Z E S Z Y T Y N A U K O W E P O L I T E C H N I K I P O Z N A Ń S K I E J
Nr 87 Organizacja i Zarządzanie 2023

Md Ferdous AHMED[*], Marek SZCZEPAŃSKI[**]

THE FACTORS DISRUPTING THE EVOLUTION OF ARTIFICIAL INTELLIGENCE IN OPERATIONAL RISK MANAGEMENT IN THE BANGLADESHI IT SECTOR – A CASE STUDY

DOI: 10.21008/j.0239-9415.2023.087.01

Despite the enormous potential and benefits of AI deployment or adoption, Bangladesh's IT sector has yet to utilize AI for operational risk management (ORM). The main purpose of this research is to identify the primary barriers to AI deployment in operational risk management, as seen by professionals at the chosen company from the IT Sector in Bangladesh, and to interpret the findings under the TOE framework (Technology-Organization-Environment Framework)**.** This study will provide a summary of the current state of artificial intelligence in operational risk management in Bangladeshi enterprises from the IT Sector, and identify the primary barriers to AI adoption in operational risk management in Bangladesh through an examination of Bangladeshi professionals' perceptions. The study's findings are determined using a quantitative approach. This article presents the findings of an online survey questionnaire conducted on IT professionals from a Bangladeshi IT organization. Results indicate that the internal culture and social components, transparency issues, insufficient financial investment, sufficient non-AI techniques, insufficient legal and ethical framework, bias, inaccuracy, feedback, and algorithm misuse are key challenges. Applying the TOE framework, the above have been classified into three categories of barriers: organizational, environmental, and technical.

Keywords: operational risk management, artificial intelligence, machine learning, IT, Bangladesh

[*] Poznań University of Technology, Faculty of Engineering Management. ORCID: 0000--0001-6722-4592.

[**] Poznań University of Technology, Faculty of Engineering Management, Institute of Logistics. ORCID: 0000-0002-8929-7490.

1. INTRODUCTION

The aim of the paper is to identify the main challenges to the integration of artificial intelligence (AI) technology, instruments, and procedures into the operational risk management (ORM) process. The main research question of this study is what are the significant impediments to the adoption of artificial intelligence in operational risk management in Bangladeshi enterprises from the IT Sector? The article is based on a literature analysis and an empirical survey conducted in chosen IT companies in Bangladesh. The justification for undertaking the research, the results of which will be presented in this article, was the identified research gap regarding the integration of AI with operational risk management processes from the perspective of management science.

This is a research issue important not only from the cognitive point of view but also from the practical point of view. From the perspective of developing Industry 4.0, the automation and digitization of selected operational risk management processes, using AI tools, becomes a necessity.

2. LITERATURE REVIEW

Operational risk is the risk of loss due to improper or inadequate internal processes, people, systems, or external events. This includes legal risks but excludes strategic and reputational concerns (Moosa, 2007). It is a type of risk that arises from the day-to-day operations of the business, rather than from financial or market risk. Operational risk is a complex and multifaceted type of risk, that can arise from a wide range of internal and external factors. The literature regarding the nature of operational risk indicates the following key points (Thompson, 2021):

1. **Broad scope**: Operational risk covers a wide range of potential losses, including those resulting from inadequate or failed internal processes, people, and systems, as well as natural disasters, cyber-attacks, and regulatory changes.
2. **Uncertainty**: Operational risk is often characterized by a high degree of uncertainty.
3. **Interconnectedness**: Operational risk can be connected with other types of risk, such as credit risk and market risk.
4. **The human factor**: Operational risk is often associated with human factors, such as human errors, misconduct, or inadequate training.
5. **Importance of controls**: Effective control and risk management practices are crucial for mitigating operational risk because they can help to identify potential issues, and prevent and limit losses.

6. **Role of culture**: Organizational culture plays also a significant role in operational risk management. A strong risk culture promotes transparency and accountability. Proactive risk management can help to prevent and mitigate operational losses.

Overall, operational risk is an important area of concern in businesses and organizations, as it can lead to significant losses, reputational damage, and legal and regulatory penalties. Effective management of operational risk requires a thorough understanding of all types of risks that can arise in a company, as well as robust internal controls, a strong risk culture, and a risk management process.

The enterprise's operational risk management encompasses defining, assessing, monitoring, mitigating, and managing risk. Each enterprise unit is directly responsible for managing its operational risk and adopting measures to minimize and manage risk to the set level by allocating the necessary resources and building an organizational culture for managing operational risk (Khan, Islam, n.d.). According to Alam (n.d.), in Bangladesh, high tech/telecom, automotive/assembly, and financial services have the highest AI adoption rates. Retail, media/entertainment, and consumer packaged goods also exhibit media adoption. In the fields of education, healthcare, and travel/tourism, AI adoption is low. Frederica and Murwaningsari (2021) demonstrated that the use of AI has little influence on the performance of banks. However, operational risk management boosted banks' performance. It was proved that implementing regulations boosted AI's effect on banking performance. The effect of operational risk management on banking performance is not comparable. To determine the amount of advancement toward the use of AI in supply chain risk management, organizations should evaluate their data collecting, storage, administration, processing, interchange, and application of risk estimation methods (Zigiene et al., 2020). Two data sources required by artificial intelligence technologies are the data on risk occurrence and the accompanying indicators used to anticipate risk events. Primarily, the use of artificial intelligence in supply chain risk management is hindered by the lack of data required to compute and then assess the probability of risk occurrence. The forms, methods, and procedures of the aforementioned data collection, storage, administration, and application reflect the nature of the obstacles associated with the application of artificial intelligence to supply chain risk management. The required data could not be acquired, saved, processed, and applied personally, in non-systematized methods and formats, and without the approval of systematized and interactive organization-wide processes. The established nature of data collecting, processing, and application dictates the constraints, difficulties, and restrictions encountered while using artificial intelligence for supply chain risk management. Limitations result from the lack of systematization in data collection, administration, and application for risk estimation along both sides of the scope. When one of the directions is not developed adequately, a variety of obstacles and limitations exist. This approach assists in identifying improvement possibilities. According to Aziz and Dowling (2018), before AI and machine learning approaches for risk management can realize their full potential, there are substantial practical concerns that must

