# BANKS AND ESG PILLARS SCORE: DOES CYBERSECURITY POLICY MATTER?

Elena Bruno [*], Giuseppina Iacoviello [**], Raffaele Casella [*]

* Department of Economics and Management, University of Pisa, Pisa, Italy
** *Corresponding author*, Department of Economics and Management, University of Pisa, Pisa, Italy
Contact details: Department of Economics and Management, University of Pisa, Via Cosimo Ridolfi, 10, 56124 Pisa, Italy

**How to cite this paper:** Bruno, E., Iacoviello, G., & Casella, R. (2024). Banks and ESG pillars score: Does cybersecurity policy matter? [Special issue]. *Corporate Ownership & Control, 21*(3), 8–17. https://doi.org/10.22495/cocv21i3siart1



**ISSN Online:** 1810-3057
**ISSN Print:** 1727-9232

**Received:** 24.05.2024
**Accepted:** 22.08.2024

**JEL Classification:** G2, M1
**DOI:** 10.22495/cocv21i3siart1

## Abstract

This paper investigates the relationship between cybersecurity policy and the environmental, social, and governance (ESG) pillar scores in banks, considering the geographical area (European and non-European), the size (total assets), and the profitability (pre-tax return on assets) from 2017 to 2022 by incorporating and building on previous studies. The results show that the data are both significant and non-significant in terms of using a one-way ANOVA approach. Specifically, a significant relationship was found between cyber policy and the governance (*GOV*) and social (*SOC*) component indicators, except for major banks. The cyber policy may be responsible for an increase in the environmental (*ENV*) pillar scores in the European subsample.

**Keywords:** Banks, Cybersecurity Policy, ESG, ANOVA

**Authors' individual contribution:** Conceptualization — G.I.; Methodology — R.C.; Investigation — G.I. and R.C.; Writing — Original Draft — E.B. and R.C.; Writing — Review & Editing — E.B.; Supervision — E.B. and G.I.

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

## 1. INTRODUCTION

Banks have to utilize their tremendous profitability resources to support the structural modernization of their services industry through new, revolutionary innovation efforts to support their country's growth (Ooi et al., 2023; Madanchian, 2024). Due to new regulatory difficulties and increasing risks in areas such as artificial intelligence (Jin et al., 2023), cyber risks (Omarini, 2023), and ESG (Shackelford, 2023), these challenges highlight the difficult balancing act between innovative and legacy banking models. As a result, banks will be more susceptible to cyberattacks, and security lapses will increase their endogenous fragility (Porcellacchia & Sheedy, 2023). According to Smaili et al. (2023) and the Securities and Exchange Commission (SEC, 2023), improving the disclosure of cybersecurity risks is one approach to ethical decision-making. Thus, the research question can be formulated as follows:

*RQ: Can the environmental, social, and governance (ESG) pillar scores be affected by cybersecurity policy?*

This study examines the relationship between cybersecurity policy (for countries with a cyber policy) and the ESG pillars score in the Group of Ten (G10) and EU banks.

The study examines a sample of banks (commercial banks, investment banks, and financial services) operating in G10 countries (initially in Basel) and the European Union (EU).

To the best of our knowledge, this is the first study to investigate the possible impact of a cybersecurity policy on the ESG pillars score.

Therefore, we created the subgroup total assets and pre-tax return on assets (ROA) ratio, in a one-way analysis-of-variance (ANOVA) of the ESG pillars score.

The remainder of the paper is structured as follows. Section 2 comprises a literature review. Section 3 describes our methodology (an empirical model, variable definitions, the sample, and the data). Section 4 provides the empirical results and discussion. Section 5 concludes the study.

## 2. LITERATURE REVIEW

Several studies urge banks and, more broadly, financial institutions in the EU and G10 countries to take action to improve their awareness, strategies, organisational, and operational defence to control and manage current and prospective risks related to the ESG and technology scores as well as the value chain complexity (Barrett, 2018; National Institute of

Standards and Technology [NIST], 2022; International Organization for Standardization [ISO], 2022; Center for Internet Security [CIS], n.d.; Cloud Security Alliance [CSA], n.d.).

Cyber risk is a dynamic risk category that has evolved substantially, although its protective processes and systems are still fundamentally evolving. In addition, data breaches can lead to financial losses, as well as harm to a company's physical assets and a company's reputation (Baror & Venter, 2019; Roskot et al., 2020). Owing to the banking industry's significant exposure to information technology (IT) and its function as a credit intermediary, hackers regularly target it (Kopp et al., 2017).

According to Yusif and Hafeez-Baig (2021), managerial culture and technical factors, which serve as the first lines of defence drive cyberattacks on the financial industry and can lead to cascading failures that business models do not fully comprehend or cannot quantify.

This study examines the importance of cyber risk management's integrated approaches to ESG principles and argues that the adoption of cyber policies by banks can help them achieve their ESG objectives. The European, international, and national Supervisory Authorities require banks to adopt a cyber policy (EBA, 2017, 2019; Organization for Economic Co-operation and Development [OECD], 2020, 2022; Banca d'Italia, 2013). Beginning in 2024 and 2025, all banks in the EU will be required to adopt a cyber policy (Directive (EU) 2022/2555, Regulation (EU) 2022/2554).

A large body of literature explores technological factors' influence on ESG performance (Batae et al., 2020; Birindelli & Intonti, 2021; Chiaramonte et al., 2022), while very few studies have focused on the relationship between cyber risk and the ESG pillars (Karagozoglu, 2021; Kluza & Kluza, 2022; Ziolo et al., 2023). Huang et al. (2023), in turn, analysed the impact of digital transformation on ESG pillars to improve the transparency of soft information, limit management myopia, and improve the ability of internal processes by enhancing their technological innovation. Qian et al. (2023) found that technological innovation also improves the supervision mechanism.

