Indian Journal of Information Sources and Services
ISSN: 2231-6094 (P) Vol.14, No.4, 2024, pp.16-21

DOI: https://doi.org/10.51983/ijiss-2024.14.4.03

Digital Risk Management: A Study of How Firms Mitigate Digital Risks and Threats

Dr. Byju John[1] and Dr. Atul Dattatraya Ghate[2]

[1]Professor, Department of Management, Kalinga University, Raipur, India
[2]Professor, Department of Management, Kalinga University, Raipur, India
E-mail: [1]ku.byjujohn@kalingauniversity.ac.in, [2]ku.atuldattatrayaghate@kalingauniversity.ac.in
ORCID: [1]https://orcid.org/0009-0003-1216-0810, [2]https://orcid.org/0009-0009-0869-2957
(Received 07 July 2024; Revised 11 August 2024, Accepted 23 September 2024; Available online 15 November 2024)

Abstract **- The banking industry has seen a sharp rise in the use of AI services over the last ten years, which has improved client satisfaction and efficiency. The machine learning (ML), one of artificial intelligence's primary building blocks, has caused a paradigm change in the banking services sector. Every new technology that is introduced carries with it new threats. Finding such hazards is only the first step; you also need to analyse, evaluate, treat, regulate, and keep an eye on them. Risk is characterised by three elements: the possibility of loss, the unpredictability of the result, and the necessity of making a decision. According to this concept, a risk management strategy should be divided into three stages to address risks: planning ahead, carrying out risk management tasks, and maintaining and enhancing risk management. The first two stages could appear self-evident. But it's critical to recognise that risk management is a continuous process that requires constant attention. Continuous risk management is intended to avert issues, enhance product quality, make better use of available resources, and foster teamwork.**

Keywords: **Digital Transformation, Digital Risk, Business Management**

I. INTRODUCTION

These days, banks use artificial intelligence (AI) to enhance or automate a number of critical procedures, including chatbots, risk management, know-your-customer, personalised banking, document processing, and visualisation, and anti-money laundering (AML) and fraud pattern detection (Tupa et al., 2017). claim that employing robots may save up to 87% of costs when compared to hiring full-time or contract workers, suggesting that banks will keep investing in AI to reach maximum efficiency without sacrificing customer experience.

There are always new hazards associated with implementing new technologies. AI is frequently used to handle sensitive data, making it a target for businesses attempting to carry out massive network attacks or steal people's personal information (AL-Dosari & Fetais, 2023). Clarify that artificial intelligence (AI) is merely a technological tool, and its usefulness depends on how it is applied. AI can be harmful in the same ways that it can be used to help processes. As a result, misuse of the technology—such as AI-driven cyberattacks—may be considered a security risk. Furthermore, there are still numerous systems with security flaws that need to be fixed, and AI has not yet reached its full potential. In the worst-case situations, these technical flaws have resulted in worker deaths in factories when AI-driven robots have attacked (Boyson et al., 2022). A less violent but no less catastrophic event brought about by an AI flaw occurred when an AI-powered stock trading bot triggered a trillion-dollar stock market flash crash. Apart from technological misuse and flaws, the potential for AI to become self-aware intelligence presents a security risk.

In addition to issues with cybersecurity, ethical and legal concerns arise when it comes to AI security. Data ethics is a typical difficulty in AI system development, because massive volumes of data are handled while machine learning is utilised to train the system. The difficulty lies in utilising the most data while posing the fewest hazards. Making decisions based on generalised data would therefore provide the next data ethical dilemma. An example of this would be whether the safety of a pedestrian or the driver should come first in a self-driving automobile; this might potentially result in legal problems. While the AI system is being trained, there may also be legal concerns because a large amount of required personal data may be classified (Thach et al., 2021).

