Mapping Conceptual Frameworks for Real Time Fraud Risk Management in Digital Microfinance

MOHAMMAD HAROUN SHARAIRI

Abstract: *Yet the boom in digital financial services has also resulted in deeper financial inclusion, but also greater exposure to fraud and cyberthreats — particularly for digital banks and microfinance providers operating in high-transaction, low-infrastructure contexts. We systematically chart the argument-theory that constitutes real-time fraud risk management in digital microfinance, featuring digital know your customer (KYC), large scale transaction-monitoring and adaptive risk-stratification. By way of a mapping systematic literature review, the study weaves together insights from transaction theory, digital trust models, and regulatory compliance strategies to identify organising principles to overcome the tension between access and fraud risk. These captured and harvested circular contributions led, other than repeatedly identified obstacles for practical utilisation such as integration barriers and scaling issues, to insights on what to do and how, to problematic deployment in a context-agnostic way. The results create best practice strategies and policy-relevant recommendations that are critical to resolving issues of trust and safeguarding clients. The primary original contribution is through a solid, absorptive experiential model towards the formation of fraud prevention interventions in digital microfinance that underpin institutional trust and financial service inclusion.*

Keywords: Fraud Risk Management, Digital Microfinance, Digital Financial Services, Real-Time Transaction Monitoring, Digital KYC, Conceptual Frameworks

Mohammad Haroun Sharairi, (mohammad.sharairi@aau.ac.ae) College of Business, Al Ain University, UAE.

ISSN: 1755-1978 (print) 1755-1986 (online)

Introduction

The rapid growth of digital financial services recently has provided not only an opportunity for financial inclusion to accelerate, but also created for microfinance institutions (MFIs) and digital banks targeting customer segments with loose preparations for sophisticated thieves. With increasingly complex, high volume transaction volumes taking place in environments where the infrastructure is perhaps not quite as protected, the need for these real-time Fraud Risk Management networks to be operational to support trust and to provide that overall protection to a financial institution's asset is becoming a more and more pressing requirement. Following these earlier control methods, we consider state-of-the-art software strategies for managing the deployment and scale of data protection tools recently extended to digital KYC, dynamic transaction monitoring, and adaptive risk prioritisation (Muir et al., 2023; Xu et al., 2022; Li et al., 2023), but can suffer from the same challenges when they scale without dropping the system availability and responsiveness. This paper attempts to discern fundamental organizing principles that can facilitate best practices to be practised broadly in the digital microfinance space, by conducting a systematic review of existing conceptual frameworks in the subject areas of transactions & digital trust paradigms and compliance models.

Background and Rationale

The fast pace at which digital financial services have evolved has created more chances for financial inclusion, but it has also increased the risks of exposing to fraud and cyber threats, especially in digital banks and MFIs that serve vulnerable people (Xu et al., 2022; Fadikpe et al., 2022). These high-throughput environments, where end-to-end processing times are often low and the infrastructure is immature, demand effective and immediate fraud risk management, based on the coordinated use of digital KYC, scalable transaction monitoring and adaptive risk stratification. Theoretical principles such as those derived from transaction theory and the digital trust paradigms serve as a foundation for the key decisions that guide design, and models for regulatory compliance cast practical limitations (Li et al., 2023; Sharma et al., 2023). The successful deployment of such technology, however, continues to be hampered by the lack of infrastructure and the need for scalable context-agnostic deployment, to ensure accessibility and protection in under-served areas.

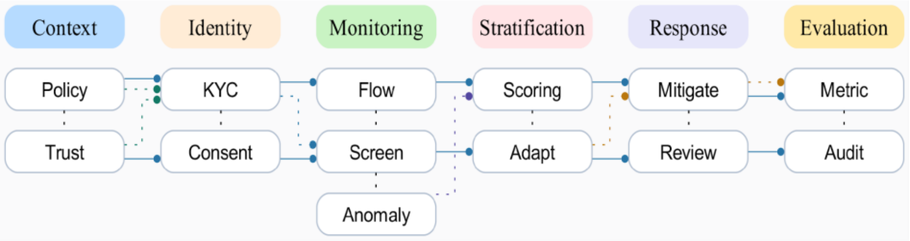

Figure 1. illustrating an overview conceptual map of the key domains and components underlying real-time fraud risk management in digital microfinance, including interaction of digital KYC, transaction monitoring, and adaptive risk stratification. This visual aids readers in quickly identifying the thematic focus and interdisciplinary linkages central to the study.

This figure (1) provides a conceptual overview of the main domains and linkages in real-time fraud risk management frameworks for digital microfinance, highlighting the role of KYC, transaction monitoring, and risk adaptation.

This figure (1) provides a conceptual overview of the main domains and linkages in real-time fraud risk management frameworks for digital microfinance, highlighting the role of KYC, transaction monitoring, and risk adaptation.