be addressed. The availability of relevant data is the most crucial of these. The availability of trained personnel to execute these new procedures is a further concern. There are also practical concerns regarding the precision of machine learning systems. This third point is to introduce the last significant problem related to transparency and ethics that AI-driven solutions must address in greater depth. According to Arsic (2021), to minimize external losses, the adoption of artificial intelligence in operational risk management must begin with the preparation, classification, and analysis of enormous data sets, as well as performance evaluation. The core domains where machine learning algorithms may improve operational risk management are data quality assurance, text mining for data augmentation, and fraud detection. Data gathering may be aided by machine learning by more precisely identifying duplicate data entries and extreme data values (e.g., unsystematic or less probable risk identification). Machine learning may facilitate the processing and storage of the huge amounts of data necessary for risk management (e.g., internal and external data loss, internal risk indicators, macroeconomic data, etc.) Consequently, several machine learning techniques may identify individual inputs and augment the data.

According to Arsic (2021), AI can be used to devise a suitable operational risk mitigation strategy and determine whether or not to transfer or trade this risk, as well as how to do so. Utilizing artificial intelligence and machine learning in particular can enhance operational risk management. The benefits include: the reduction or elimination of time-consuming and repetitive tasks and processes (e.g., some financial institutions were able to reduce the number of processes requiring review), greater insight into data (to obtain valuable data), and easier decision-making as a result of providing both broader and more concise information. Mohammed (2020) highlighted the benefits of AI in cybersecurity, including the detection of new threats, elimination of malware, prediction of breach risks, and enhancement of endpoint security. Rapid threat analysis and mitigation are among the main benefits of cloud computing for cybersecurity. In addition, artificial intelligence can aid in the identification and classification of hazards, the direction of incident response, and the prediction of malware attacks. Artificial intelligence operations are conducted in the presence of vast quantities of data and identify patterns that may elude human observers (Soni, 2019). Artificial intelligence may play a significant role in preventing fraud: 24% of banks use AI-based solutions for cyber/IT risk analysis and 19% for cyber fraud detection and prevention (Khan et al., n.d.). It suggests that cyber security is a more expansive field where AI may be utilized extensively. According to Aziz and Dowling (2018), banks attempt to manage risk by analyzing the most effective methods for securing their systems, data, and, ultimately, customers. The ability of artificial intelligence to improve process automation enables the acceleration of routine tasks, the reduction of human error, the processing of unstructured data to filter out relevant content or negative news, and the evaluation of risky clients and networks based on the interconnections between individuals (Daniotti et al., 2020). NLP is utilized for Case-Based Reasoning (CBR) in terms of safety risk

management. CBR is an indispensable technique of risk management for construction undertakings. It emphasizes that prior knowledge and experience of incidents and dangers are extremely beneficial and may aid in averting similar risks in new situations. According to Singh and Pathak (2020) the escalation of cybercrime is a cause for grave concern as organizations expand their digital operations. Managing Internet-scale risk manually or with obsolete information technologies is difficult. Using AI technology, the majority of banks in India and some of the country's largest private banks are always able to evaluate all transactions in real time. Moreover, machine learning aids in the prevention of fraud by evaluating transactions in real-time for suspicious patterns, validating pertinent customer information for credit evaluation and providing risk analysts with suggestions for reducing risk (Fernandez, 2019). Using technology such as natural language processing and image recognition, financial institutions can automate mundane or low-value tasks (such as FAQ responses). This reduces the probability of human error, increases productivity, and reduces the cost of these duties. As a result, customer satisfaction increases as consumers receive better service (quicker response time and greater availability of services) and possibly at a lower price. In addition, due to the cost savings brought about by employment automation, it may be able to offer formerly exclusive services (such as financial counseling) to a larger audience (i.e., a larger user base). According to Leone and Porretta (2018), operational risk functions will benefit from machine learning in five areas: releasing valuable properties, obtaining deeper data insights, supporting business requirements efficiently, acquiring the skills for a more challenging task, profiting from economies of scale. Perhaps the greatest benefits of applying machine learning are the reduction or elimination of time-intensive and repetitive processes that occupy the valuable time of operational risk teams. Frequently included in these responsibilities are the accumulation, administration, and evaluation of operational risk. Several of these occupations are amenable to robotic process automation, and even modest implementations of machine learning techniques may provide substantial value in this context. By recognizing similar controls and inferring missing features in control libraries based on free-text descriptions of the control, these methods can enhance and accelerate the rationalization of control data, for example. In addition, machine learning techniques may further improve previously automated processes.

