Journal of Economics, Finance and Management Studies

ISSN (print): 2644-0490, ISSN (online): 2644-0504

Volume 09 Issue 02 February 2026

Article DOI: 10.47191/jefms/v9-i2-02, Impact Factor: 8.317

Page No: 567-572

Integrating Climate, Digital, and Cyber Risks into Traditional Banking Risk Types: A Conceptual IMRAD Framework Based on COSO ERM and NIST CSF 2.0

Johanes K. Adisardjono[1*], Saripudin[2], Donasius Sagita Nanlohy[3], Adrian Eka Darma Serang[4]

[1,2,3,4] Doctoral Student in Sustainable Economic, Faculty of Economics and Business Perbanas Institute Jakarta,

ABSTRACT: Climate risk, digital transformation, and cyber threats now mutually reinforce and complicate the traditional banking risk landscape, directly affecting credit, market, liquidity, operational, legal/compliance, and reputational risk types. This study aims to develop a comprehensive integrated banking risk management framework to respond to this threat convergence. Using conceptual design and literature synthesis methods, this framework is built with COSO ERM as the governance backbone and NIST CSF 2.0 (encompassing Govern, Identify, Protect, Detect, Respond, Recover functions) as the cyber operational model. The results present three main artifacts: Figure 1 as the integrated risk framework, Table 1 as a two-page crosswalk mapping risk drivers to bank risk types, and Box 1 as an Indonesian regulatory vignette. Managerial implications of this framework include the provision of concise key risk indicators (KRIs/KPIs), clarity of risk ownership based on the Three Lines of Defense (3LoD) model, and mitigation options equipped with pros and cons analysis.

KEYWORDS: climate risk, digital disruption, cybersecurity, COSO ERM, NIST CSF 2.0, banking risk.

I. INTRODUCTION

Banking risk management currently faces multidimensional challenges where physical and transition risks from climate change, accelerated digital disruption, and cyber threats can no longer be managed in isolation (silos). Global supervisory and advisory bodies emphasize the necessity of this integration; for instance, the Climaterelated Financial Risk Advisory Committee [CFRAC] (2025) highlights the importance of incorporating climate risk into financial stability frameworks. The Basel Committee on Banking Supervision [BCBS] (2022) has also established principles for effective climate-related financial risk management. On the technology operations side, the National Institute of Standards and Technology [NIST] (2024) released the Cybersecurity Framework (CSF) 2.0, reinforcing cyber risk governance as a strategic enterprise component. Therefore, banks require a unified approach to translate these external risk drivers into existing traditional risk taxonomies.

The primary contribution of this paper is the provision of ready-to-use managerial artifacts to bridge the gap between theory and practice. This paper presents Figure 1: *Integrated Banking Risk Integration Framework*, which visualizes the risk governance architecture. Additionally, Table 1 presents a two-page crosswalk mapping climate-digital-cyber risk drivers into bank risk types, complete with risk ownership, indicators, and mitigations. Finally, Box 1 presents an Indonesian regulatory vignette referencing the Financial Services Authority [OJK] (2025) policy regarding special credit treatment post-disaster, as well as relevant OJK Regulations (2022), providing tangible local context to the global framework.

It is important to note that this paper does not statistically test empirical relationships but provides managerial artifacts for further study and bank management. Its main focus is on the construction of governance logic and policy operationalization.

II. METHODOLOGY

Conceptual Design

This framework is designed using the *Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management* (COSO ERM) as the governance backbone. COSO ERM was selected due to its flexibility in aligning risk with strategy and performance. For the cybersecurity operational layer, this framework adopts NIST CSF 2.0 (NIST, 2024), centered on six core functions: *Govern, Identify, Protect, Detect, Respond,* and *Recover* (GV-ID-PR-DE-RS-RC). This combination ensures that high-level strategic risks can be translated into measurable operational actions.

Integrating Climate, Digital, and Cyber Risks into Traditional Banking Risk Types: A Conceptual IMRAD Framework Based on COSO ERM and NIST CSF 2.0

Literature Synthesis

Material development is based on a literature synthesis with inclusion criteria prioritizing publications between 2022 and 2026. Reference sources include a mix of high-quality peer-reviewed academic journals as well as standard documents from regulators, central banks, and international standard-setting bodies. This is done to ensure practical relevance and compliance with the latest regulatory landscape, such as guidance from BCBS (2022) and CFRAC (2025).