Fiordelisi et al. (2013) analysed how cyber risk can affect a bank's reputation and might even compromise the strategic processes, thereby impacting the total risk exposure, capitalization, financial and economic performance, as well as banking business models. However, to our knowledge, our study is the first to examine the potential impact of cyber policies on the assessment of ESG pillars. Our research also uses the existing literature to innovate in other aspects. First, from a methodological perspective, the adoption of a one-way ANOVA is appropriate for a complex analysis of the relationship between the ESG and defending against cyber risk, since it applies to the ESG pillars score when a bank adopts this. Second, this study supports supervisors who argue that ESG drivers are important for all financial (EBA, 2021) and IT risks (EBA, 2017, 2019). The results are useful for the discussion of the European Central Bank's (ECB) guidelines on climate change risks (ECB, 2020), the Basel Committee on Banking Supervision (BCBS) published financial risks and climate measurement methodologies (BCBS, 2021), and the European Banking Authority's (EBA) guidelines on cyberattacks (EBA, 2019). Compared to previous studies that focused on the linear symmetry and significance of individual variables, the ANOVA method allows us to combine multiple filter variables, such as the geographic area, total assets, and banks' profitability. Consequently, the results are more likely to provide insights into the significance or non-significance of the connection between the individual ESG pillars score and the cyber policy.

The objective of the study is to examine the relationship between the three components of ESG assessment and the implementation of cybersecurity policies. We propose to take into account profitability, size, and geographic location in the analysis.

## 3. RESEARCH METHODOLOGY

### 3.1. Empirical model

We conducted a series of one-way analysis of variance (ANOVA) tests on the ESG pillars score. The ANOVA method is an effective statistical strategy for analysing the group mean differences and determining how different factors affect the variability of a data set.

Various authors have used ANOVA to study various events in the context of banking and financial research (Al-Dmour, 2023; Kim et al., 2023; Noreen et al., 2023). Almatari et al. (2023) emphasised cybersecurity threats' effect on banking services in the cybersecurity and banking contexts. The study highlighted the serious issues that cybersecurity threats cause in banks. Using statistical techniques, like an ANOVA, we can determine the magnitude of these risks. This method has also been used to evaluate the variables affecting bank performance. Gao and Guo (2022), for instance, assessed the green credit policy's impact on Chinese commercial banks' financial performances by using the difference-in-differences (DID) method, which integrates the ANOVA principles.

### 3.2. Variable definitions

Refinitiv Eikon[1] (ex. Thomson Reuters Financial & Risk) provided the data for the analysis of cybersecurity policy, and financial and economic information, and the ESG pillar scores were specially scored from 0 to 100 using a proprietary algorithm. Moreover, the ESG scores used in the analysis are environmental (*ENV*), social (*SOC*), and governance (*GOV*).

Table 1 provides a summary of the dependent (*ESG pillars score*) and the independent variables that the research examined.

### 3.3. Sample and data

This study examines a sample of N = 343 listed banks covering the period from 2017 to 2022. Only banks with more than 250 employees and revenues of more than €50 million or assets of €43 million

[1] https://eikon.refinitiv.com/

and a market capitalization of more than €1 billion, operating in G10 and EU countries were selected.

Following the application of the filters and using an ANOVA, Table 2 and Table 3 show the subsamples' composition, the number of observations, the mean value, and the cyber policy groups' standard error (SE).

**Table 1.** Variables' description, source, and type

| *Variables* | *Description* | *Type* |
|---|---|---|
| *Policy cybersecurity (Cyber policy)* | Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access | Independent |
| *Environmental pillar score (ENV)* | The environmental pillar reflects how well a company uses best management practices to avoid environmental risks and capitalize on environmental opportunities to generate long-term shareholder value | Dependent |
| *Social pillar score (SOC)* | The social pillar measures are a reflection of the company's reputation and the health of its license to operate, which are key factors in determining its ability to generate long-term shareholder value | Dependent |
| *Governance pillar score (GOV)* | The corporate governance pillar reflects a company's capacity, through its use of best management practices, to direct and control its rights and responsibilities through the creation of incentives, as well as checks and balances to generate long-term shareholder value | Dependent |

*Source: Authors' elaboration*

**Table 2.** Sample, filters' type, and global observations

| *Sample* | *Type and observations* |
|---|---|
| Geographical area (from G10 and EU countries) | European (ex-EU 28 + Switzerland; Obs. = 594) and non-European (USA, Canada, Japan; Obs. = 1464) |
| Profitability (pre-tax ROA) | Pre-tax ROA1 (> 2%; Obs. = 425) and pre-tax ROA2 (< = 2%; Obs. = 1633) |
| Size (total assets) | Assets A (> €120,212,588,045.85; Obs. = 409) and Assets B (< = €120,212,588,045.85, Obs. = 1649) |

*Source: Authors' elaboration*

**Table 3.** Observation in the sample with the mean and standard error (SE) of policy cybersecurity groups

| *Sample and subsample* | *Obs. false* | *Obs. true* | *Mean and SE of ENV* | *Mean and SE of SOC* | *Mean and SE of GOV* |
|---|---|---|---|---|---|
| *All sample* | 918 (45%) | 1140 (55%) | False (29.547; 1.045)<br>True (33.699; 0.938) | False (42.174; 0.737)<br>True (50.41; 0.661) | False (49.599; 0.730)<br>True (55.632; 0.655) |
| *European subsample* | 260 (44%) | 334 (56%) | False (53.027; 1.74)<br>True (61.077; 1.535) | False (57.259; 1.176)<br>True (66.54; 1.038) | False (56.782; 1.283)<br>True (65.663; 1.132) |
| *Non-European subsample* | 658 (45%) | 806 (55%) | False (20.269; 1.041)<br>True (22.354; 0.94) | False (36.213; 0.794)<br>True (43.725; 0.718) | False (46.76; 0.845)<br>True (51.476; 0.763) |
| *Assets_A* | 158 (39%) | 251 (61%) | False (71.579; 1.528)<br>True (69.603; 1.926) | False (72.458; 1.154)<br>True (70.057; 1.455) | False (68.472; 1.314)<br>True (64.81; 1.657) |
| *Assets_B* | 760 (46%) | 889 (54%) | False (21.219; 0.912)<br>True (23.004; 0.849) | False (36.377; 0.683)<br>True (44.184; 0.632) | False (46.436; 0.765)<br>True (52.007; 0.707) |
| *Pre-tax ROA1* | 201 (47%) | 224 (53%) | False (25.96; 1.799)<br>True (32.677; 1.705) | False (43.437; 1.183)<br>True (53.906; 1.120) | False (45.454; 1.660)<br>True (51.795; 1.572) |
| *Pre-tax ROA2* | 717 (44%) | 916 (56%) | False (30.552; 1.234)<br>True (33.949; 1.092) | False (41.819; 0.878)<br>True (49.555; 0.777) | False (50.761; 0.808)<br>True (56.571; 0.715) |