Due to their generally poor data management, expansive and complicated paperwork, and lack of well-structured benchmark and credit curve data, commercial banks provide a significant obstacle to AI applications. Certain tasks, such as passive tactics, must be partially automated to ensure successful operations (Žigienė et al., 2019). In many applications, such as prediction, it is necessary to take an extra step to properly deploy machine learning algorithms and produce accurate results, i.e., to forecast the output. This process is known as feature engineering or building. Observing a range of financial data, for instance, it would be challenging for machine learning to determine whether the investigated scenario is dangerous. In the financial area, however, this process is made simpler by the fact that inputs are often designated as Xs and outputs as Ys. Even though financial institutions are uncovering new

applications for machine learning and AI, top management might remain hesitant regarding projected investment returns. Frequently, experience with these applications is still limited, particularly in terms of operational risk. This makes it even more vital to explicitly identify their application scope and anticipated advantages. Having a convincing proof of concept and a properly defined project is likely to have a greater impact on senior management and will result in greater long-term advantages. With the rising focus on advanced analytics, more sectors are attempting to capitalize on the prospects offered by machine learning. This also means that organizations are fighting more than ever to recruit candidates with the appropriate quantitative skill set and implementation expertise.

Typically, machine learning applications demand vast quantities of data, which raises two major concerns. On the one hand, there is a concern regarding the data that may be utilized to feed algorithms. On the other hand, when it comes to consumer data, financial institutions are generally aware that they must proceed with caution. The Carvalho (2021) investigation of a series of interviews indicated a lack of investment in operational risk as well as a lack of expertise and information on the development of artificial intelligence technologies relevant to operational risk controls. As impediments to the implementation of AI systems in ORM, the respondents cited a lack of human resources competencies and a focus on other industries. According to their research, the most significant barrier to deploying AI systems in ORM may be the early age of the industry, which is still evolving, and the lack of investment in it (Singh & Pathak, 2020). There are several hurdles to the implementation of AI. Due to the increasing likelihood of internet fraud, hacking, etc., individuals still choose brick-and-mortar banking over automated technologies. The AI's trust will be severely damaged if it processes incorrect information based on deceptive data. The success of artificial intelligence is contingent on the availability of authentic data, the absence of which might render AI useless (Khan et al., n.d.). Banks confront several obstacles when integrating AI technologies. According to the study, to 71% of the respondents, the greatest obstacles to integrating AI solutions in banks are the high cost of AI solutions and the lack of local, cost-effective AI solutions. Nonetheless, 67% of respondents said that a shortage of experienced labor and an inadequate budget also hamper the use of AI in banks. Inadequate local support and service, human behavior, a secure cloud computing platform, and a dependable high-speed network channel are further obstacles.

3. METHODOLOGICAL APPROACH

3.1. Assumptions – the TOE framework

This study will utilize the TOE framework, which is a concept at the organizational level that describes how three distinct factors of a company's context impact adoption choices (Baker, 2011). The technology context, the organizational context,

and the environmental context are these three factors. All three factors are believed to impact technological innovation. According to Julies and Zuva (2021) T-O-E is a prominent framework for the three stimuli that drive organizational adoption: technology, organization, and environment. Particularly, the Technological-Organizational-Environmental (TOE) paradigm had been extensively utilized to examine the aspects that influence IT adoption. The TOE framework investigates not just the technological elements, but also their organizational and environmental settings. Therefore, this model gives a comprehensive study of all conceivable considerations. Awa et al. (2016) gained insight into IS adoption by examining how 12 elements within the technology-organization-environment (T-O-E) framework explain the adoption of enterprise resource planning (ERP) software by small and medium-sized enterprises (SMEs). Significant internal and external technologies are referred to in the context of technology. Internal technologies refer to an organization's current technologies, which limit the rate and breadth of technical development, whereas external technologies refer to newly available technologies on the market. Several aspects, including the company's size, administrative structures, and human resources, among others, form the organizational context. The environmental context in which a business operates describes the structures and regulatory environment of the relevant sector. The components of the TOE framework in AI adoption challenges in ORM are depicted in Fig. 1.