According to (Bucovetchi & Vevera, 2024), a certain risk management methodology appropriate for software must be utilised when examining IT systems, including AI. From a security standpoint, risk management for IT systems could be broken down into three stages, as shown in (Brender & Markov, 2013). The stages are named risk mitigation, risk assessment, and risk management planning, nevertheless. These stages could be broken down even further into steps that include both quantitative and qualitative procedures. While risk mitigation may seem straightforward, with popular practices like password strengthening, the risk assessment that precedes risk reduction is typically intricate. When deploying a new IT solution, it is also advised that risk management be incorporated into the project management framework (Prabadevi et al., 2024).

In this case, the introduction is examined in section 1 of the article. Section 2 describes the review of the work further

Section 2 and 3 explains the goal of the work digital technologies, and Section 4 concludes the project (Oleksandr et al., 2024).

II. Literature Review

The field of using AI to handle information in business models is still in its infancy. As a result, there is not much research done in the area of cybersecurity as it relates to business applications of AI. After reviewing the state of the industry (Linkov et al., 2018) came to the conclusion that AI may help companies protect their data against creative hackers. When applying AI to address cybersecurity problems, they did find a number of issues with the anomaly detection systems. These included possible openings for abuse and a deficiency in human connection and interpretation. Similar worries were expressed (Chen et al., 2021), who also mentioned that societal effects might result from AI solutions. They contend that there are other dangers in addition to cybersecurity, such as organisational and regulatory concerns. The authors come to the conclusion that a holistic approach—addressing all pertinent perspectives—is necessary when analysing the influence of artificial intelligence. Liu and Murphy contend that business managers must use this strategy to train their staff and develop policies for the safe deployment of AI systems. A related framework known as the Multi-Level perspective (MLP) was developed (Eltweri et al., 2020). A broader range of parameters can be included in the theoretical framework of MLP in order to better comprehend the impact of innovation. The user can evaluate the interactions at three different analytical levels with this approach: the niche level, the socio-technical regime level, and the external socio-technical landscape level.

The application of AI in the banking industry is the phenomenon that this thesis examines. More precisely, the thesis examines the hazards that the implementation presents from a variety of angles. The study will concentrate on the risk management strategies used by industry players. The research gap this study aims to fill is the lack of a thorough grasp of how this phenomena could effect the banking sector in the current literature. The application of AI solutions in banking may bring up new opportunities as well as risks (Brockett et al., 2012; Rami et al., 2024). Although (Edu et al., 2021) notes that AI is being used more frequently in the financial industry as a tool to fight cyberattacks, little research has been done on the problems that AI itself may offer. It is necessary to screen all risks, not just cybersecurity-related ones, in order to completely understand how AI impacts businesses and their risk management procedures. One method for examining how the risk management procedure has changed inside the company is to use the Dynamic Risk Management Framework (DRMF) developed (Avci, 2020). By using this kind of instrument, the research can comprehend how AI affects risk management in organisations (Kul & Upadhyaya, 2015).

Now more than ever, the investigated phenomenon's significance is clear. With a 64% growth in global investment on cybersecurity between 2015 and 2020, cybersecurity is becoming a critical component of every business strategy. Cybersecurity awareness is important since research indicates a direct positive association between it and a company's market worth (McClure & Parkinson, 2017). From a managerial standpoint, researching the hazards related to AI will add to the field's expertise. Because AI is becoming more and more important in cybersecurity, it will be important to look into every facet of the phenomena, which may be done with the help of an MLP. Adopting an MLP in its whole entails accepting that artificial intelligence (AI) carries risks outside of cybersecurity, like organisational and regulatory concerns. This study offers an examination of how risk management in the banking industry will evolve as a result of the introduction of AI, since it has been demonstrated that the existing literature lacks deeper analysis about the effects of AI (Yang et al., 2021).

III. Research Framework

The aim of this research is to use a mixed-methods approach to examine the ways in which the adoption of AI affects risk management in the banking industry, taking into account the effects of different approaches at different stages of the process. The project also plans to use the DRMF to examine AI risk management. The DRMF is being used since it will enable the study to comprehend how risk management is currently carried out in practice as well as how artificial intelligence will alter these practices. As a result, the study will examine the area from an industrial standpoint in order to comprehend how the phenomena affects various analytical (Ciborra, 2006).