*Note: Sample and subsample = type; Obs. false = observation of bank — it does not have a cyber policy; Obs. true = observation of bank — it has a cyber policy; Mean and SE = the group's mean and standard error (false/true).*
*Source: Authors' elaboration using one-way ANOVA.*

## 4. EMPIRICAL RESULTS AND DISCUSSION

Tables 4, 5, and 6 show the ANOVA's results. The significant relationship between the cyber policy and the ESG pillars score when the *F*-value is more than 3.84 and the *p*-value is less than 0.05 at an $\alpha = 0.05$. This means that a cyber policy could improve the ESG pillars score.

The summary of results in Table 4 indicates that there is a significant relationship between cybersecurity policy and *ENV* pillar score in the *All sample* (F-value = 8.74 and *p*-value = 0.0031), in the *European* subsample (F-value = 12.04 and *p*-value = 0.006), in the *Pre-tax ROA1* subsample (F-value = 7.34 and *p*-value = 0.007), and in the *Pre-tax ROA2* subsample (F-value = 4.25 and *p*-value = 0.0395). The results are consistent with the studies on the relationship between a cyber policy and the ESG pillars score (Cai et al., 2023; Liu et al., 2023) and with the BCBS (2021) guidelines on climate financial risks and measurement methodologies, as well as the EBA (2019) guidelines on cyberattacks. All of these suggest that there are parallels between the ESG risks and cyber risks in terms of their measurement, but also integration in terms of the risk management approach. The current risk management models need to be updated to address the increased risks, which are likely to arise with new technologies' extensive use.

The analysis shows no significance for the *non-European* subsample, the *Assets_A* subsample, and the *Assets_B* subsample. The results show a non-significant relationship between cyber policy and the *ENV* pillar score.

The European subsample explains almost all of the increase in the policy's mean in the all sample; the shift is equal to 4 in the all sample and the European subsample, while the shift in the non-European subsamples is respectively equal to 8

and 2. The findings verify that European and non-European banks differ significantly.

Figures 1 and 3 show that cyber policy banks' and no-policy banks' composition is not relevant for ENV's upgrading in the *non-European* subsample. This result originates from existing literature; we note that the higher significance of the *European* subsample points is due to European banks capturing the significant shift in the *ENV* pillar score in the all sample. This is linked to the main advantage of using an ANOVA test, while regression is the ability to distinguish between homogeneous groups, here European banks with a policy, those without a policy, and a *non-European* subsample.

A cyber policy's impact on the *ENV* pillar score is also not significant concerning the *Assets_A* subsample (see Figures 2 and 4) since the subsample comprises 39 per cent of banks without a cyber policy (Mean = 69.603; SE = 1.926), and 61 per cent with a cyber policy (Mean = 71.579, the SE = 1.528).

This is probably due to the relatively small number of banks in *Assets_A* (see Table 3). We note that the SE doubles in the *Assets_A* subsample compared to the *Assets_B* subsample and the all sample.

**Figure 1.** Non-European subsample's box plot (ENV)

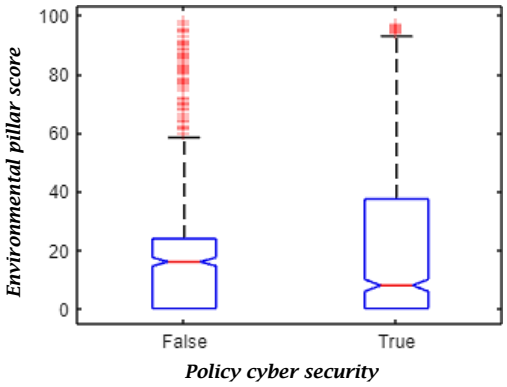
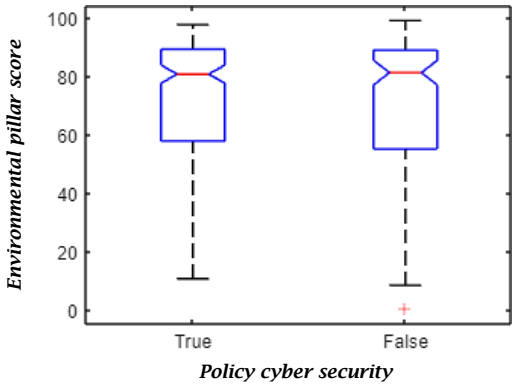



**Figure 2.** Assets_A subsample's box plot (ENV)




*Source: Authors' elaboration*

**Table 4.** ENV's results

| *Sample and subsample* | *SS* | *dF* | *MS* | *F* | *Prob > F* |
|---|---|---|---|---|---|
| ***All sample*** | | | | | |
| Policy cybersecurity | 8767.36 | 1 | 8767.36 | 8.74 | 0.0031 |
| Error | 2061354.49 | 2056 | 1002.6 | | |
| Total | 2070121.85 | 2057 | | | |
| ***European subsample*** | | | | | |
| Policy cybersecurity | 9472 | 1 | 9472.02 | 12.04 | 0.0006 |
| Error | 465858.8 | 592 | 786.92 | | |
| Total | 475330.8 | 593 | | | |
| ***Non-European subsample*** | | | | | |
| Policy cybersecurity | 1575.19 | 1 | 1575.19 | 2.21 | 0.1372 |
| Error | 1041416.43 | 1462 | 712.32 | | |
| Total | 1042991.61 | 1463 | | | |
| ***Assets_A subsample*** | | | | | |
| Policy cybersecurity | 378.7 | 1 | 378.683 | 0.65 | 0.4219 |
| Error | 238505.7 | 407 | 586.009 | | |
| Total | 238884.3 | 408 | | | |
| ***Assets_B subsample*** | | | | | |
| Policy cybersecurity | 1304.94 | 1 | 1304.94 | 2.04 | 0.1536 |
| Error | 1054775.23 | 1647 | 640.42 | | |
| Total | 1056080.17 | 1648 | | | |
| ***Pre-tax ROA1 subsample*** | | | | | |
| Policy cybersecurity | 4780.5 | 1 | 4780.49 | 7.34 | 0.007 |
| Error | 275443.2 | 423 | 651.17 | | |
| Total | 280223.7 | 424 | | | |
| ***Pre-tax ROA2 subsample*** | | | | | |
| Policy cybersecurity | 4639.85 | 1 | 4639.85 | 4.25 | 0.0395 |
| Error | 1782309.25 | 1631 | 1092.77 | | |
| Total | 1786949.1 | 1632 | | | |