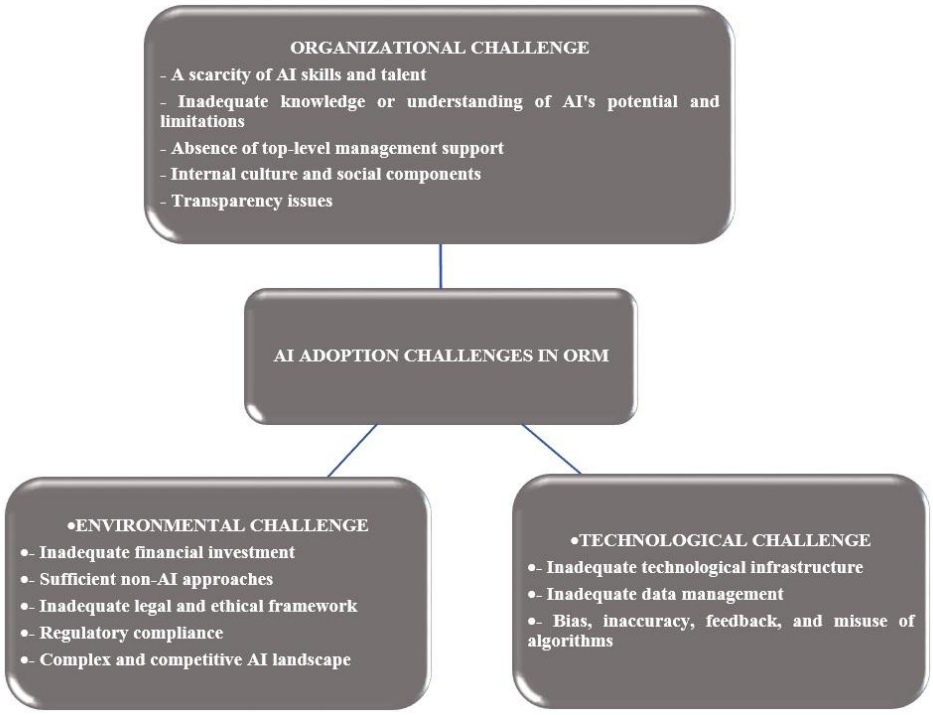


Fig. 1. AI adoption Challenges in ORM (own work)

3.2. Research approach and methods

The research's outcomes have been determined using a quantitative method. The survey questionnaire for this study was structured, and close-ended, with the majority of the questions based on the theoretical framework and a prior literature review. The online survey was conducted using a "Google Form". Through Gmail and LinkedIn, the chosen IT institution was approached to participate in this study's survey. This survey initially contacted professionals based in a well-known IT company from Dhaka. The questionnaire was sent via LinkedIn and/or Gmail to the professionals. Primary data was analyzed to ascertain the professionals' perceptions of the current state of artificial intelligence in operational risk management within the chosen company from the IT Sector in Bangladesh, as well as to ascertain the primary factors impeding AI adoption in operational risk management. The result is presented in graphical form.

This research was conducted with a medium-sized Bangladeshi private limited software firm that primarily delivers the UCAM System, an educational ERP higher education management solution utilized as an IT campus management system. This firm primarily develops Comprehensive Academic Manager software for Bangladeshi institutions, colleges, and schools. This firm now provides six types of software to twenty educational institutions in Bangladesh. The firm employs more than 103 individuals. Marketing, software development, help desk, setup center, and human resources make up the majority of this company's departments.

4. PRESENTATION OF RESEARCH RESULTS

4.1. Datasets description

The survey's overall population size is N = 103. The sample size for statistical purposes is 61 respondents. This survey has a total of fifteen attributes (values are nominal). There were 61 respondents with a confidence or trust level of 75% and a maximum error rate of 5%.

4.2. Research setup

This research was conducted on a Dell Inc. A 5559 laptop equipped with an Intel Core i7 CPU and 8 GB of RAM. The questions were listed in Microsoft Excel, and Google Forms was used to build the survey. Google Form responses were collected in a graphical format. SPSS was utilized for analysis. Google Forms and SPSS were used to create graphical representations of the results.

4.3. Results and discussion

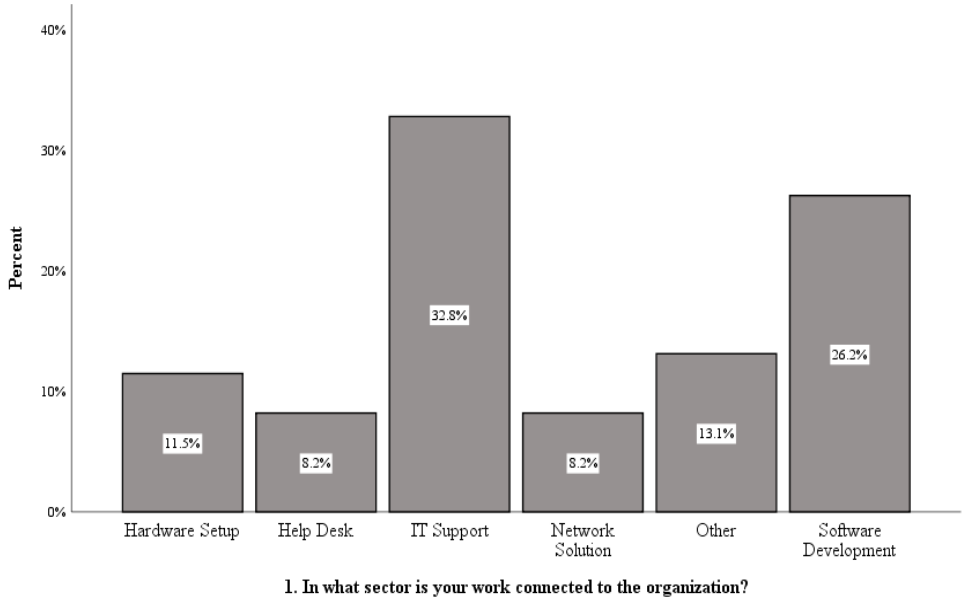


Fig. 2. Responses to Question No. 1 (own work)

