accounting Studies*, *9*(1), 506–538. https://doi.org/10.1007/s11142-013-9253-8
33. Institute of Singapore Chartered Accountants (ISCA). (2018). *Cybersecurity risk considerations in a financial statements audit.* https://isca.org.sg/media/2240014/isca-cyber-security-risk-report.pdf
34. International Federation of Accountants (IFAC). (2020). *Summary of COVID-19 audit consideration.* https://www.ifac.org/knowledge-gateway/supporting-international-standards/discussion/summary-covid-19-audit-considerations
35. Junaidi, Khasanah, N. N., & Nurdiono. (2016). The effects of company size, company risk and auditor's reputation on tenure: An artificial rotation testing. *Journal of Indonesian Economy and Business, 31*(3), 247–259. https://doi.org/10.22146/jieb.23269
36. Karyani, E., Dewo, S. A., Santoso, W., & Frensidy, B. (2020). Risk governance and bank profitability in ASEAN-5: A comparative and empirical study. *International Journal of Emerging Markets*, *15*(5), 949–969. https://doi.org/10.1108/IJOEM-03-2018-0132
37. Khalil, S., Magnan, M. L., & Cohen, J. R. (2008). Dual-class shares and audit pricing: Evidence from the Canadian markets. *AUDITING: A Journal of Practice & Theory*, *27*(2), 199–216. https://doi.org/10.2308/aud.2008.27.2.199