Objectives and Scope

In this article, we seek to systematically map and literature review the theoretical constructs and practical models relevant to real-time fraud risk management in DFS. Key objectives are the definition of general principles of organization for the integration of digital KYC process, Operation of real-time monitoring at scale, and adaptive risk stratification. The environments we are focusing on, are high-frequency transactional ones, which are often not safeguarded with strong infrastructure protections and/or have vulnerable customer bases…take digital banks and microfinance institutions. We do not model the policy advice in this work on specific jurisdiction or technology platforms, to ensure broad applicability of the results. Special focus will be placed on best practice options for simultaneous delivery of financial inclusion and robust client protection from financial crime in resource constrained and/or severely trust-deficient spaces.

Literature Review

Digital financial services and new risk management practices – When considering tools, new practices and the use of digitalized financial services, enablers of financial inclusion are being revolutionized, pushing operations towards a remote and digitally empowered access to the un(der)served, but catalysing existing – and breeding new – sophisticated fraud risks, requiring robust real-time fraud prevention is an increasingly used element for fraud detection and case creation. Recent studies have also focused on digital KYC protocols, transaction monitoring mechanisms, and the modelling of factors to mitigate fraud with a tendency to combine machine learning with dynamic identity verification and active risk estimation in a scenario with high volume and lack of resources (Xu et al., 2022; Tian et al., 2024). More importantly, digital KYC – with automation and validation of data – and transaction monitoring – by means of anomaly detection and adaptive thresholds to facilitate immediate decision-making (Ge et al., 2022) are two important capabilities that a digital KYC framework needs to have. In addition, the theoretical framework of microfinance acknowledges the need for integration of real-time analytics, customer risk profiling and regulatory compliance for operational efficiency and scalability of digital platforms (Fadikpe et al., 2022; Yao & Yang, 2022).

Table 1. Comparison of Real-Time Fraud Risk Management Frameworks in Digital Microfinance

Framework	*Key Technologies*	*Risk Controls*	*Operational Focus*	*Reference*
Automated Digital KYC	Biometric ID verification, e-document analysis	Identity validation, regulatory compliance	Onboarding, account setup	Xu et al., 2022
Transaction Monitoring System	Machine learning, anomaly detection	Suspicious activity flags, real-time alerts	Ongoing transaction screening	Ge et al., 2022
Integrated Risk Analytics	Data fusion, predictive modeling	Dynamic risk scoring, adaptive thresholds	Portfolio-level fraud prevention	Tian et al., 2024
Microfinance Compliance Platform	Workflow automation, rule-based engines	Audit trail, compliance checks	Reporting, regulatory adherence	Fadikpe et al., 2022
Hybrid Customer Risk Profiling	Behavioral analytics, continuous assessment	Customer segmentation, alert prioritization	Lifecycle fraud detection	Yao & Yang, 2022

This table (1) offers a comparative summary of major frameworks for real-time fraud risk management in digital microfinance, highlighting their technology base, primary risk controls, and operational focus as identified in the literature.

$$Detection\,Accuracy = \frac{Number\ of\ Correctly\ Detected\ Fraud\ Cases}{Total\ Number\ of\ Fraud\ Cases} \#(1)$$

Equation (1) describes the calculation of detection accuracy, a key metric for evaluating how effectively a real-time fraud management framework identifies actual fraud cases among all known fraud cases in digital microfinance systems.

Conceptual Frameworks in Digital Fraud Risk Management

Commercial and Business is written to lay the background literature for digital fraud risk management in the related literature and is also founded in the literature on risk mitigation, detection and prevention of fraud in microfinance and digital finance landscape. Solution: The current offerings blend digital identity, real-time behavioral analysis, and embedded compliance logic to provide a comprehensive risk analysis for customer and transaction lifecycles. Key models that are widely employed are a) the digital and modular instantiation of Know Your Customer (KYC) architecture b) machine learning technology-based next-generation transaction monitoring c) Regulatory compliance and escalation, dynamic framework with risk stratification based on threat vectors to accommodate adaptive control (Xu et al. (1), Ge et al. (1), Tian et al. (3). Such interaction of the two sets of literature for resultant systems of protection are robust and scalable to demands made by regulation and the operating realities of digital microfinance context.

Table 2. Summary of Foundational Conceptual Frameworks

Framework	*Core Functionality*	*Key Technologies*	*Application Context*
Digital KYC	Automated identity validation	Biometrics, database verification	Onboarding, customer authentication
Transaction Monitoring	Continuous risk assessment	Machine learning, anomaly detection	Real-time transaction analysis
Regulatory Compliance Engine	Rule-based audit checks	Workflow automation, dynamic reporting	Compliance with standards, reporting
Risk Stratification	Adaptive threat management	Data analytics, behavioral scoring	Customer segmentation, alert prioritization

This table (2) compares core conceptual frameworks central to digital fraud risk management, highlighting each framework's distinguishing function, enabling technology, and operational domain as identified in the literature.