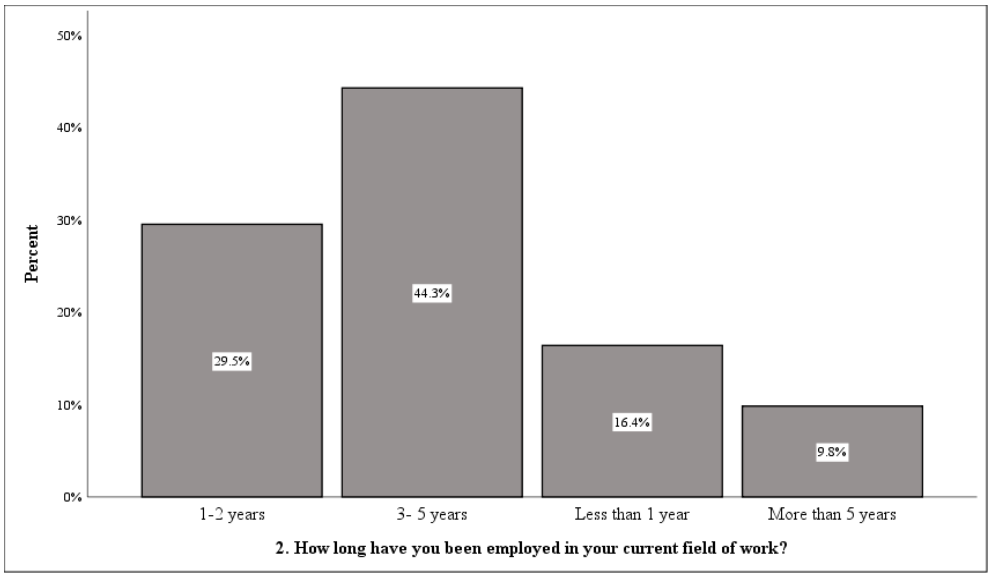


Fig. 3. Responses to Question No. 2 (own work)

As can be seen in Fig. 2, 61 respondents participated in the survey and most of the respondents were from the IT Support department (32.8%) and helpdesk (8.2%), hardware setup (11.5%) which is considered to be the Tier 1 level of an IT career. Software development (26.2%) and network solutions (8.2%) are considered to be an advanced-level profession in IT careers, therefore most of the respondents have a Tier 1 career. As can be seen in Fig. 3, most of the respondents (44.3%) are employed for 3-5 years in their current position, indicating they are skilled, aware of their role and responsibilities, and understand the strengths and weaknesses of the chosen companies. Only 9.8% are employed for more than 5 years and have the most experience in their current position.

Table 1. Participants according to the job sectors

1. In what sector is your work connected to the organization?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Hardware Setup	7	11.5	11.5	11.5
	Help Desk	5	8.2	8.2	19.7
	IT Support	20	32.8	32.8	52.5
	Network Solution	5	8.2	8.2	60.7
	Other	8	13.1	13.1	73.8
	Software Development	16	26.2	26.2	100.0
	Total	61	100.0	100.0	

Source: own work.

Table 2. Participants according to their job experience

2. How long have you been employed in your current field of work?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1-2 years	18	29.5	29.5	29.5
	3-5 years	27	44.3	44.3	73.8
	Less than 1 year	10	16.4	16.4	90.2
	More than 5 years	6	9.8	9.8	100.0
	Total	61	100.0	100.0	

Source: own work.

The participants were asked whether they understand the fundamentals of artificial intelligence. This query was posed to IT professionals to assess their AI knowledge base. According to Fig. 4. only 9.8% of 61 IT professionals responded that they have an excellent functional knowledge of AI, while 57.4% responded they have a fundamental understanding of AI. However, a significant number of IT professionals believe they are familiar with AI but lack actual knowledge. However,

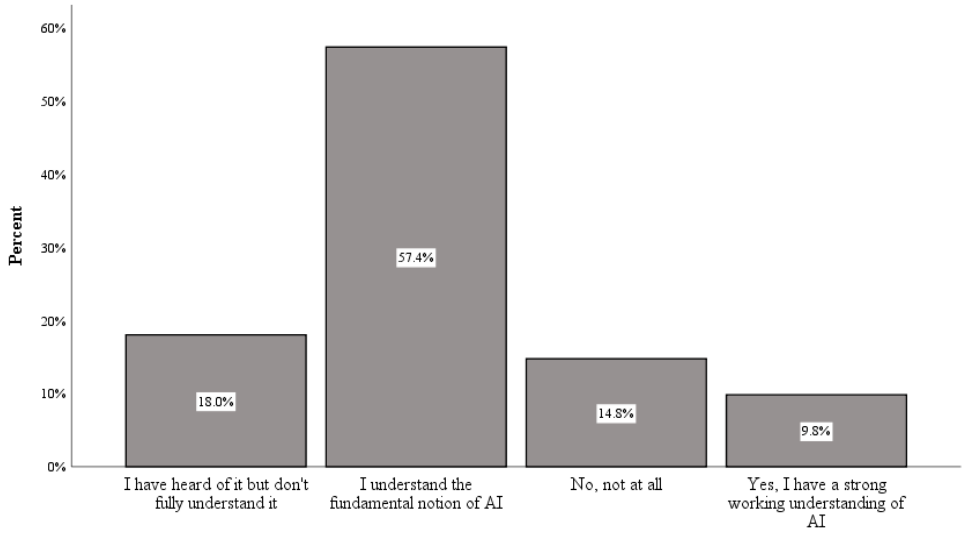


Fig. 4. Responses to Question No. 3 (own work)