By analysing the present risk management and AI deployment procedures, the study seeks to close the gap in the literature surrounding security aspects of AI in the banking sector. The study then attempts to create a framework solution for managers concerning AI risk management. The study's output is to advance knowledge in the industry and serve as a manual for businesses integrating AI into their operations. This will be accomplished by going over the dynamic relationships between the sector's risk management procedures at various MLP framework levels (Brzica & Brzica, 2021). Illustration of the Identified Codes and Themes shown in Fig. 1.

In light of the problem formulation and the study's objectives, the following research questions will be addressed.

- How can banking institutions apply the Dynamic Risk Management Framework to reduce the risks associated with AI solutions?
- What are the Multi-Level Effects of AI Implementation on Risk Management in Banking?

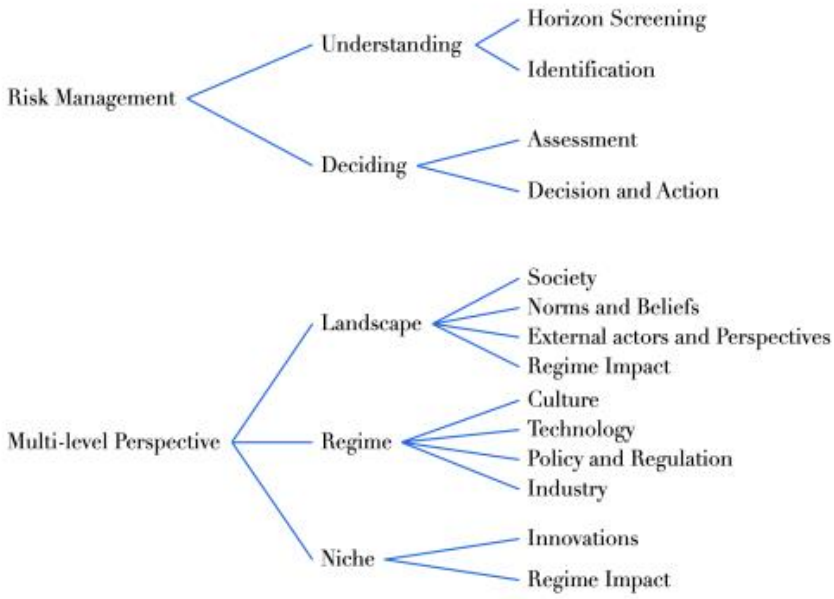

Fig. 1: Illustration of the Identified Codes and Themes

According to the framework, risk management may be divided into two broad stages: understanding and deciding, each of which consists of two parts. In order to identify hazards, as well as the data, information, and knowledge associated with each risk, understanding refers to the process of processing and managing knowledge and information. The two stages of comprehending risk are identification and horizon screening. The practice of outlining hazards for a certain scenario, such as a business, service, or product, is known as "horizon screening." This include determining the parties involved, setting boundaries and other restrictions, and locating any serious risks. The process continues with the identification step, which deals with the actual identification and conceptualisation of the hazards. Using the information gathered from the horizon screening step, the risks are precisely identified in this phase (Ivanov et al., 2019).

After the risks are identified, the second stage, decision-making, deals with potential courses of action. The two stages of assessment, choice, and action make up the deciding step. The procedures used to determine what risk management actions are required are part of the assessment phase. Examples include employing forecasting techniques to predict results or rating potential measures based on certain metrics or criteria.

Every stage of this otherwise linear process is linked to two comprehensive, never-ending activities. The first suggests that risk management is an ongoing activity and is characterised by monitoring, review, and continual improvement. An company must always strive to manage risks effectively and efficiently because the conditions associated with them are ever-changing. Examples include adjustments to the workforce or industry, as well as new external risks and opportunities that could be tracked using various KPIs. The other activity is referred to as "communication & consultation" and it deals with the ongoing sharing of knowledge and information. This involves all elected stakeholders as well as those who deal directly with the risk management process.