Crosswalk Construction

The construction of the crosswalk table was conducted through systematic mapping. Risk Drivers consisting of Climate, Digital, and Cyber domains were mapped for their transmission into six traditional bank risk types: credit, market, liquidity, operational, legal/compliance, and reputational. Each risk intersection was then equipped with managerial attributes: risk owners based on the *Three Lines of Defense* model (3LoD: 1st/2nd/3rd line), key risk indicators (KRI/KPI), and mitigation strategies along with their pros and cons analysis.

Indonesian Regulatory Vignette

To provide specific implementation context, a mini case study (vignette) was developed based on the Indonesian regulatory framework. This vignette uses OJK Press Release SP-220 (OJK, 2025) and OJK Regulation Number 19 of 2022 (OJK, 2022) as the basis for special treatment for disaster-affected debtors. This approach was chosen to illustrate how climate risk (natural disasters) triggers regulatory responses that directly affect bank credit and operational risks.

The advantage of this conceptual design method is transparency and the ability to be repeatable by practitioners. However, its limitation is that this framework may be viewed as subjective opinion unless the results and discussion are clearly separated and supported by strong references.

RESULTS

This section presents the primary artifacts: Figure 1 (integrated framework), Box 1 (Indonesian vignette), and Table 1 (two-page crosswalk).

Figure 1. Integrated Banking Risk Integration Framework: Operationalizing Climate, Digital Disruption, and Cybersecurity into Traditional Banking Risk Types using a COSO ERM backbone, Three Lines of Defense governance, and NIST CSF 2.0 operational lens (GV–ID–PR–DE–RS–RC).

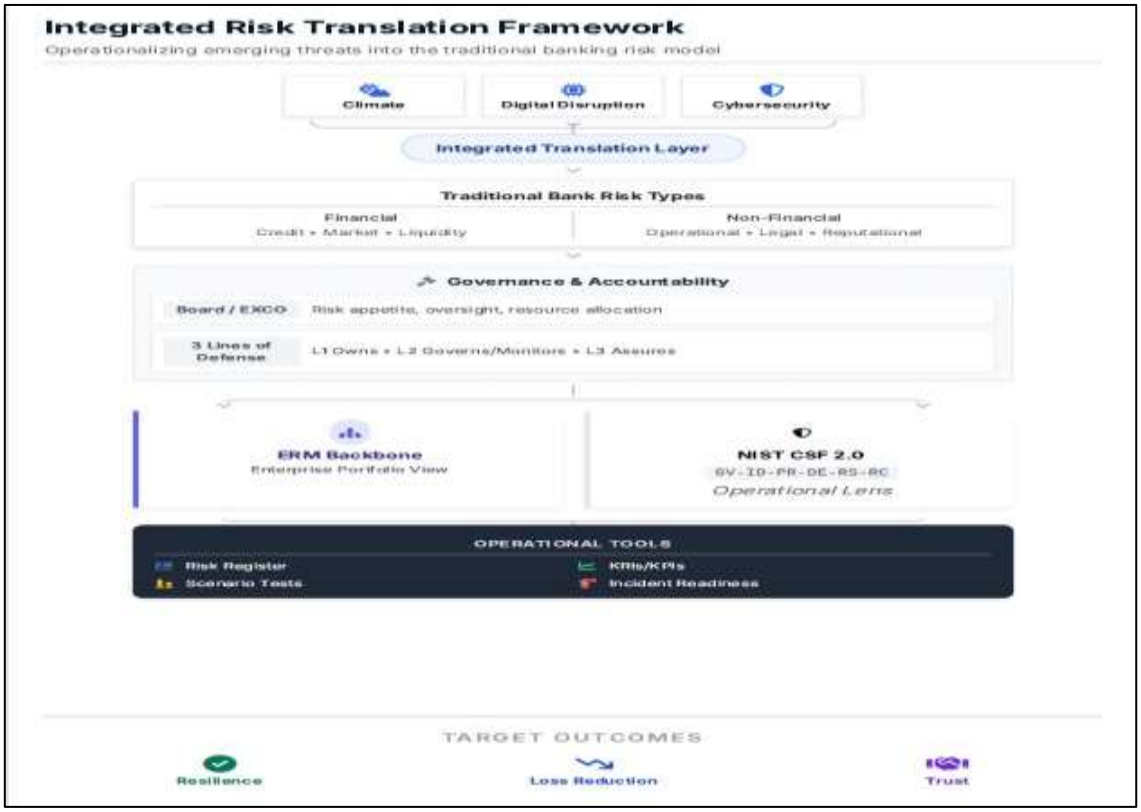

Figure 1. Coso ERM

Figure 1 above illustrates how COSO ERM functions as the primary structure supporting the entire risk architecture. The *Three Lines of Defense* (3LoD) governance layer ensures clear accountability at every organizational level. The NIST CSF 2.0 overlay with GV-ID-PR-DE-RS-RC functions provides specific operational guidance to detect and respond to cyber and digital threats within the broader context of banking risk.