14.8% of IT professionals lack even the most fundamental AI knowledge. To comprehend the participants' level of knowledge regarding artificial intelligence technology, the results of questions included in the survey are depicted in Figs. 5 and 6. According to the responses of the participants (IT professionals), the majority of participants have a basic understanding of AI. Over fifty percent of respondents are knowledgeable about machine learning, image recognition, speech and voice recognition, video recognition, robotics, neural networks, and knowledge-based systems. Of the respondents, 57.2% reported using an AI-based system or application at work. It is a positive sign that the majority of the company's systems are founded on AI, but this could also increase the risk associated with AI.

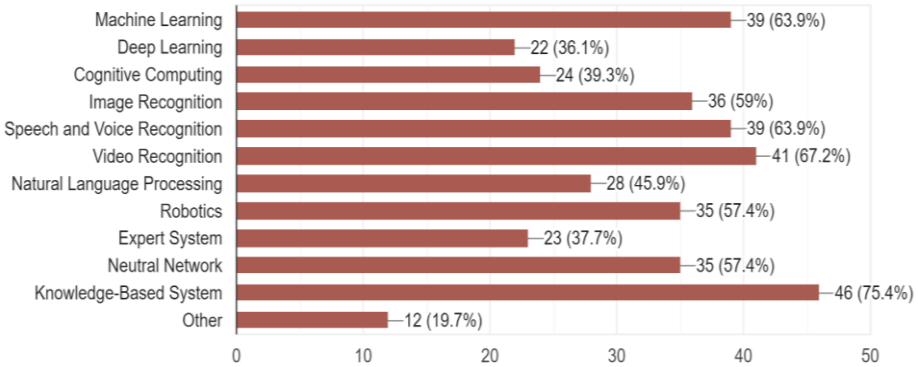


Fig. 5. Responses to Question No. 5 (own work)

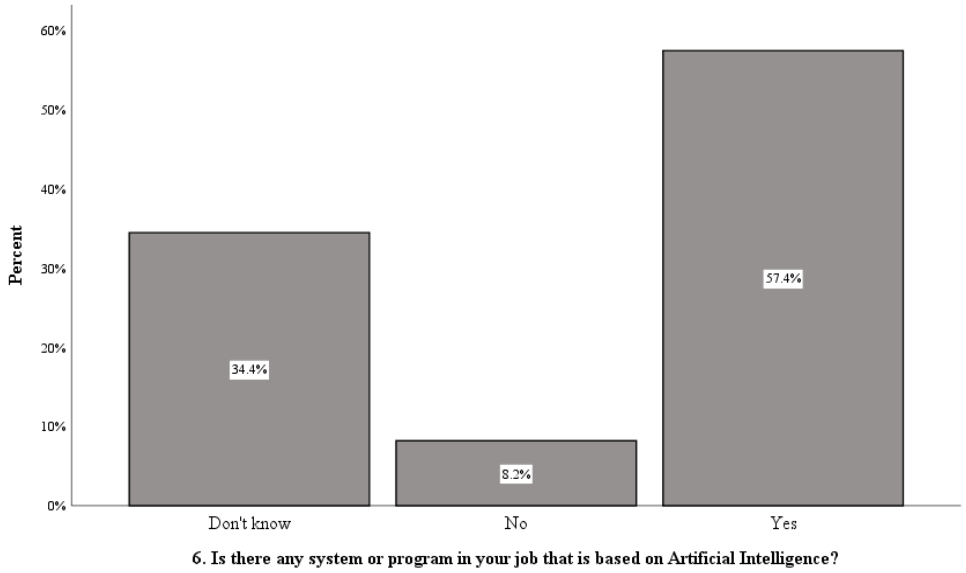


Fig. 6. Responses to Question No.6 (own work)

The participants were asked whether they comprehend the fundamentals of operational risk management. This question was posed to IT professionals to evaluate their knowledge of operational risk management. Only 27.9% of 61 IT professionals reported having outstanding functional knowledge of ORM, while 37.7% reported having a basic understanding of ORM. However, a significant number of IT professionals do not believe they are knowledgeable about ORM. Nevertheless, 9.8% of IT professionals lack even the most basic AI knowledge. The results of the survey are depicted in Figs. 8, 9 and 11 to comprehend the participants' knowledge regarding ORM and the companies' efforts to mitigate operational risk. The majority of participants (IT professionals) have a fundamental comprehension of ORM, according to their responses. The majority of respondents do not know if the organization employs an AI-based system/software/application to mitigate hazards posed by its PEOPLE/HUMANS. There may be a communication divide regarding the risk associated with people. Of the respondents, 47.5% reported that their organization employs an AI-based system/software/application to mitigate any associated PROCESS risk.

Nearly 65.6% of respondents indicated that their organization uses an AI-based system/software/application to safeguard against IT SYSTEM hazards. More than fifty percent of respondents have encountered viruses, insufficient system capacity, inappropriate data, and processing techniques.