*Note: j-sample (Bank): source, SS = sum of square due to each source, dF = degrees of freedom, MS = SS/dF (it is the mean square for each source), F = F-statistics (it is the ratio of mean squares), Prob > F = p-value, Policy cybersecurity = variability between groups, Error = variability within groups, Total = total variability.*
*Source: Authors' elaboration.*

**Figure 3**. Annual trend of the banks' ENV (non-European subsample)

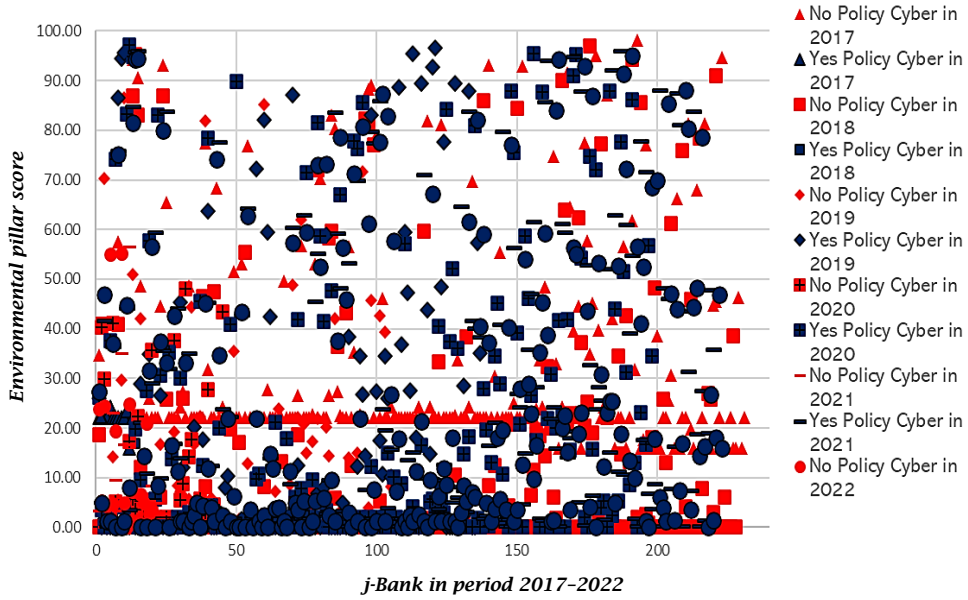
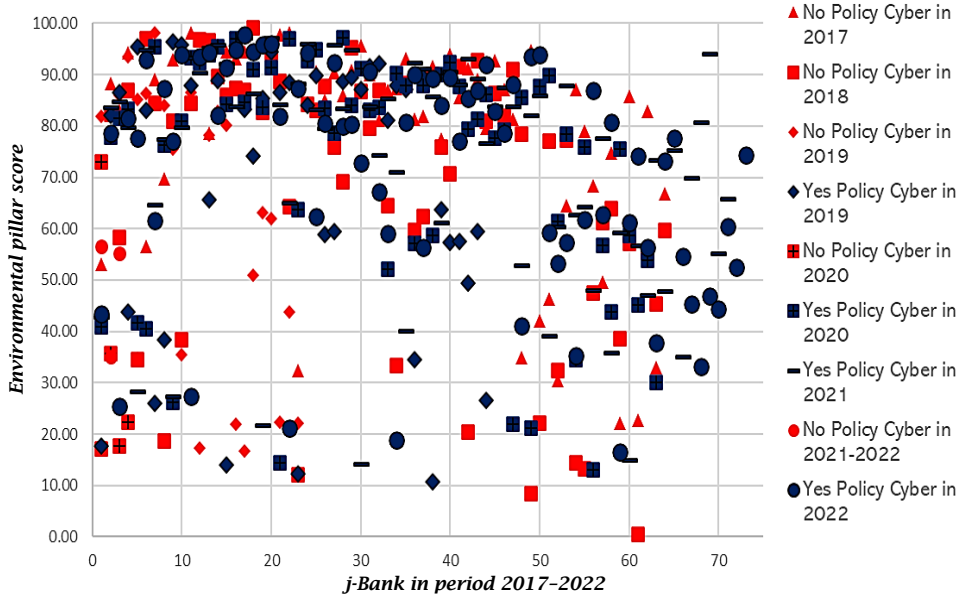



**Figure 4.** Annual trend of the banks' ENV (Assets_A subsample)

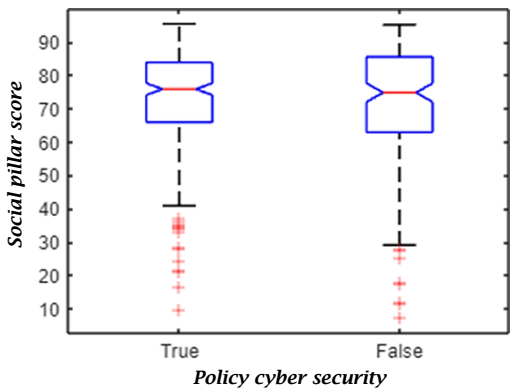



*Source: Authors' elaboration.*

The summary of the results in Table 5 indicates that there is a significant relationship between a cyber policy and the *SOC* pillars in the *All sample* (F-value = 69.18 and *p*-value = 0), in the *European* subsample (F-value = 35.02 and *p*-value = 0), in the *non-European* subsample (F-value = 49.26 and *p*-value = 0), in the *Assets_B* subsample (F-value = 70.41 and *p*-value = 0), in the *Pre-tax ROA1* sample (F-value = 41.31 and p-value = 0), and in the *Pre-tax ROA2* subsample (F-value = 43.49 and *p*-value = 0).