In Box 1 below showing The Indonesian Regulatory Vignette: OJK SP-220 (2025) in responding the impact of natural disaster in Sumatera late 2025.

Box 1. Indonesian Regulatory Vignette: OJK SP-220 (2025) and POJK 19/2022

In response to the impact of natural disasters, which are tangible manifestations of climate risk, the Financial Services Authority (OJK) issued a special treatment policy.

- **Affected Regions:** Aceh, North Sumatra, and West Sumatra provinces.
- **Maximum Relief:** Ceiling up to Rp10 billion per debtor for MSMEs and KUR.
- **Credit Status:** Credit quality set to "Performing" after restructuring.
- **New Financing:** Quality determined separately from old facilities (*new financing*).
- **Effective Period:** Valid for 3 years from December 10, 2025.
- **Reporting:** Obligation to report to SLIK and adjust business planning. **Decision Basis:** Board of Commissioners Meeting (RDK) dated December 10, 2025.
- **Publication:** Press Release dated December 11, 2025.

References: OJK (2025) SP-220; OJK (2022) POJK 19/2022; Republika Online (2025).

Table 1 below describe how the three of external risk transmit and combine into classical banking risk

Table 1. Two-Page Crosswalk: Climate–Digital–Cyber to Traditional Banking Risk Types (Risk Owner via 3LoD, KRI/KPI, Mitigation with Pros/Cons, References)

Domain / Driver	Transmission → Risk Type	Risk Owner (3LoD)	Sample KRI / KPI	Sample Mitigations (Pros / Cons)	Key References
Climate	→ Credit Risk	1st Line	Climat eadjust ed PD/LG D volatility	Climate-scenario stress testing *Pro:* Quantifies tail risk *Con:* Data gaps, model risk	(Pozdyshev et al., 2025; BCBS, 2022)
Climate	→ Market Risk	2nd Line	Stranded asset valuation drift	Portfolio rebalancing *Pro:* Early risk capture *Con:* Exit costs	(Jung et al., 2025; Bank of England, 2024)
Climate	→ Liquidity Risk	2nd Line	Deposit outflow volatility	Contingent funding plan *Pro:* Preparedness *Con:* Cost of idle collateral	(CFRAC, 2025; BCBS, 2022)
Climate	→ Operational Risk	1st Line	Business disruption days	BCP / disaster recovery *Pro:* Minimizes downtime *Con:* Capital/resourceintensive	(OJK, 2025; OJK, 2022)

Domain / Driver	Transmission → Risk Type	Risk Owner (3LoD)	Sample KRI / KPI	Sample Mitigations (Pros / Cons)	Key References
Climate	→ Legal / Compliance	2nd Line	Noncomplian ce events	Regulatory monitoring dashboard *Pro:* Early alert *Con:* Regulatory uncertainty	(BCBS, 2022; CFRAC, 2025)
Climate	→ Reputational Risk	1st/2 nd Line	Media sentiment index	ESG disclosure enhancement *Pro:* Stakeholder trust *Con:* Greenwashing risk	(Bruno et al., 2025; Ren et al., 2025)
Digital	→ Credit Risk	1st Line	Fintech default correlation	Credit scoring algorithm upgrades *Pro:* Speed *Con:* Bias/opacity	(Liu et al., 2025; Uddin et al., 2023)
Digital	→ Market Risk	2nd Line	Algotrading volatility	Kill-switch mechanism *Pro:* Rapid response *Con:* False positives	(Gaviyau & Godi, 2025)
Digital	→ Liquidity Risk	2nd Line	E-deposit run velocity	Real-time liquidity monitoring *Pro:* Early warning *Con:* System latency	(Uddin et al., 2023)
Digital	→ Operational Risk	1st Line	System downti me frequen cy	Cloud redundancy *Pro:* Scalability *Con:* Vendor lock-in	(European Union, 2023; ISACA, 2025)
Digital	→ Legal / Compliance	2nd Line	Regulator y breach count	RegTech adoption *Pro:* Automation *Con:* Regulatory lag	(European Union, 2023)
Digital	→ Reputational Risk	1st/2 nd Line	Customer churn rate	Digital UX enhancement *Pro:* Retention *Con:* Upfront investment	(Liu et al., 2025)
Cyber	→ Credit Risk	1st Line	Fraud loss ratio	AI-based fraud detection *Pro:* Precision *Con:* Adversarial attacks	(Azura et al., 2025; NIST, 2024)
Cyber	→ Market Risk	2nd Line	Trading disrupti on incident s	Cybersecurity penetration testing *Pro:* Resilience *Con:* Cost/scope	(NIST, 2024)
Cyber	→ Liquidity Risk	2nd Line	Payment-rail outage minutes	Multi-channel payment backup *Pro:* Continuity *Con:* Complexity	(OCC, 2025; NIST, 2024)