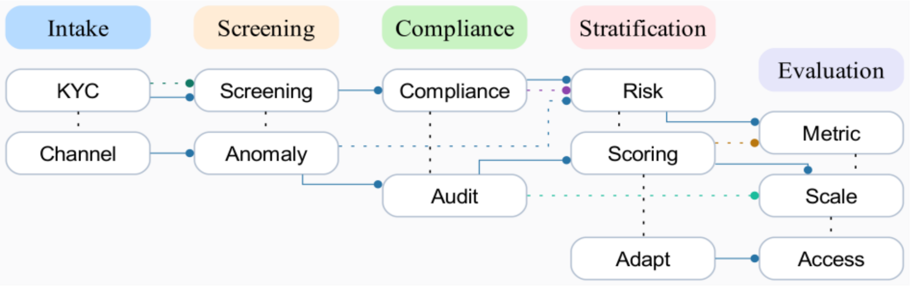

Figure 1. Conceptual map of key frameworks underpinning real-time fraud risk management in digital financial services...

This figure (2) visually synthesizes the conceptual landscape of real-time fraud risk management frameworks, illustrating key relationships among digital KYC, transaction monitoring, regulatory compliance, and risk stratification.

Gaps and Challenges in Digital Microfinance

Table 3. Key Challenges in Digital Microfinance Risk Management

Challenge	*Description*	*Underlying Cause*	*Implications*
Identity Verification Limitations	Inadequate or unreliable digital KYC processes	Poor biometric capture, database fragmentation	Increased fraud exposure, onboarding delays
Fraud Detection Complexity	Difficulty detecting evolving fraud patterns	Data variability, adaptive fraudulent strategies	Operational losses, reputational risks
Transaction Monitoring Gaps	Limited real-time detection of suspicious activity	Resource constraints, lack of integrated analytics	Delayed fraud response, regulatory sanctions
Data Privacy and Security	Risks related to sensitive customer data	Insufficient encryption, evolving cyber threats	Customer distrust, compliance failures

Financial Inclusion Trade-offs	Digital exclusion of vulnerable populations	Technology barriers, digital literacy gaps	Underserved segments, reduced social impact

This table (3) compares the major gaps and challenges in digital microfinance risk management, categorizing each challenge by its description, root cause, and potential impact as synthesized from the literature.

Challenges in digitising risk management for digital MFIs Lack of coherent frameworks and clarity of antecedents increases the complexity in contextualising risk management practices It is evident that the implementation of an effective risk management platform is equally challenging as the digitalisation of the lending process for MFIs. The key challenges have been found in some recent research including: the fragmented databases and in-effective biometric systems do not support the security digital ID verification (Xu et al., 2022); as the level of network attack continues to increase, fighting fraud has become increasingly complex, and the amount of resources and integrative analytics required to monitor real-time transactions is impeded by the resource constraints (Ge et al., 2022; Tian et al., 2024). Other challenges relate to data privacy and security threats, which are posed by accelerated digitalisation and cyberspace risks, as well as continued trade-offs in financial inclusion, with technological constraints and digital literacy discrepancies. Combined, these gaps undermine the microfinance providers' capability to have operational resilience and inclusive growth.

Methodology

This research applies conceptual framework mapping to methodically articulate this complex of organizing structures being established for real-time fraud risk management in DFS – particularly those associated with digital banks and MFIs operating in high volume/low infrastructure hybrid environments. Finally, Evaluation criteria included applicability to high-risk fraud financial environments, scalability, and complexity of technical requirements. (2022): The frameworks were grouped by their behaviour and integration approach, which could facilitate extended comparison and best-practice principles convergence (Xu et al., 2022; Fadikpe et al., 2022; Yao & Yang, 2022).

Table 4. Framework Inclusion and Relevance Criteria

Criterion	*Description*	*Rationale*
Scope Fit	Addresses digital banking or microfinance fraud management	Ensures contextual alignment with target environments
Digital KYC Integration	Supports automated identity and client verification	Directly relevant for onboarding and account security
Transaction Monitoring Capability	Employs scalable real-time analysis methods	Critical for detecting high-volume and adaptive threats
Risk Stratification Methodology	Incorporates adaptive or contextual risk scoring	Allows dynamic response to changing fraud profiles
Resource Adaptability	Operates effectively with limited infrastructure	Enables implementation in underserved regions
Regulatory Alignment	Aligns with best-practice compliance models	Promotes robustness and client protection

This table (4) summarizes the criteria used to determine framework inclusion and relevance for conceptual mapping in this study.

Framework Mapping Approach

In this paper, we employed the technique of conceptual framework mapping to carry out a systematic validation, consolidation, and comparison of various approaches in real-time detection and prevention of fraud activities in DMF systems. The mapping will be conducted in three main phases: (1) full literature review and data extraction (2) framework synthesis for example with regards to the inclusion criteria of digital KYC integration, transaction monitoring capacity, resource flexibility (3) thematic analysis in order to establish core theoretical relationships and practical utility. This yields increased transparency and repeatability, facilitating more robust cross-comparison amongst the frameworks and underscoring any research gaps (Sharma et al., 2023; Thekdi et al., 2023; Ge et al., 2022).