The non-significance of the *Assets_A* subsample is highlighted in Table 3, concerning banks without a cyber policy (Obs. = 158) and those with one (Obs. = 251); the *Assets_A* subsample's banks behave similarly. The adoption or non-adoption of a cyber policy is not significant.

**Figure 5**. Assets_A subsample's box plot (SOC)



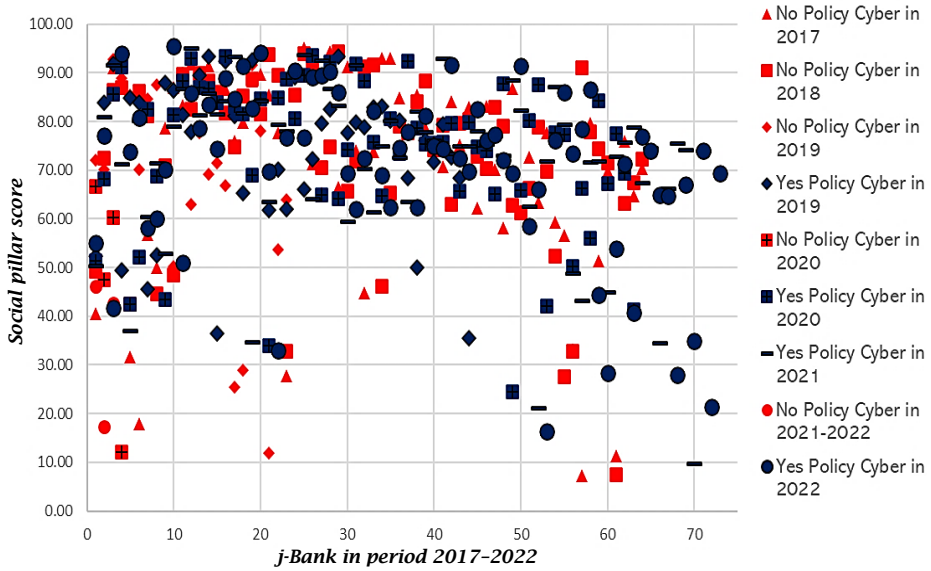
Even when we examine the mean, we notice that the level remains roughly aligned for banks with a cyber policy (Mean = 72.458; SE = 1.154) and those without a cyber policy (Mean = 70.057; SE = 1.455). Figures 5 and 6 show that a cyber policy is not relevant concerning upgrading the *SOC* pillar score. The situation is similar to an analysis of the *ENV* pillar's impact on the *European* subsample or *non-European* subsample, with the *Assets_B* subsample capturing almost all the impact of a cyber policy's adoption (the shift is the same, i.e., 8 points if the variance is similar).

**Table 5**. SOC's results

| *Sample and subsample* | *SS* | *dF* | *MS* | *F* | *Prob > F* |
|---|---|---|---|---|---|
| ***All sample*** | | | | | |
| Policy Cybersecurity | 34494.6 | 1 | 34494.6 | 69.18 | 0 |
| Error | 1025178.8 | 2056 | 498.6 | | |
| Total | 1059673.4 | 2057 | | | |
| ***European subsample*** | | | | | |
| Policy Cybersecurity | 12595.5 | 1 | 12595.5 | 35.02 | 0 |
| Error | 212094 | 592 | 359.6 | | |
| Total | 225499.1 | 593 | | | |
| ***Non-European subsample*** | | | | | |
| Policy Cybersecurity | 20444.3 | 1 | 20444.3 | 49.26 | 0 |
| Error | 606809.3 | 1462 | 415.1 | | |
| Total | 627253.6 | 1463 | | | |
| ***Assets_A subsample*** | | | | | |
| Policy Cybersecurity | 559.3 | 1 | 559.27 | 1.67 | 0.1966 |
| Error | 136081.2 | 407 | 344.352 | | |
| Total | 136640.5 | 408 | | | |
| ***Assets_B subsample*** | | | | | |
| Policy Cybersecurity | 24977.1 | 1 | 24977.1 | 70.41 | 0 |
| Error | 584243.9 | 1647 | 354.7 | | |
| Total | 609221 | 1648 | | | |
| ***Pre-tax ROA1 subsample*** | | | | | |
| Policy Cybersecurity | 11611.8 | 1 | 11611.8 | 41.31 | 0 |
| Error | 118911.5 | 423 | 281.1 | | |
| Total | 130523.3 | 424 | | | |
| ***Pre-tax ROA2 subsample*** | | | | | |
| Policy Cybersecurity | 24064.5 | 1 | 24064.5 | 43.49 | 0 |
| Error | 902448.8 | 1631 | 553.3 | | |
| Total | 926513.3 | 1632 | | | |

*Note: j-sample (Bank): source, SS = sum of square due to each source, dF = degrees of freedom, MS = SS/dF (it is the mean square for each source), F = F-statistics (it is the ratio of mean squares), Prob > F = p-value, Policy cybersecurity = variability between groups, Error = variability within groups, Total = total variability.*
*Source: Authors' elaboration.*

**Figure 6**. Annual trend of the banks' SOC (Assets_A subsample)




*Source: Authors' elaboration*

The summary of the results in Table 6 indicates that there is a significant relationship between a cyber policy and the *GOV* pillar score concerning the *All sample* (F-value = *37*.82 and *p*-value = 0), the *European* subsample (F-value = 26.94 and *p*-value = 0), the *non-European* subsample (F-value = 17.14 and *p*-value = 0), the *Assets_B* subsample (F-value = 28.58 and *p*-value = 0), the *Pre-tax ROA1* subsample (F-value = 7.69 and *p*-value = 0.0058), and the *Pre-tax ROA2* subsample

(F-value = 29 and *p*-value = 0). Using the *Total assets* filter, we show that there is no significant relationship between a cyber policy and the *GOV* pillar score in the *Assets_A* subsample.

Banks without a cyber policy (Mean = 68.472; SE = 1.314) and those with one (Mean = 64.81; SE = 1.657) behave similarly. Consequently, a cyber policy does not improve the *GOV* pillar score (Figures 7 and 8). The cyber policy might be significant if the α were 0.1.