Data Collection

Three distinct subjects comprise the study's scope: cybersecurity, artificial intelligence, and the banking industry. Respondents who understood at least one, but ideally more, of these three themes as well as elements of risk management had to be chosen. Selecting respondents with different levels of experience also enables the study to have a comprehensive understanding of the subject, which is essential to preserving an industrial viewpoint.

The first step in the selection process was determining the competences needed to accomplish the study's goal. In order to better understand what insights would be required to construct a comprehensive solution, this approach was carried out in tandem with the literature research. An knowledge of the relationships between the previously stated areas would be a crucial quality for possible respondents, in addition to having competence in one of the topics. Interviewees with perspectives on AI's interactions with cybersecurity and the financial industry were sought after.

There are two categories that can be formed from the final selection of responses. The first set of responders either worked for a bank or for an AI company that was connected to the financial industry in some way, along with security. All of the responders in the second group were employed by Company A, an IT consulting business with a focus on cybersecurity. Every respondent employed by Company A had prior banking experience, either as consultants or staff members, and a number of them also had knowledge in implementing AI. Using both current banking sector workers and outside experts was done for a number of reasons. In

order to ensure that the study would obtain an up-to-date picture of how the sector currently operates, the study first sought perspectives from respondents who would not be biassed towards the current processes within the sector. Second, it was critical to identify responders who had sufficient knowledge of all three subjects; this could be done by making use of Company A's competences (Creazza et al., 2022).

The creation of an interview guide was the initial stage of the main data collecting. In order to prevent making the interview feel awkward, this guide provides a broad overview of the interview questions without becoming too specific. Rather, it is the interviewer's responsibility to ask pertinent follow-up questions that both keep the interview interesting and address the research topics.

A literature review has been carried out in order to gather secondary data. Reviewing and condensing all of the accessible material served the goal of understanding the state of the examined field (Luo, 2022). To be more precise, the literature review used a semi-systematic approach, which means that its scope was predetermined.

IV. Experimental Analysis

Examining the raw data and turning it into insightful and useful information is the aim of this project. We compile the primary data collected during fieldwork in this chapter. We obtain broad insights and broad observations through data analysis. We used MS-Excel 2019, JAMOVI 2.3.28.0, and the Statistical Package for Social Sciences (SPSS) version 23.0 to analyse the data. A range of statistical tests were carried out in accordance with the variables under investigation. Participants Profile shown in Table I.

TABLE I PARTICIPANTS PROFILE

Sl. No	Variable	Sample	Numbers
1	Gender	Male	207
		Female	202
2	Age	Low (below 30yr)	174
		High (above 30yr)	235
3	Educational Qualification	Graduate	149
		Post-Graduate	260
4	Type of purchasing	Online	246
		offline	163
5	Marital status	Married	290
		Unmarried	119
6	Transaction Preference of Respondents	Mobile	287
		UPI	90
		Net banking	32
		Internet banking	250
		Bank	159
		Debit card	195
		Credit card	214
7	Income (Monthly)	Low (Up to Rs.10,000)	175
		High (Above Rs.10,000)	234
Total			

Technology has completely changed the way the financial system operates. The fintech industry was created by fusing finance and technology. In terms of financial services, goods, institutions, and markets, the new sector is entirely digital. It includes digital financial advice, digital insurance, digital payments, digital investments, digital money, and digital financing. Adopting a digital economy has several benefits for service providers, customers, and governments. Increased financial inclusion helps governments because it allows marginalised people to engage in the financial system, which lowers poverty (Rodríguez-Espíndola et al., 2022). Compared to traditional models, it implies that the digital economy can increase GDP growth by an extra 6%, especially in emerging economies. When interacting with digital services, users benefit from the digital landscape by saving time and resources. Usage of e-banking Products shown in Fig. 2.