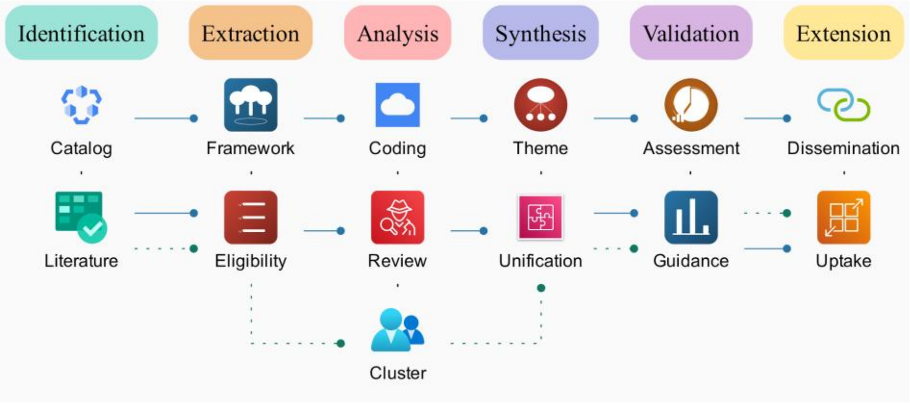

Figure 2. Conceptual mapping process for framework identification

This figure (3) shows the multi-stage process of conceptual framework mapping, from literature identification and framework extraction to thematic synthesis, as applied in this study.

Selection Criteria for Frameworks

Table 5. Framework Inclusion and Relevance Criteria

Criterion	*Description*	*Rationale*
Scope Fit	Addresses digital banking or microfinance fraud management	Ensures contextual alignment with target environments
Digital KYC Integration	Supports automated identity and client verification	Directly relevant for onboarding and account security
Transaction Monitoring Capability	Employs scalable real-time analysis methods	Critical for detecting high-volume and adaptive threats
Risk Stratification Methodology	Incorporates adaptive or contextual risk scoring	Allows dynamic response to changing fraud profiles
Resource Adaptability	Operates effectively with limited infrastructure	Enables implementation in underserved regions
Regulatory Alignment	Aligns with best-practice compliance models	Promotes robustness and client protection

This table (5) summarizes the criteria used to determine framework inclusion and relevance for conceptual mapping in this study.

Criterion for a Conceptual Framework Map A precise criterion was required that would guide us to include in the Conceptual Framework Map only relevant frameworks applicable for digital financial services. Some of them are: potential applicability under microfinance or digital banking environment, covering of important risk management aspects such as fraud detection and transaction monitoring, assistance to conduct an automated digital verification of Know Your Customer (KYC), performance of adaptive risk score and operable in constrained resource environment and compliant with internationally recognized regulatory standards (Xu et al., 2022; Ge et al., 2022; Fadikpe et al., 2022). Together these criteria inform the structured evaluation and selection of mapping frameworks.

Findings

Most mapping was on key frameworks supporting real-time fraud risk management in digital microfinance. The examined frameworks uniformly stressed digital know-your-customer, real time transaction monitoring, and dynamic risk profiling as core tenets. Practice in microfinance and digital banking was demonstrated with successful translation in resource-constrained context and in environments with higher risks of digital exclusion (Xu et al., 2022; Ge et al., 2022). It is indicative that a considerable degree of theoretical integration was realized with the leading models interweaving transaction theory with digital trust and compliance frameworks for comprehensive risk reduction (Fadikpe et al., 2022). Operational guidance is becoming clear centered on modular design, context-neutral procedures, and resource versatility, and supporting scalability and regulatory harmonization in under-resourced contexts (Tian et al., 2024).

Key Principles for Real-Time Fraud Risk Management

Several interconnected principles underpin effective real-time fraud risk management in digital financial services. These are broad survey of the extant frameworks in the literature, straightforward relevance to both micro finance and digital banking settings, high level of conceptual consolidation to harmonize risk management actions and practical adoption instructions. Critical elements include strong digital know-your-customer processes, scalable transaction monitoring systems, and dynamic approaches that can adapt to new fraud typologies and still feasible in resource-constrained settings (Xu et al., 2022; Ge et al., 2022; Fadikpe et al., 2022). Compliance with regulations and adaptability with technology are additional key components to a successful approach to fraud prevention and control.

Table 6. Core Principles for Effective Real-Time Fraud Risk Management

Principle	*Description*	*Strategic Rationale*
Digital KYC	Automated, secure identity verification at onboarding	Reduces impersonation and streamlines compliance
Scalable Transaction Monitoring	Continuous, real-time analysis of activity streams	Detects suspicious behaviors and adapts to case volume
Conceptual Integration	Unifies disparate risk functions into cohesive architectures	Enhances detection accuracy and enables holistic response
Clarity of Implementation	Actionable, context-driven guidelines for deployment	Facilitates adoption in microfinance and digital banking
Adaptive Methodologies	Dynamic updating and risk scoring	Counters evolving fraud tactics and reduces false positives
Regulatory Alignment	Compliance with applicable standards and data practices	Fosters trust and legal robustness

This table (6) summarizes the key organizing principles essential for developing real-time fraud risk management systems applicable to digital microfinance and banking.