38. Kopp, E., Kaffenberger, L., & Wilson, C. (2017). *Cyber risk, market failures, and financial stability* (IMF Working Paper No. WP/17/185). International Monetary Fund. https://doi.org/10.5089/9781484313787.001
39. Krishnan, G. V., & Zhang, Y. (2014). Is there a relation between audit fee cuts during the global financial crisis and banks' financial reporting quality? *Journal of Accounting and Public Policy, 33*(3), 279–300. https://doi.org/10.1016/j.jaccpubpol.2014.02.004
40. Krishnan, G. V., Pevzner, M., & Sengupta, P. (2012). How do auditors view managers' voluntary disclosure strategy? The effect of earnings guidance on audit fees. *Journal of Accounting and Public Policy*, *31*(5), 492–515. https://doi.org/10.1016/j.jaccpubpol.2011.10.009
41. Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? *AUDITING: A Journal of Practice & Theory*, *37*(1), 139–165. https://doi.org/10.2308/ajpt-51784
42. Lee, H.-Y., Mande, V., & Son, M. (2009). Do lengthy auditor tenure and the provision of non-audit services by the external auditor reduce audit report lags? *International Journal of Auditing*, *13*(2), 87–104. https://doi.org/10.1111/j.1099-1123.2008.00406.x
43. Leventis, S., & Dimitropoulos, P. E. (2010). Audit pricing, quality of earnings and board independence: The case of the Athens stock exchange. *Advances in Accounting*, *26*(2), 325–332. https://doi.org/10.1016/j.adiac.2010.08.002
44. Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *AUDITING: A Journal of Practice & Theory*, *39*(1), 151–171. https://doi.org/10.2308/ajpt-52593
45. Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40–55. https://doi.org/10.1016/j.accinf.2018.06.003
46. Lyubimov, A. (2019). How do audit fees change? Effects of firm size and section 404(b) compliance. *Managerial Auditing Journal, 34*(4), 393–433. https://doi.org/10.1108/MAJ-07-2018-1938
47. Masoud, N., & Al-Utaibi, G. (2022). The determinants of cybersecurity risk disclosure in firms' financial reporting: Empirical evidence. *Research in Economics*, *76*(2), 131–140. https://doi.org/10.1016/j.rie.2022.07.001
48. Moreira, G. P. (2019). *Cybersecurity and external audit: The disclosure of risk factors in annual reports*. Católica Porto Business School. https://core.ac.uk/download/pdf/237231002.pdf
49. Musa, W. A., Salman, R. T., & Amoo, I. O. (2021). Determinants of audit fees in quoted financial and nonfinancial firms. *Corporate Law & Governance Review*, *3*(2), 30–40. https://doi.org/10.22495/clgrv3i2p3
50. Nasser, A. T. A., Wahid, E. A., Nazri, S. N. F. S. M., & Hudaib, M. (2006). Auditor-client relationship: The case of audit tenure and auditor switching in Malaysia. *Managerial Auditing Journal*, *21*(7), 724–737. https://doi.org/10.1108/02686900610680512
51. Nelson, S. P., & Mohamed-Rusdi, N. F. (2015). Ownership structures influence on audit fee. *Journal of Accounting in Emerging Economies, 5*(4), 457–478. https://doi.org/10.1108/JAEE-05-2013-0027
52. Pan, K. Q. (2008). Corporate governance, audit risk and audit pricing: empirical evidence based on CCGINK. *Nankai Business Review*, *1*, 106–112. https://caod.oriprobe.com/articles/13504368/Corporate_Governance__Audit_Risk_and_Audit_Pricing.htm
53. Personal Data Protection Act B.E. 2562 (2019). https://thainetizen.org/wp-content/uploads/2019/11/thailand-personal-data-protection-act-2019-en.pdf
54. Public Company Accounting Oversight Board (PCAOB). (2014). *Cybersecurity: Standing advisory group meeting.* https://pcaobus.org/News/Events/Documents/0624252014_SAG_Meeting/06252014_Cybersecurity.pdf
55. Qawqzeh, H. K., Bshayreh, M. M., & Alharbi, A. W. (2021). Does ownership structure affect audit quality in countries characterized by weak legal protection of the shareholders*? Journal of Financial Reporting and Accounting*, *19*(5), 707–724. https://doi.org/10.1108/JFRA-08-2020-0226
56. Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: Evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, *54*(3), Article 1950013. https://doi.org/10.1142/S1094406019500136
57. Rosnidah, I., Johari, R. J., Mohd Hairudin, N. A., Hussin, S. A. H. S., & Musyaffi, A. M. (2022). Detecting and preventing fraud with big data analytics: Auditing perspective. *Journal of Governance & Regulation, 11*(4), 8–15. https://doi.org/10.22495/jgrv11i4art1
58. Rusmanto, T., & Waworuntu, S. R. (2015). Factors influencing audit fee in Indonesian publicly listed companies applying GCG. *Procedia — Social and Behavioral Sciences*, *172*, 63–67. https://doi.org/10.1016/j.sbspro.2015.01.336
59. Securities and Exchange Commission (SEC) Philippines. (2020). *Request for comments on "Guidance for regulated entities on establishing and maintaining a cybersecurity framework"*. https://www.sec.gov.ph/notices/request-for-comments-on-guidance-for-regulated-entities-on-establishing-and-maintaining-a-cybersecurity-framework/
60. Securities and Exchange Commission (SEC). (2011, October 13). *CF disclosure guidance: Topic No. 2.* https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
61. Securities Commission (SC) Malaysia. (2016). *Guidelines on management of cyber risk (SC-GL/2-2016).* https://www.sc.com.my/api/documentms/download.ashx?id=9aaddb2e-aa13-409a-a47f-8d0124afd229
62. Shakhatreh, M. Z., & Alsmadi, S. A. (2021). Determinants of audit fees and the role of the board of directors and ownership structure: Evidence from Jordan. *Journal of Asian Finance, Economics and Business*, *8*(5), 627–637. https://www.researchgate.net/publication/351391240_Determinants_of_Audit_Fees_and_the_Role_of_the_Board_of_Directors_and_Ownership_Structure_Evidence_from_Jordan
63. Shu, S. Z. (2000). Auditor resignations: Clientele effects and legal liability. *Journal of Accounting and Economics*, *29*(2), 173–205. https://doi.org/10.1016/S0165-4101(00)00019-7
64. Simunic, D. A. (1980). The pricing of audit services: Theory and evidence. *Journal of Accounting Research, 18*(1), 161–190. https://doi.org/10.2307/2490397
65. Sinason, D. H., Jones, J. P., & Waller Shelton, S. (2009). An investigation of auditor and client tenure. *American Journal of Business, 16*(2), 31–40. https://doi.org/10.1108/19355181200100010
66. Smith, T. J., Higgs, J. L., & Pinsker, R. E. (2019). Do auditors price breach risk in their audit fees? *Journal of Information Systems, 33*(2), 177–204. https://doi.org/10.2308/isys-52241
67. Uddin, M. H., Ali, M. H., & Hassan, M. K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, *22*(4), 239–309. https://doi.org/10.1057/s41283-020-00063-2