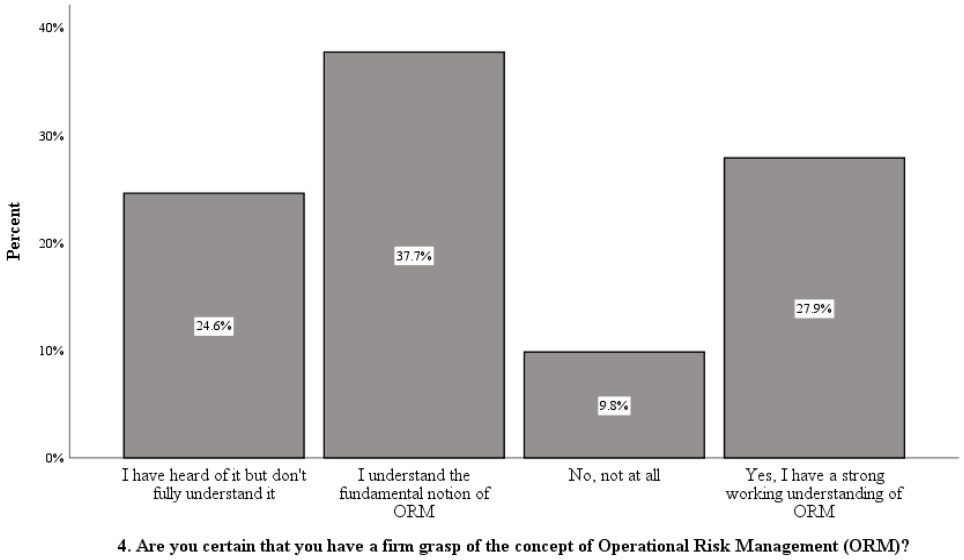


Fig. 7. Responses to Question No. 4 (own work)

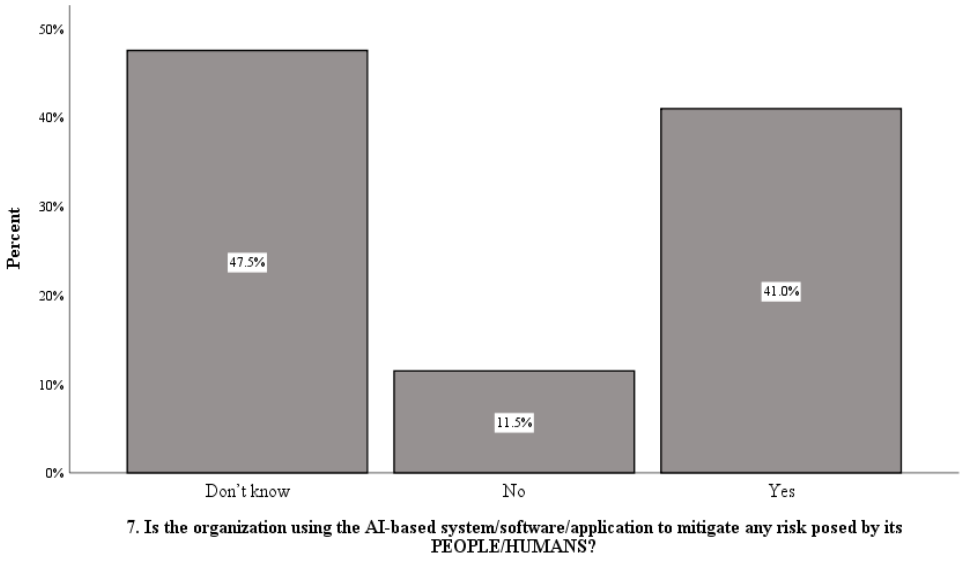
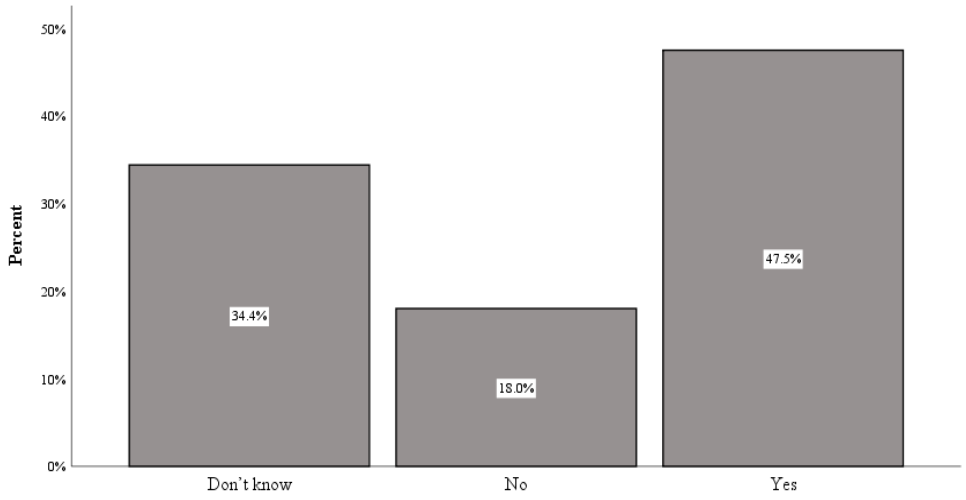
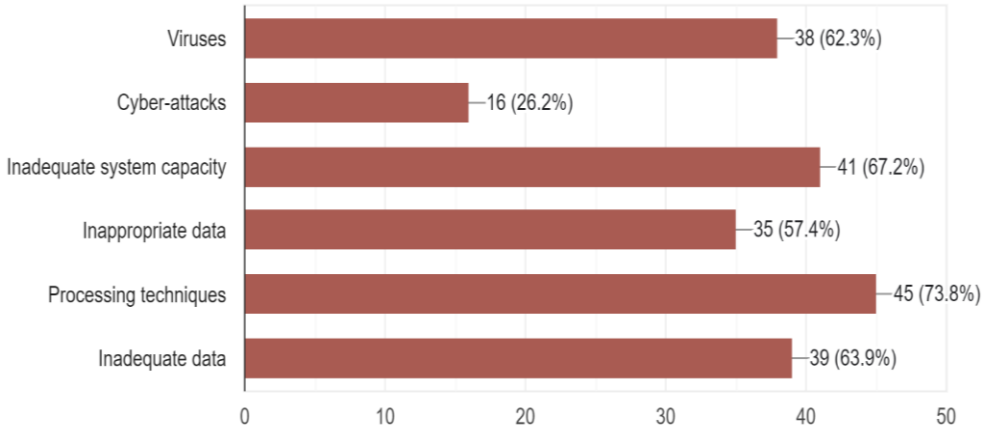