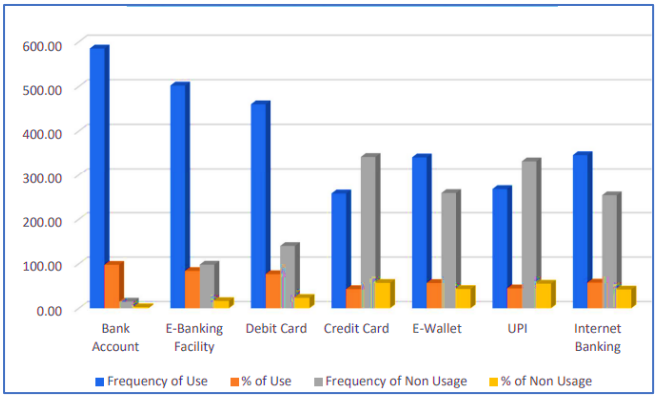

Fig. 2: Usage of e-banking Products

The data that has been supplied provides information regarding the frequency of use and non-use of a number of goods and services. Let's look at each entry separately. Monthly Frequency of Usage of Banking Services shown in Fig. 3.

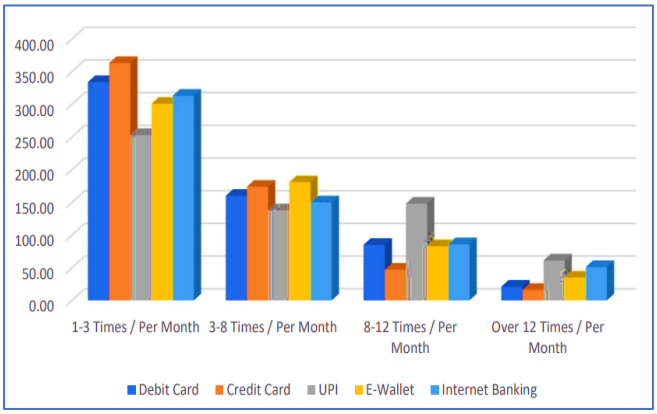

Fig. 3: Monthly Frequency of Usage of Banking Services

Based on the frequency of usage within predetermined time intervals, the data supplied illustrates the usage patterns of various products and services. Type of Transactions You Use Internet Banking Services Mostly shown in Fig. 4.

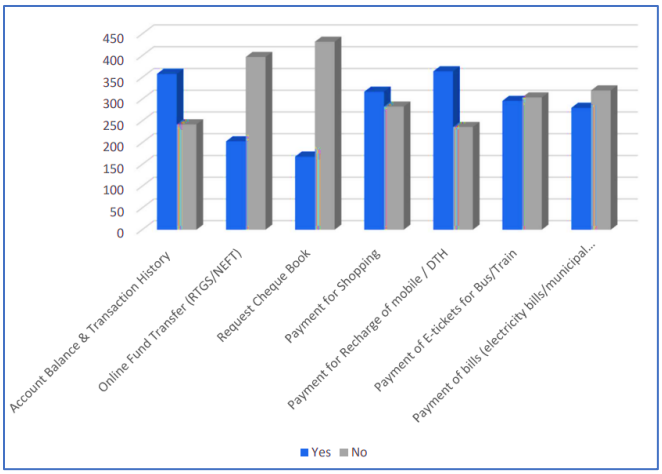

Fig. 4: Type of Transactions You Use Internet Banking Services Mostly

Information about the use of various banking services or transactions is included in the data that has been provided. Attributes of Internet Banking shown in Fig. 5.

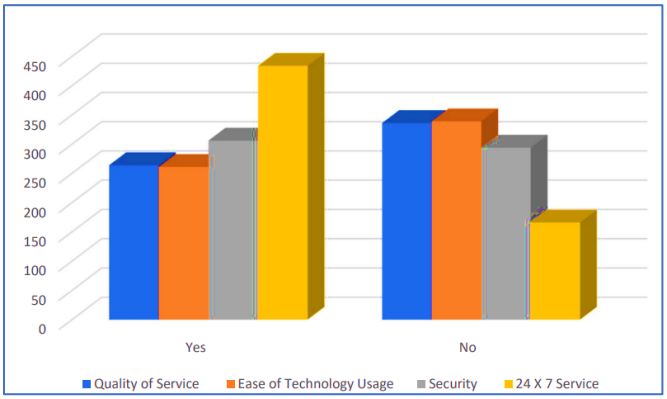

Fig. 5: Attributes of Internet Banking

Data on customer satisfaction and perception of various service characteristics are provided in the Table II.