68. Van, H. N., Thanh, H. P., Thanh, C. N., Ngoc, D. N., & Hai, G. H. (2022). Study on factors affecting audit fees and audit quality through auditors' perceptions: Evidence from an emerging economy. *Problems and Perspectives in Management*, *20*(2), 471–485. http://doi.org/10.21511/ppm.20(2).2022.39
69. World Bank. (n.d.). *Indicators*. https://data.worldbank.org/indicator
70. Wu, X. (2012). Corporate governance and audit fees: Evidence from companies listed on the Shanghai Stock Exchange. *China Journal of Accounting Research, 5*(4), 321–342. https://doi.org/10.1016/j.cjar.2012.10.001
71. Yang, H. (2015). Corporate governance, political connection and audit fees: Empirical evidence from listed companies in China's A-share chemical industry from 2011 to 2013. *Public Finance Research*, *8*, 107–112.
72. Yang, R., Yu, Y., Liu, M., & Wu, K. (2018). Corporate risk disclosure and audit fee: A text mining approach. *European Accounting Review*, *27*(3), 583–594. https://doi.org/10.1080/09638180.2017.1329660
73. Ye, X. (2020). Literature review on influencing factors of audit fees. *Modern Economy, 11*(2), 249–260. https://doi.org/10.4236/me.2020.112022

APPENDIX

Table A.1. Correlation matrix

Variables	***lnAFee***	***CRD***	***GCR***	***CAUSE***	***IMPACT***	***COVID***	***lnSIZE***	***LEV***	***NPL***	***EFFI***	***SECUR***	***CAR***	***NLOSS***	***GCO***	***BIG4***
CRD	0.343***	1													
GCR	0.386***	0.864***	1												
CAUSE	0.216***	0.757***	0.389***	1											
IMPACT	-0.063	0.292***	0.135**	-0.007	1										
COVID	0.022	0.279***	0.170***	0.068	0.650***	1									
lnSIZE	0.770***	0.334***	0.391***	0.209***	-0.099*	0.001	1								
LEV	0.066	-0.031	-0.001	-0.045	-0.039	-0.028	0.203***	1							
NPL	-0.242***	-0.168***	-0.246***	-0.081	0.122**	0.160***	-0.294***	0.041	1						
EFF	-0.075	0.054	0.031	-0.009	0.184***	0.062	-0.175***	-0.341***	-0.013	1					
SECUR	0.224***	-0.036	0.010	-0.063	-0.051	-0.036	0.437***	0.512***	-0.061	-0.333***	1				
CAR	-0.213***	-0.079	-0.109**	-0.096*	-0.169***	0.170***	-0.305***	-0.169***	0.236***	0.008	0.061	1			
NLOSS	-0.230***	-0.197***	-0.254***	-0.099*	0.077	0.054	-0.380***	0.061	0.411***	-0.038	-0.163***	0.003	1		
GCO	-0.148***	-0.109**	-0.127**	-0.066	0.029	0.048	-0.243***	0.046	0.269***	-0.022	-0.216***	0.001	0.457***		
BIG4	0.433***	0.168***	0.195***	0.115**	-0.058	-0.065	0.400***	-0.080	-0.361***	0.2655*	0.259***	-0.184***	-0.341***	-9.355***	1
GDPG	-0.102*	-0.271***	-0.187***	-0.083	-0.521**	-0.909***	-0.079	0.092*	-0.166***	-0.116**	0.041	-0.106**	0.012	-0.005	-0.008

*Note: *** $p < 0.01$, ** $p < 0.05$, * $p < 0.1$.*