**Figure 7**. Assets_A subsample's box plot (GOV)

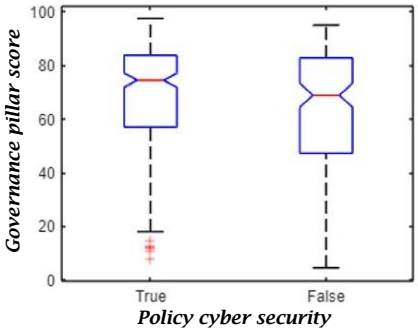
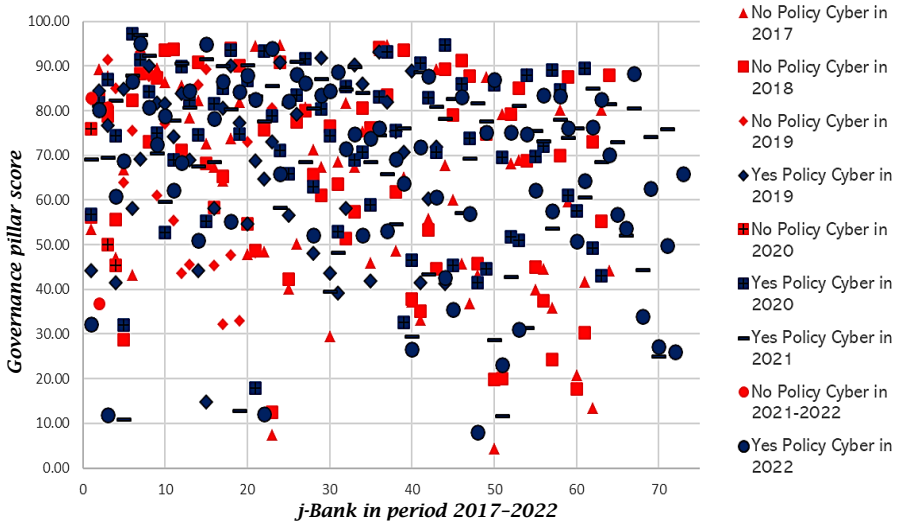



**Table 6**. GOV's results

| *Sample and subsample* | *SS* | *dF* | *MS* | *F* | *Prob > F* |
|---|---|---|---|---|---|
| ***All sample*** | | | | | |
| Policy Cybersecurity | 18512 | 1 | 18512 | 37.82 | 0 |
| Error | 1006454.83 | 2056 | 489.52 | | |
| Total | 1024966.83 | 2057 | | | |
| ***European subsample*** | | | | | |
| Policy Cybersecurity | 11531 | 1 | 11530.98 | 26.94 | 0 |
| Error | 253356.2 | 592 | 427.97 | | |
| Total | 264887.2 | 593 | | | |
| ***Non-European subsample*** | | | | | |
| Policy Cybersecurity | 8054.5 | 1 | 8054.47 | 17.14 | 0 |
| Error | 686853.1 | 1462 | 469.8 | | |
| Total | 694907.6 | 1463 | | | |
| ***Assets_A subsample*** | | | | | |
| Policy Cybersecurity | 1300.8 | 1 | 1300.82 | 3 | 0.084 |
| Error | 176480.3 | 407 | 433.61 | | |
| Total | 177781.1 | 408 | | | |
| ***Assets_B subsample*** | | | | | |
| Policy Cybersecurity | 12714.4 | 1 | 12714.4 | 28.58 | 0 |
| Error | 732750 | 1647 | 444.9 | | |
| Total | 745464.4 | 1648 | | | |
| ***Pre-tax ROA1 subsample*** | | | | | |
| Policy Cybersecurity | 4259.91 | 1 | 4259.91 | 7.69 | 0.0058 |
| Error | 234311.4 | 423 | 553.93 | | |
| Total | 238571.3 | 424 | | | |
| ***Pre-tax ROA2 subsample*** | | | | | |
| Policy Cybersecurity | 13576.3 | 1 | 13576.3 | 29 | 0 |
| Error | 763617.6 | 1631 | 468.2 | | |
| Total | 777193.9 | 1632 | | | |

*Note: j-sample (Bank): source, SS = sum of square due to each source, dF = degrees of freedom, MS = SS/dF (it is the mean square for each source), F = F-statistics (it is the ratio of mean squares), Prob > F = p-value, Policy cybersecurity = variability between groups, Error = variability within groups, Total = total variability.*
*Source: Authors' elaboration.*

**Figure 8**. Annual trend of the banks' GOV (Assets_A subsample)



When the dimensional variable is considered as a distinguishing factor, the relationship between cyber policy and *ENV* score makes an explanation.

Cyber policy is typically unrelated to ESG scores in very large banks (*Asset_A*). In actuality, these businesses have other controls and procedures that permit a greater *ESG* score even in the absence of a cyber policy.

The regulations related to cybersecurity and ESG policies have significance in the examination of banks located in various geographical areas, making it impossible to determine any relation between them.

Since both large and small sample sizes are included, profitability does not show an apparent relationship between cyber and ESG pillar scores.

## 5. CONCLUSION

To examine the relationship between the policy cyber security and the ESG pillar scores, banks were divided by geographic region, size, and profitability. For the *All sample* over the period 2017–2022, we note that only cyber policy in the *European* subsample explains the increase in the *ENV* pillar score; for the other subsamples, we observe that they are substantially independent of cyber policy. The results confirm that European and non-European banks differ significantly.

In the *Assets_A* and *Assets_B* subsamples, the cyber policy has the same effect on the *ENV* pillar score, although with less intensity, since the shifts are both equal to 2 and 2 compared to 4 overall. This is due to there being few observations, which means the SE of the *Assets_A* subsample increases. We also find that the *SOC* pillar score has a significant relationship with the cyber policy except that of the *Assets_A* subsample. The presence of three bank groups explains this finding since the subsample comprises most of the large banks with cyber policy (*Assets_A*) and small banks, some of which have a cyber policy (*Assets_B*) and some of which do not (*Assets_B*). Globally, this means that the cyber policy is not significant in respect of the *Assets_A* subsample.