TABLE II RELIABILITY ANALYSIS

Description	Cronbach's Alpha	N of Items	Comments
Understanding banking nature	0.916	3	Good
Implementing digital transaction	0.922	6	Good
Value creation from digital transformation	0.924	11	Good
Overall	0.900	20	Good

The overall Cronbach's Alpha index score is 0.900, which is considered to be quite good. According to the previously cited study, the Cronbach Alpha is greater than the allowable range of 0.6 to 0.7, demonstrating the validity of the data and its appropriateness for variable analysis.

The results of the investigation into the relationship between the socio-technical landscape and AI innovation in the banking industry show a significant association with regard to AI perception. Studies from the past demonstrate that this pattern has already occurred and that internal or external crises, such the 2008 financial crisis or cyberattacks, have accelerated the adoption of innovation. The results show that this will probably also apply to the adoption of AI, hence it is critical that AI be seen as essential by partners, customers, and organisations alike. The results also imply that, given AI's rapid evolution as a technology, quick and dependable communication channels are essential at the landscape level. According to earlier research, as the banking industry has become more digitally advanced, its network has grown to encompass new FinTech players, government agencies, and services. The findings also state that in order to strengthen AI systems and stay informed about the most recent cyber dangers, the industry at the network level needs to establish norms for sharing data. In conclusion, more use cases will result from emerging AI products' increased computing capabilities. These products must comply with stringent laws as well as public opinion. As a result, the success of an organisation depends not just on its ability to encourage internal AI use, but also on how well it can collaborate with its stakeholders to provide secure solutions that enhance internal processes.

V. Conclusion

The information indicates that the banking industry lacks expertise and understanding in AI and security. The employees and organisational structure of banks may not be as clearly reflecting the broad digitisation of the industry as their internal procedures, services, and goods are. The personnel is proficient in using the new AI-driven systems, but there are still gaps in their understanding of the security features unique to AI. All things considered, the industry needs to educate itself more, general employees need to know how to respond to AI, and decision-makers at all levels need to comprehend how organisational aspects need to evolve in order to effectively handle AI's rise. The research indicates that while some bank activities will become more efficient and require more time and resources, others will become more time-consuming as a result of the deployment of AI technologies. The growing need for large volumes of high-quality data will compel banks to establish new procedures for obtaining and retaining data across all divisions, which will alter staff members' perspectives on data collection and management at all levels. Therefore, decision-makers tasked with adopting AI have an obligation to fully comprehend what data, supporting processes and software, security measures, and other resources a given AI solution will demand from its environment. As demonstrated by both primary and secondary data, technology also presents excellent chances to automate manual operations, such as various screening procedures and client engagement. On the other hand, the use of AI may result in a reduction in the amount of data, procedures, and resources needed. Consequently, the decision-maker must obtain all pertinent data in order to determine whether or not AI technology will be worthwhile to employ.

References

[1] AL-Dosari, K., & Fetais, N. (2023). Risk-management framework and information-security systems for small and medium enterprises (SMES): A meta-analysis approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629.

[2] Avci, S. B. (2020). A new era in the risk management of financial firms. *Ecological, Societal, and Technological Risks and the Financial Sector*, 389-417.

[3] Boyson, S., Corsi, T. M., & Paraskevas, J. P. (2022). Defending digital supply chains: Evidence from a decade-long research program. *Technovation*, *118*, 102380. https://doi.org/10.1016/j.technovation.2021.102380

[4] Brender, N., & Markov, I. (2013). Risk perception and risk management in cloud computing: Results from a case study of Swiss companies. *International Journal of Information Management*, *33*(5), 726-733.

[5] Brockett, P. L., Golden, L. L., & Wolman, W. (2012). Enterprise cyber risk management. *Risk Management for the Future–Theory and Cases*, 319-340.