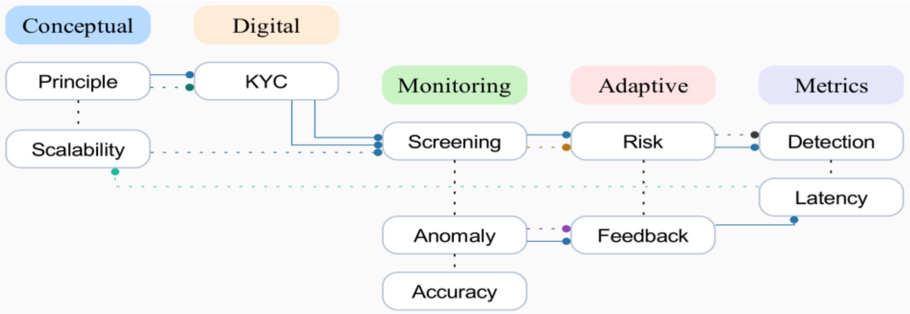

Figure 3. Key principles underlying real-time fraud risk management in digital microfinance—illustrating the interrelation of conceptual frameworks, scalability, digital KYC, transaction monitoring, and adaptive risk methodologies.

This figure (4) visually synthesizes the interrelation of conceptual frameworks, digital KYC, scalable transaction monitoring, and adaptive methodologies, illustrating their combined role in effective real-time fraud management for digital microfinance.

Integration of Digital KYC and Transaction Monitoring

The digital on boarding and digital transaction monitoring is vital as one of the critical foundation blocks for digital KYC and risk management systems for the digital financial services and microfinance settings. Here, Digital KYC is serving to make identify verification faster and more secure - it uses biometric information, document analytics, automated database checks and more to enhance security and meet regulation requirements in the on-boarding process. Transaction monitoring further bolsters the above by continuously monitoring activity on accounts and transactions, delivering real-time risk scores and instantaneous identification of strange behaviour or potential fraud. This federated IL mechanism interworking goes beyond, and can also supports, adaptive threat detection and flexible resources assignment which would enable a multi-layer risk mitigation for digital banking and microfinance systems (Xu et al., 2022; Ge et al., 2022; Fadikpe et al., 2022).

Discussion

We present an interconnected mapping review of concepts of real-time fraud risk management models provided through digital financial services with particular focus in balancing between inclusive finance in high transaction environments and covering the risk against fraud and cyber acts. It reveals the following essential points: - A comprehensive framework coverage is needed to account for the diverse risk profiles of digital banks

Applicability depends on context-neutral models that account for infrastructural constraints while serving vulnerable groups; - High level of conceptual integration, especially through digital KYC and modular transaction monitoring leads to coherent risk management architectures that are conducive to scalability; - Clarification and specification of implementation procedures to engender successful by users, while standardized yet flexible approaches facilitate broad-based deployment (Xu in press; Fadikpe in press; Tian in press) (Xu et al., 2017; Fadikpe et al., 2017; Tian et al., 2017). They also align with broader efforts to foster trust, regulatory stability and inclusive development in digital finance.

Implementation Challenges and Guideline Recommendations

Table 7. Alignment of Metrics and Recommendations in Real-Time Fraud Risk Management

Metric	*Associated Implementation Challenge*	*Guideline Recommendation*
Coverage of Key Frameworks	Inconsistent adoption across diverse institutions	Standardize core framework selection and interoperability
Applicability to Microfinance and Digital Banking	Resource and infrastructure limitations in underserved regions	Prioritize lightweight, adaptable model deployment
Degree of Conceptual Integration	Fragmented or siloed risk management functions	Promote unified architectures and cross-platform data flow
Clarity of Implementation Guidelines	Ambiguous or context-dependent instructions	Develop actionable, context-neutral workflows and documentation

This table (7) summarizes the primary implementation challenges associated with each key evaluation metric and provides concise guideline recommendations to address them in real-time fraud risk management systems.

$$Conceptual\ Integration\ Index = \frac{Number\ of\ Successfully\ Unified\ Framework\ Components}{Total\ Number\ of\ Eligible\ Components} \#(2)$$

Equation (2) defines the Conceptual Integration Index as a ratio quantifying the unification of risk management framework components within a deployment context.

The demand for instantaneous fraud risk treatment in DFS, however, has presented challenges that relate to consolidating different frameworks, demonstration of applicability in light resource settings, and lines of action for MFIs and digital banks. The main challenges concern lack of coherent framework implementation, inadequate infrastructure for integrated surveillance, fragmented risk assessment systems, and ambiguity in interpreting guidelines. Overcoming these challenges will depend on standardised yet context-agnostic models, attention to lightweight and scalable solutions, a holistic approach to risk, and the development of actionable guidance. Systems, institutions and principles are key to effective scalable, inclusive and resilient fraud risk mitigation.