Domain / Driver	Transmission → Risk Type	Risk Owner (3LoD)	Sample KRI / KPI	Sample Mitigations (Pros / Cons)	Key References
Cyber	→ Operational Risk	1st Line	Cyber incident frequency	IST CSF 2.0 implementation *Pro:* Standardized *Con:* Cultural resistance	(NIST, 2024; Kuhn et al., 2025)
Cyber	→ Legal / Compliance	2nd Line	Data breach notificatio ns	Encryption & access control *Pro:* Reduces breach impact *Con:* Key mgmt burden	(NIST, 2024; European Union, 2023)
Cyber	→ Reputational Risk	1st/2nd Line	Customer trust scores	Cyber-resilience disclosure *Pro:* Transparency *Con:* Revealing vulnerabilities	(Bruno et al., 2025; OCC, 2025)

Notes. KRI = Key Risk Indicator; KPI = Key Performance Indicator; 3LoD = Three Lines of Defense; 1st line = business/operational units; 2nd line = risk management & compliance; 3rd line = internal audit. References are presented in abbreviated format; see References for full details.

DISCUSSION

Managerial Implications

The integration of climate, digital, and cyber risks demands the reduction of silos within the bank's organizational structure. Management must establish clear escalation mechanisms and standardize Key Risk Indicators (KRIs) across domains to ensure holistic risk visibility. The use of governance functions (GOVERN) within NIST CSF 2.0 is crucial for enforcing accountability from the board level down to operations (NIST, 2024; CFRAC, 2025). This enables banks to respond to threats with greater agility and coordination.

Trade-offs and Risks

Implementing this framework is not without *trade-offs*. The use of climate-adjusted credit risk models (*climateadjusted PD/LGD*) faces challenges of model risk and historical data gaps (Pozdyshev et al., 2025). Furthermore, disaster relief policies such as those implemented in Indonesia may give rise to *moral hazard* if not strictly monitored, where debtors who are actually capable of paying take advantage of relief facilities (OJK, 2025). Management must also be vigilant against the danger of *KPI overload*, where too many indicators obscure actual risk signals.

VRIO Analysis

From a strategic perspective, the capability of integrating risk governance can be analyzed using the VRIO framework. This integration is valuable (*Value*) as it protects bank capital and reputation. This capability is also rare (*Rarity*) because few banks have fully integrated these three risk domains. However, the *Imitability* aspect may be high as regulatory standardization increases, so long-term competitive advantage depends on the *Organization* aspect—the extent to which risk culture is embedded in every bank business decision.

CONCLUSION

This paper has presented a conceptual framework integrating climate, digital, and cyber risks into traditional banking risk taxonomy. Through Figure 1, Table 1, and Box 1, this research provides concrete managerial artifacts. Key benefits for practitioners include the availability of a concise list of KRIs/KPIs, clarity of risk ownership within the 3LoD structure, and mitigation options evaluated for pros and cons. Future research is suggested to empirically test the effectiveness of proposed KRIs, conduct in-depth case studies, and evaluate the long-term impact of disaster relief policies on bank stability (OJK, 2025; OJK, 2022).