The results also show that the *GOV* pillar score has a significant relationship with the cyber policy, except for the *Assets_A* subsample. Consequently, the cyber policy does not improve the *GOV* pillar score ($\alpha = 0.05$) and the cyber policy might only be significant if the $\alpha$ were 0.1. In addition, limiting the variability needs to be included in the study findings. Owing to the variability's wildly varied magnitude, the size was used to split the data into two subsamples (*Assets_A, Assets_B*), meaning the data became more like two groups than like a continuous variable. Similar research but using mixed methodologies could be very useful.

## REFERENCES


Al-Dmour, H., Saad, N., Basheer Amin, E., Al-Dmour, R., & Al-Dmour, A. (2023). The influence of the practices of big data analytics applications on bank performance: Filed study. *VINE Journal of Information and Knowledge Management Systems, 53*(1), 119–141. https://doi.org/10.1108/VJIKMS-08-2020-0151

Almatari, O., Wang, X., Zhang, W., & Khan, M. K. (2023). *Vtaim: Volatile transaction authentication insurance method for cyber security risk insurance of banking services.* Research Square. https://doi.org/10.21203/rs.3.rs-2413299/v1

Aradhna, A., Kumar, S., & Shukla, A. K. (2023). *Role of multimedia innovative technology in green banking.* In S. Grima, K. Sood, & E. Özen (Eds.), *Contemporary studies of risks in emerging technology* (Emerald Studies in Finance, Insurance, and Risk Management, Part B, pp. 275–297). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-566-820231015

Banca d'Italia. (2013). *Disposizioni di vigilanza per le Banche (Circolare Circ. 285/13)* [Supervisory provisions for banks]. Retrieved January 29, 2024, from https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/aggiornamenti/Aggiornamento-n.40-del-2-novembre-2022.pdf

Baror, S. O., & Venter, H. (2019, February 3). A taxonomy for cybercrime attack in the public cloud. In N. van der Waag-Cowling, & L. Leenen (Eds.), *Proceedings of the 14th International Conference on Cyber Warfare and Security* (pp. 505-X). Academic Conferences International Limited. https://www.researchgate.net/publication/335927227_A_Taxonomy_for_Cybercrime_Attack_in_the_Public_Cloud

Barrett, M. (2018, April 16). *Framework for improving critical infrastructure Cybersecurity Version 1.1.* NIST Cybersecurity Framework. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Basel Committee on Banking Supervision (BCBS). (2021). *Climate-related financial risks — measurement methodologies.* BIS. https://www.bis.org/bcbs/publ/d518.pdf

Batae, O. M., Dragomir, V. D., & Feleaga, L. (2020). Environmental, social, governance (ESG), and financial performance of European banks. *Journal of Accounting and Management Information Systems, 19*(3), 480–501. https://www.econbiz.de/Record/environmental-social-governance-esg-and-financial-performance-of-european-banks-b%C4%83tae-oana-marina/10012388767

Birindelli, G., & Intonti, M. (2021). Governare la transizione verso le logiche ESG nelle banche [Governing the transition towards ESG logics in banks]. In *L'integrazione dei fattori ESG nella valutazione del rischio di credito* (Position Paper N°29, pp. 35–42). AIFIRM. http://www.aifirm.it/wp-content/uploads/2016/03/2021-Position-Paper-29-ESG-e-rischio-credito.pdf

Cai, C., Tu, Y., & Li, Z. (2023). Enterprise digital transformation and ESG performance. *Finance Research Letters, 58*, Part D, Article 104692. https://doi.org/10.1016/j.frl.2023.104692

Center for Internet Security (CIS). (n.d.). 20 years of creating confidence in the connected world. Retrieved February 2, 2024, from https://www.cisecurity.org/insights/blog/20-years-of-creating-confidence-in-the-connected-world

Chiaramonte, L., Dreassi, A., Girardone, C., & Piserà, S. (2022). Do ESG strategies enhance bank stability during financial turmoil? Evidence from Europe. *The European Journal of Finance, 28*(12), 1173–1211. https://doi.org/10.1080/1351847X.2021.1964556

Cloud Security Alliance (CSA). (n.d.). Cloud controls matrix: Working group. Retrieved February 2, 2024, from https://cloudsecurityalliance.org/research/working-groups/cloud-controls-matrix

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). (2022). *Official Journal*, L 333, 80–152. http://data.europa.eu/eli/dir/2022/2555/oj

European Banking Authority (EBA). (2017, May 5). *Guidelines on security measures for operational and security risks under PSD2*. EBA. https://www.eba.europa.eu/guidelines-security-measures-operational-and-security-risks-under-psd2

European Banking Authority (EBA). (2019, November 29). *Final report: EBA Guidelines on ICT and security risk management*. EBA. https://www.eba.europa.eu/guidelines-ict-and-security-risk-management

European Banking Authority (EBA). (2021, June). *Report on management and supervision of ESG risks for credit institutions and investment firms* (EBA/REP/2021/18). EBA. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Reports/2021/1015656/EBA%20Report%20on%20ESG%20risks%20management%20and%20supervision.pdf

European Central Bank (ECB). (2020, November). *Guide on climate-related and environmental risks supervisory expectations relating to risk management and disclosure*. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm.202011finalguideonclimate-relatedandenvironmentalrisks~58213f6564.en.pdf

Fiordelisi, F., Soana, M. G., & Schwizer, P. (2013). The determinants of reputational risk in the banking sector. *Journal of Banking & Finance, 37*(5), 1359–1371. https://doi.org/10.1016/j.jbankfin.2012.04.021

Gao, X., & Guo, Y. (2022). The green credit policy impact on the financial performance of commercial banks: A quasi-natural experiment from China. *Mathematical Problems in Engineering, 2022*(1), Article 9087498. https://doi.org/10.1155/2022/9087498

Houston, J. F., & Shan, H. (2022). Corporate ESG profiles and banking relationships. *The Review of Financial Studies 35*(7), 3373–3417. https://doi.org/10.1093/rfs/hhab125

Huang, Q., Fang, J., Xue, X., & Gao, H. (2023). Does digital innovation cause better ESG performance? An empirical test of a-listed firms in China. *Research in International Business and Finance, 66,* Article 102049. https://doi.org/10.1016/j.ribaf.2023.102049