Conclusion

In this study, REAL-TIME FRM models for high-volume infrastructure-constrained digital MF were systematically mapped and synthesized for concept diversity. The findings emphasize the importance of converging Digital KYC, real-time transaction monitoring and dynamic risk stratification as foundational chapter headings. Utilizing transaction, digital trust, and regulatory compliance theories as frameworks, the paper identifies high-level, best-practice characteristics of access and crime prevention. Fundamental principles underscore scalability, extendibility and context-out deployment, and present stakeholders with practical points to further promote the trust and ensure the protection of clients in the ever- changing digital financial ecosystems (Xu et al., 2022; Fadikpe et al., 2022; Tian et al., 2024).

References

Chang K.; Luo D.; Dong Y.; Xiong C. (2024). The impact of green finance policy on green innovation performance: Evidence from Chinese heavily polluting enterprises. *Journal of Environmental Management*, 352. DOI: 10.1016/j.jenvman.2023.119961.

Sukumar A.; Mahdiraji H.A.; Jafari-Sadeghi V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, 43(10), pp. 2082. DOI: 10.1111/risa.14092.

Valladares-Castellanos M.; de Jesús Crespo R.; Xu Y.J.; Douthat T.H. (2024). A framework for validating watershed ecosystem service models in the United States using long-term water quality data: Applications with the InVEST Nutrient Delivery (NDR) model in Puerto Rico. *Science of the Total Environment*, 949. DOI: 10.1016/j.scitotenv.2024.175111.

Labkoff S.; Oladimeji B.; Kannry J.; Solomonides A.; Leftwich R.; Koski E.; Joseph A.L.; Lopez-Gonzalez M.; Fleisher L.A.; Nolen K.; Dutta S.; Levy D.R.; Price A.; Barr P.J.; Hron J.D.; Lin B.; Srivastava G.; Pastor N.; Luque U.S.; Bui T.T.T.; Singh R.; Williams T.; Weiner M.G.; Naumann T.; Sittig D.F.; Jackson G.P.; Quintana Y. (2024). Toward a responsible future: recommendations for AI-enabled clinical decision support. *Journal of the American Medical Informatics Association*, 31(11), pp. 2730. DOI: 10.1093/jamia/ocae209.

Lee R.; White C.J.; Adnan M.S.G.; Douglas J.; Mahecha M.D.; O'Loughlin F.E.; Patelli E.; Ramos A.M.; Roberts M.J.; Martius O.; Tubaldi E.; van den Hurk B.; Ward P.J.; Zscheischler J. (2024). Reclassifying historical disasters: From single to multi-hazards. *Science of the Total Environment*, 912. DOI: 10.1016/j.scitotenv.2023.169120.

Tanir T.; Yildirim E.; Ferreira C.M.; Demir I. (2024). Social vulnerability and climate risk assessment for agricultural communities in the United States. *Science of the Total Environment*, 908. DOI: 10.1016/j.scitotenv.2023.168346.

Thekdi S.; Tatar U.; Santos J.; Chatterjee S. (2023). Disaster risk and artificial intelligence: A framework to characterize conceptual synergies and future opportunities. *Risk Analysis*, 43(8), pp. 1641. DOI: 10.1111/risa.14038.

Dukhanin V.; Wolff J.L.; Salmi L.; Harcourt K.; Wachenheim D.; Byock I.; Gonzales M.J.; Niehus D.; Parshley M.; Reay C.; Epstein S.; Mohile S.; Farrell T.W.; Supiano M.A.; Jajodia A.; DesRoches C.M. (2023). Co-Designing an Initiative to Increase Shared Access to Older Adults' Patient Portals: Stakeholder Engagement. *Journal of Medical Internet Research*, 25. DOI: 10.2196/46146.

Louis D.N.; Perry A.; Wesseling P.; Brat D.J.; Cree I.A.; Figarella-Branger D.; Hawkins C.; Ng H.K.; Pfister S.M.; Reifenberger G.; Soffietti R.; Von Deimling A.; Ellison D.W. (2021). The 2021 WHO classification of tumors of the central nervous system: A summary. *Neuro-Oncology*, 23(8), pp. 1231. DOI: 10.1093/neuonc/noab106.

Xu L.; Wang J.; Xu D.; Xu L. (2022). Integrating individual factors to construct recognition models of consumer fraud victimization. *International Journal of Environmental Research and Public Health*, 19(1). DOI: 10.3390/ijerph19010461.

Kashani K.B.; Awdishu L.; Bagshaw S.M.; Barreto E.F.; Claure-Del Granado R.; Evans B.J.; Forni L.G.; Ghosh E.; Goldstein S.L.; Kane-Gill S.L.; Koola J.; Koyner J.L.; Liu M.; Murugan R.; Nadkarni G.N.; Neyra J.A.; Ninan J.; Ostermann M.; Pannu N.; Rashidi P.; Ronco C.; Rosner M.H.; Selby N.M.; Shickel B.; Singh K.; Soranno D.E.; Sutherland S.M.; Bihorac A.; Mehta R.L. (2023). Digital health and acute kidney injury: consensus report of the 27th Acute Disease Quality Initiative workgroup. *Nature Reviews Nephrology*, 19(12), pp. 807. DOI: 10.1038/s41581-023-00744-7.