REFERENCES

1) Azura, S. N., Azad, M. A., & Ahmed, Y. (2025). An integrated cyber security risk management framework for online banking systems. *Journal of Banking and Financial Technology, 9*, 85–104. https://doi.org/10.1007/s42786-025-00056-3
2) Bank of England. (2024). Measuring climate-related financial risks using scenario analysis. *Bank of England Quarterly Bulletin, 2024*. https://www.bankofengland.co.uk/quarterly-bulletin/2024/2024/measuringclimate related financial risk usuing scenario analysis-
3) Basel Committee on Banking Supervision [BCBS]. (2022). *Principles for the effective management and supervision of climate-related financial risks* (BCBS D532). Bank for International Settlements. https://www.bis.org/bcbs/publ/d532.htm
4) Bruno, E., Pistolesi, N., & Teti, E. (2025). Cybersecurity policy, ESG and operational risk: A virtuous relationship to improve banks' performance. *International Review of Economics & Finance, 99*, Article S1059056025002163. https://www.sciencedirect.com/science/article/pii/S1059056025002163
5) Climate-related Financial Risk Advisory Committee [CFRAC]. (2025). *CFRAC Key Themes 2025*. U.S. Department of the Treasury. https://home.treasury.gov/system/files/261/CFRAC-Key-Themes20250115.pdf
6) European Union. (2023). *Digital Operational Resilience Act (DORA)* (Regulation 2022/2554). https://www.sciencedirect.com/science/article/abs/pii/S0267364923001413
7) Gaviyau, W., & Godi, J. (2025). Emerging risks in the fintech-driven digital banking environment: A bibliometric review of China and India. *Risks, 13*(10), Article 186. https://www.mdpi.com/22279091/13/10/186
8) Institute of Information Security and Cyber Assurance [ISACA]. (2025). European financial industry shifts toward digital operational resilience. *ISACA Journal, 2025*(3). https://www.isaca.org/resources/isacajournal/issues/2024/volume-3/european-financial-industry-shifts-toward-digital-operational-resilience
9) Jung, H., Lee, J., & Yoon, S.-M. (2025). The climate-related financial risks measurement methodologies: Advances, challenges, and frontiers. *Research in International Business and Finance, 79*, Article S0275531925003101. https://www.sciencedirect.com/science/article/pii/S0275531925003101
10) Kuhn, J., Scott, W., & Taylor, M. (2025). Cybersecurity governance and organizational resilience: A framework for sustainable risk management. *Journal of Accountancy & Information Systems*. https://doi.org/10.1080/07366981.2025.2596943
11) Liu, Y., Wang, X., & Zhang, L. (2025). Navigating fintech and banking risks: Insights from a systematic literature review. *Nature Humanities and Social Sciences Communications, 12*, Article 05055. https://www.nature.com/articles/s41599-025-05055-9
12) National Institute of Standards and Technology [NIST]. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
13) Office of the Comptroller of the Currency [OCC]. (2025). *Cybersecurity and Financial System Resilience Report 2025*. https://www.occ.gov/publications-and-resources/publications/cybersecurityand-financial-system-resilience/files/pub-2025-cybersecurity-report.pdf
14) Otoritas Jasa Keuangan [OJK]. (2025, 11 Desember). *OJK keluarkan kebijakan perlakuan khusus kredit/pembiayaan korban bencana Aceh, Sumut dan Sumbar* [Siaran pers]. https://ojk.go.id/id/berita-dan-kegiatan/siaran-pers/Pages/OJK-Keluarkan-Kebijakan-Perlakuan-KhususKredit-Pembiayaan-Korban-Bencana-Aceh,-Sumut-dan-Sumbar.aspx
15) Otoritas Jasa Keuangan [OJK]. (2022). *Peraturan Otoritas Jasa Keuangan Nomor 19/POJK.03/2022 tentang perlakuan khusus untuk lembaga jasa keuangan pada daerah dan sektor tertentu di Indonesia yang terkena dampak bencana*. https://ojk.go.id/id/regulasi/Documents/Pages/Perlakuan-Khusus-untukLembaga-Jasa-Keuangan-Pada-Daerah-dan-Sektor-Tertentu-di-Indonesia-yang-Terkena-DampakBencana/POJK%2019-2022.%20Dampak%20Bencana.pdf
16) Pozdyshev, M., Renzhi, N., & Serletis, A. (2025). *Climate risk and credit: The role of climate-sensitive PD/LGD modelling* (BIS Working Paper No. 1274). Bank for International Settlements. https://www.bis.org/publ/work1274.pdf
17) Ren, X., Li, W., & Li, Y. (2025). Climate risk, digital transformation and corporate green innovation efficiency: Evidence from China. *Technological Forecasting and Social Change, 195*, Article 122754. https://www.sciencedirect.com/science/article/pii/S0040162524005754
18) Republika Online. (2025). *Kebijakan Relaksasi* [Tag page]. https://republika.co.id/tag/kebijakan relaksasi
19) Uddin, M. H., Mollah, S., Islam, N., & Ali, M. H. (2023). Does digital transformation matter for operational risk exposure? *Technological Forecasting and Social Change, 197*, Article 122919. https://www.sciencedirect.com/science/article/pii/S0040162523006042