International Organization for Standardization (ISO). (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (ISO/IEC 27001:2022). https://www.iso.org/standard/27001

Jin, J., Li, N., Liu, S., & Khalid Nainar, S M. (2023). Cyber-attacks, discretionary loan loss provisions, and banks' earnings management. *Finance Research Letters, 54*, Article 103705. https://doi.org/10.1016/j.frl.2023.103705

Karagozoglu, A. K. (2021). Novel risks: A research and policy overview. *The Journal of Portfolio Management, 47*(9), 11–34. https://doi.org/10.3905/jpm.2021.1.287

Kim, M. G., Kang, S. A., & Ryu, M. H. (2023). Rethinking bank branch closure strategies through omni-channel usage data analysis. In *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)* (pp. 610-612). IEEE. https://doi.org/10.1109/ICAIIC57133.2023.10066991

Kluza, K., & Kluza, S. (2022). Addressing the new global challenges and risks in financial market. In M. Ziolo, E. Escrig-Olmedo, & R. Lozano (Eds.), *Fostering sustainable business models through financial markets* (pp. 1–34). Springer. https://doi.org/10.1007/978-3-031-07398-4_1

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Papers, 2017*(185). https://doi.org/10.2139/ssrn.3030776

Liu, J., Zhou, K., Zhang, Y., Tang, F., 2023. The effect of finance. digital transformation on financial performance: The intermediary effect of information symmetry and operating costs. *Sustainability*, *15*(6), Article 5059. https://doi.org/10.3390/su15065059

Madanchian, M. (2024). Leading the fintech revolution: Navigating the future of finance. In H. Taherdoost, N. Le, M. Madanchian, & Y. Farhaoui (Eds.), *Exploring global fintech advancement and applications* (pp. 1–18). IGI Global. https://doi.org/10.4018/979-8-3693-1561-3.ch001

Mertzanis, C. (2023). FinTech finance and social-environmental performance around the world. *Finance Research Letters, 56*, Article 104107. https://doi.org/10.1016/j.frl.2023.104107

Morgan, W. R. (2023). Finance must be defended: Cybernetics, neoliberalism and environmental, social, and governance (ESG). *Sustainability, 15*(4), Article 3707. https://doi.org/10.3390/su15043707

National Institute of Standards and Technology (NIST). (2022, June 18). *The NIST Cybersecurity Framework (CSF) 2.0.* https://doi.org/10.6028/NIST.CSWP.29

Noreen, U., Shafique, A., Ahmed, Z., & Ashfaq, M. (2023). Banking 4.0: Artificial intelligence (AI) in banking industry & consumer's perspective. *Sustainability, 15*(4), Article 3682. https://doi.org/10.3390/su15043682

Omarini, A. (2023). From digital technologies to new economics in banking: How to drive the future of digital money and data information knowledge. In P. Łasak & J. Williams (Eds.), *Digital Transformation and the Economics of Banking* (pp. 31–49). Routledge. https://doi.org/10.4324/9781003340454-3

Ooi, K. B., Tan, G. W. H., Aw, E. C. X., Cham, T. H., Dwivedi, Y. K., Dwivedi, R., Hughes, L., Kar, A. K., Loh, X.-M., Mogaji, E., Phau, I., & Sharma, A. (2023). Banking in the metaverse: A new frontier for financial institutions. *International Journal of Bank Marketing, 41*(7), 1829–1846. https://doi.org/10.1108/IJBM-03-2023-0168

Organization for Economic Co-operation and Development (OECD). (2020). Going digital integrated policy framework. *OECD Digital Economy Papers,* 292. OECD Publishing. https://www.oecd-ilibrary.org/docserver/dc930adc-en.pdf?expires=1722872551&id=id&accname=guest&checksum=44E20DFCEA025342CD097BB1E70AECDB

Organization for Economic Co-operation and Development (OECD). (2022). *Recommendation of the council on digital security risk management.* OECD/LEGAL/0479. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0479

Porcellacchia, D., & Sheedy, K. D. (2023, March 22). *Endogenous bank fragility in a macroeconomic model.* European Central Bank. https://www.ecb.europa.eu/press/conferences/shared/pdf/20231109_money_markets/Porcellacchia_paper.en.pdf

Qian, C., Gao, Y., & Chen, L. (2023). Green supply chain circular economy evaluation system based on industrial internet of things and blockchain technology under ESG concept. *Processes, 11*(7), Article 1999. https://doi.org/10.3390/pr11071999

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance). (2022). *Official Journal,* L 333, 1–79. http://data.europa.eu/eli/reg/2022/2554/oj

Roskot, M., Wanasika, I., & Kroupova, Z. (2020). Cybercrime in Europe: Surprising results of an expensive lapse. *Journal of Business Strategy, 42*(2), 91–98. https://doi.org/10.1108/JBS-12-2019-0235

Securities and Exchange Commission (SEC). (2023, July 26). *Cybersecurity risk management, strategy, governance, and incident disclosure*. https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Shackelford, S. J., Raymond, A., McCrory, M. A., & Bonime-Blanc, A. (2023). Cyber silent spring: Leveraging ESG+T frameworks and trustmarks to better inform investors and consumers about the sustainability, cybersecurity, and privacy of internet-connected devices. *University of Pennsylvania Journal of Business Law, 25*(2), 505–557. https://scholarship.law.upenn.edu/jbl/vol25/iss2/5

Smaili, N., Radu, C., & Khalili, A. (2023). Board effectiveness and cybersecurity disclosure. *Journal of Management and Governance, 27*(4), 1049–1071. https://doi.org/10.1007/s10997-022-09637-6

Yusif, S., & Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research, 16*(4), 490–513. https://doi.org/10.1080/19361610.2021.1918995

Ziolo, M., Bak, I., Cheba, K., Filipiak, B. Z., & Spoz, A. (2023). Environmental, social, governance risk versus cooperation models between financial institutions and businesses. Sectoral approach and ESG risk analysis. *Frontiers in Environmental Science, 10*, Article 1077947. https://doi.org/10.3389/fenvs.2022.1077947