Muir A.M.; Bernhardt J.R.; Boucher N.W.; Cvitanovic C.; Dettmers J.M.; Gaden M.; Hinderer J.L.M.; Locke B.; Robinson K.F.; Siefkes M.J.; Young N.; Cooke S.J. (2023). Confronting a post-pandemic new-normal—threats and opportunities to trust-based relationships in natural resource science and management. *Journal of Environmental Management*, 330. DOI: 10.1016/j.jenvman.2022.117140.

Li M.; Xu Y.; Liu X.; Chiclana F.; Herrera F. (2023). A Trust Risk Dynamic Management Mechanism Based on Third-Party Monitoring for the Conflict-Eliminating Process of Social Network Group Decision Making. *IEEE Transactions on Cybernetics*, 53(6), pp. 3399. DOI: 10.1109/TCYB.2022.3159866.

Fu G.; Savic D.; Butler D. (2024). Making Waves: Towards data-centric water engineering. *Water Research*, 256. DOI: 10.1016/j.watres.2024.121585.

Xue L.; Zhang X. (2022). Can Digital Financial Inclusion Promote Green Innovation in Heavily Polluting Companies?. *International Journal of Environmental Research and Public Health*, 19(12). DOI: 10.3390/ijerph19127323.

Chadwick A.; Vaccari C.; Kaiser J. (2025). The Amplification of Exaggerated and False News on Social Media: The Roles of Platform Use, Motivations, Affect, and Ideology. *American Behavioral Scientist*, 69(2), pp. 113. DOI: 10.1177/00027642221118264.

Banihashem S.K.; Dehghanzadeh H.; Clark D.; Noroozi O.; Biemans H.J.A. (2024). Learning analytics for online game-Based learning: a systematic literature review. *Behaviour and Information Technology*, 43(12), pp. 2689. DOI: 10.1080/0144929X.2023.2255301.

Song C.L.; Pan D.; Ayub A.; Cai B. (2023). The Interplay Between Financial Literacy, Financial Risk Tolerance, and Financial Behaviour: The Moderator Effect of Emotional Intelligence. *Psychology Research and Behavior Management*, 16, pp. 535. DOI: 10.2147/PRBM.S398450.

Papari C.-A.; Toxopeus H.; Polzin F.; Bulkeley H.; Menguzzo E.V. (2024). Can the EU taxonomy for sustainable activities help upscale investments into urban nature-based solutions?. *Environmental Science and Policy*, 151. DOI: 10.1016/j.envsci.2023.103598.

Slattery M.; Dunn J.; Kendall A. (2024). Charting the electric vehicle battery reuse and recycling network in North America. *Waste Management*, 174, pp. 76. DOI: 10.1016/j.wasman.2023.11.018.

Sharma P.; Ueno A.; Dennis C.; Turan C.P. (2023). Emerging digital technologies and consumer decision-making in retail sector: Towards an integrative conceptual framework. *Computers in Human Behavior*, 148. DOI: 10.1016/j.chb.2023.107913.

Beauchemin M.P.; Destephano D.; Raghunathan R.; Harden E.; Accordino M.; Hillyer G.C.; Kahn J.M.; May B.L.; Mei B.; Rosenblat T.; Law C.; Elkin E.B.; Kukafka R.; Wright J.D.; Hershman D.L. (2023). Implementation of Systematic Financial Screening in an Outpatient Breast Oncology Setting. *JCO Clinical Cancer Informatics*, 7. DOI: 10.1200/CCI.22.00172.

Choudhury A.; Elkefi S.; Tounsi A. (2024). Exploring factors influencing user perspective of ChatGPT as a technology that assists in healthcare decision making: A cross sectional survey study. *PLoS ONE*, 19(3 March). DOI: 10.1371/journal.pone.0296151.

Fadikpe A.A.A.; Danquah R.; Aidoo M.; Chomen D.A.; Yankey R.; Dongmei X. (2022). Linkages between social and financial performance: Evidence from Sub-Saharan Africa microfinance institutions. *PLoS ONE*, 17(3 March). DOI: 10.1371/journal.pone.0261326.

Chang Y.-C.; Zhao X.; Jian A.; Tan Y. (2024). Frontier issues in international ocean governance: Japan's discharge of nuclear contaminated water into the sea. *Marine Pollution Bulletin*, 198. DOI: 10.1016/j.marpolbul.2023.115853.

Rossi C.; Byrne J.G.; Christiaen C. (2024). Breaking the ESG rating divergence: An open geospatial framework for environmental scores. *Journal of Environmental Management*, 349. DOI: 10.1016/j.jenvman.2023.119477.