[6] Brzica, N., & Brzica, I. (2021). Managing security risks in international business. *Poslovna Izvrsnost*, *15*(2), 87-102.

[7] Bucovetchi, O., & Vevera, A. V. (2024). Perspective Chapter: Organizational Resilience toward Managing Risks in Digital Marketing. *Management in Marketing Communications*. https://doi.org/10.5772/intechopen.1004786.

[8] Chen, Y., Kumara, E. K., & Sivakumar, V. (2021). Invesitigation of finance industry on risk awareness model and digital economic growth. *Annals of Operations Research*, 1-22.

[9] Ciborra, C. (2006). Imbrication of representations: Risk and digital technologies. *Journal of Management Studies*, *43*(6), 1339-1356.

[10] Creazza, A., Colicchia, C., Spiezia, S., & Dallari, F. (2022). Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management: An International Journal*, *27*(1), 30-53.

[11] Edu, A. S., Agoyi, M., & Agozie, D. (2021). Digital security vulnerabilities and threats implications for financial institutions deploying digital technology platforms and application: FMEA and FTOPSIS analysis. *PeerJ Computer Science*, *7*, e658. https://doi.org/10.7717/peerj-cs.658.

[12] Eltweri, A., Faccia, A., Roxana Moþteanu, N., Sawan, N., & Pio Leonardo Cavaliere, L. (2020). The role of risk management in auditing e-business. *In Proceedings of the 4th International Conference on Software and e-Business*, 39-44.

[13] Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research*, *57*(3), 829-846.

[14] Kul, G., & Upadhyaya, S.J. (2015). Towards a Cyber Ontology for Insider Threats in the Financial Sector. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 6*(4), 64-85.

[15] Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. *Sustainability*, *10*(2), 440. https://doi.org/10.3390/su10020440.

[16] Luo, Y. (2022). A general framework of digitization risks in international business. *Journal of International Business Studies*, *53*(2), 344–361. https://doi.org/10.1057/s41267-021-00448-9.

[17] McClure, J., & Parkinson, A. (2017). The state of digital and social media risk management. *In Society for New Communications Research. The Conference Board*.

[18] Oleksandr, K., Viktoriya, G., Nataliia, A., Liliya, F., Oleh, O., & Maksym, M. (2024). Enhancing Economic Security through Digital Transformation in Investment Processes: Theoretical Perspectives and Methodological Approaches Integrating Environmental Sustainability. *Natural and Engineering Sciences, 9*(1), 26-45.

[19] Prabadevi, M.N., Mary Auxilia, P.A., Kabaly, P.S., & Rengarajan, V. (2024). Strategies for Leveraging Digital Libraries to Improve Financial Literacy among Rural Entrepreneurial Women. *Indian Journal of Information Sources and Services, 14*(2), 28–33. https://doi.org/10.51983/ijiss-2024.14.2.05

[20] Rami, S., Abrar, S., Mohammed, A.A., Tayseer, A., Belal, M.A., & Mahmaod, A. (2024). Assessment of Cybersecurity Risks and threats on Banking and Financial Services. *Journal of Internet Services and Information Security, 14*(3), 167-190.

[21] Rodríguez-Espíndola, O., Chowdhury, S., Dey, P. K., Albores, P., & Emrouznejad, A. (2022). Analysis of the adoption of emergent technologies for risk management in the era of digital manufacturing. *Technological Forecasting and Social Change*, *178*, 121562. https://doi.org/10.1016/j.techfore.2022.121562

[22] Thach, N. N., Hanh, H. T., Huy, D. T. N., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845-856.

[23] Tupa, J., Simota, J., & Steiner, F. (2017). Aspects of risk management implementation for Industry 4.0. *Procedia manufacturing*, *11*, 1223-1230.

[24] Yang, J., Kumar, V., Ekren, B., & Kuzmin, E. (2021). Understanding the role of digital technologies in supply chain risks management. *In Digital Transformation in Industry: Trends, Management, Strategies*, Cham: Springer International Publishing, 133-146.