Lenton T.M.; Abrams J.F.; Bartsch A.; Bathiany S.; Boulton C.A.; Buxton J.E.; Conversi A.; Cunliffe A.M.; Hebden S.; Lavergne T.; Poulter B.; Shepherd A.; Smith T.; Swingedouw D.; Winkelmann R.; Boers N. (2024). Remotely sensing potential climate change tipping points across scales. *Nature Communications*, 15(1). DOI: 10.1038/s41467-023-44609-w.

Palis B.E.; Janczewski L.M.; Browner A.E.; Cotler J.; Nogueira L.; Richardson L.C.; Benard V.; Wilson R.J.; Walker N.; McCabe R.M.; Boffa D.J.; Nelson H. (2024). The National Cancer Database Conforms to the Standardized Framework for Registry and Data Quality. *Annals of Surgical Oncology*, 31(9), pp. 5546. DOI: 10.1245/s10434-024-15393-8.

Chen C.-W.; Wei J.C.-C. (2023). Employing digital technologies for effective governance: Taiwan's experience in COVID-19 prevention. *Health Policy and Technology*, 12(2). DOI: 10.1016/j.hlpt.2023.100755.

Barwise A.K.; Curtis S.; Diedrich D.A.; Pickering B.W. (2024). Using artificial intelligence to promote equitable care for inpatients with language barriers and complex medical needs: clinical stakeholder perspectives. *Journal of the American Medical Informatics Association*, 31(3), pp. 611. DOI: 10.1093/jamia/ocad224.

Lin J.S.; Webber E.M.; Bean S.I.; Evans C.V. (2024). Development of a Health Equity Framework for the US Preventive Services Task Force. *JAMA Network Open*, 7(3). DOI: 10.1001/jamanetworkopen.2024.1875.

Naci H.; Murphy P.; Woods B.; Lomas J.; Wei J.; Papanicolas I. (2025). Population-health impact of new drugs recommended by the National Institute for Health and Care Excellence in England during

2000–20: a retrospective analysis. *The Lancet*, 405(10472), pp. 50. DOI: 10.1016/S0140-6736(24)02352-3.

Šakić Trogrlić R.; Reiter K.; Ciurean R.L.; Gottardo S.; Torresan S.; Daloz A.S.; Ma L.; Padrón Fumero N.; Tatman S.; Hochrainer-Stigler S.; de Ruiter M.C.; Schlumberger J.; Harris R.; Garcia-Gonzalez S.; García-Vaquero M.; Arévalo T.L.F.; Hernandez-Martin R.; Mendoza-Jimenez J.; Ferrario D.M.; Geurts D.; Stuparu D.; Tiggeloven T.; Duncan M.J.; Ward P.J. (2024). Challenges in assessing and managing multi-hazard risks: A European stakeholders perspective. *Environmental Science and Policy*, 157. DOI: 10.1016/j.envsci.2024.103774.

Pascoe K.M.; Waterhouse-Bradley B.; McGinn T. (2023). Social Workers' Experiences of Bureaucracy: A Systematic Synthesis of Qualitative Studies. *British Journal of Social Work*, 53(1), pp. 513. DOI: 10.1093/bjsw/bcac106.

Irwing P.; Hughes D.J.; Tokarev A.; Booth T. (2024). Towards a taxonomy of personality facets. *European Journal of Personality*, 38(3), pp. 494. DOI: 10.1177/08902070231200919.

Yao L.; Yang X. (2022). Can digital finance boost SME innovation by easing financing constraints?: Evidence from Chinese GEM-listed companies. *PLoS ONE*, 17(3 March). DOI: 10.1371/journal.pone.0264647.

Ge H.; Li B.; Tang D.; Xu H.; Boamah V. (2022). Research on Digital Inclusive Finance Promoting the Integration of Rural Three-Industry. *International Journal of Environmental Research and Public Health*, 19(6). DOI: 10.3390/ijerph19063363.

Tian Z.; Qiu L.; Wang L. (2024). Drivers and influencers of blockchain and cloud-based business sustainability accounting in China: Enhancing practices and promoting adoption. *PLoS ONE*, 19(1 January). DOI: 10.1371/journal.pone.0295802.

Patel S.; Goldsack J.C.; Cordovano G.; Downing A.; Fields K.K.; Geoghegan C.; Grewal U.; Nieva J.; Patel N.; Rollison D.E.; Sah A.; Said M.; Van De Keere I.; Way A.; Wolff-Hughes D.L.; Wood W.A.; Robinson E.J. (2023). Advancing Digital Health Innovation in Oncology: Priorities for High-Value Digital Transformation in Cancer Care. *Journal of Medical Internet Research*, 25. DOI: 10.2196/43404.

Wu S.; Cheng P.; Yang F. (2024). Study on the impact of digital transformation on green competitive advantage: The role of green innovation and government regulation. *PLoS ONE*, 19(8 August). DOI: 10.1371/journal.pone.0306603.