Fig. 8. Responses to Question No. 7 (own work)



8. Is the organization using the AI-based system/software/application to mitigate any risk associated with the PROCESS?

Fig. 9. Responses to Question No. 8 (own work)



9. Which IT SYSTEM risk have you encountered in your profession?

Fig. 10. Responses to Question No. 9 (own work)

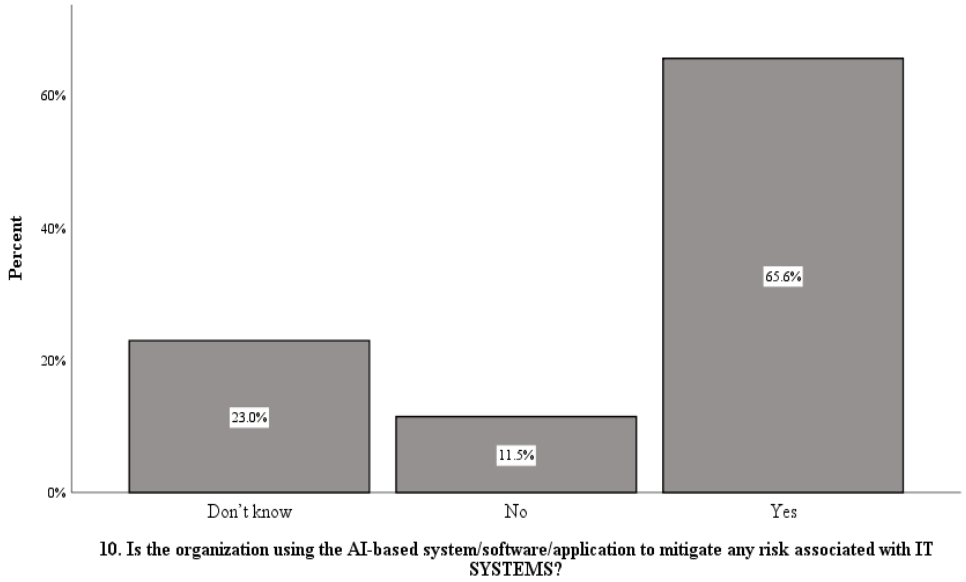
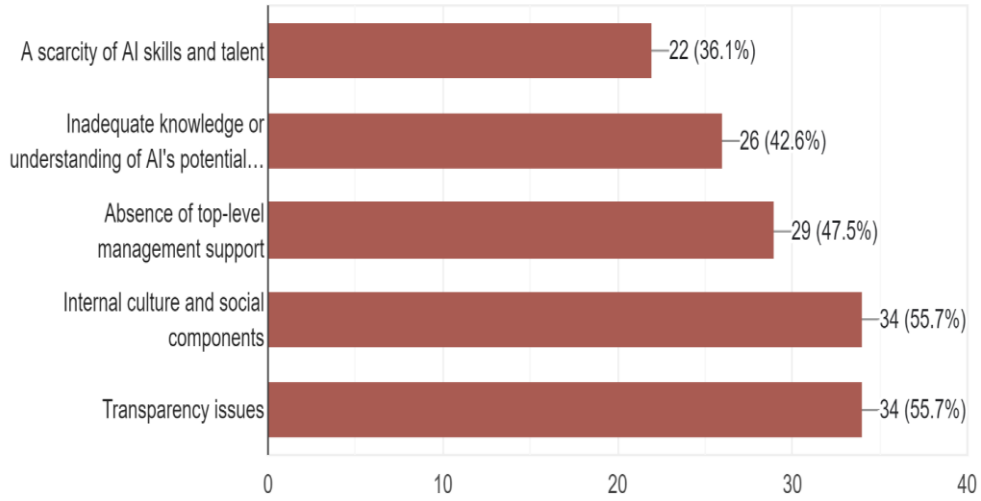


Fig. 11. Responses to Question No. 10 (own work)

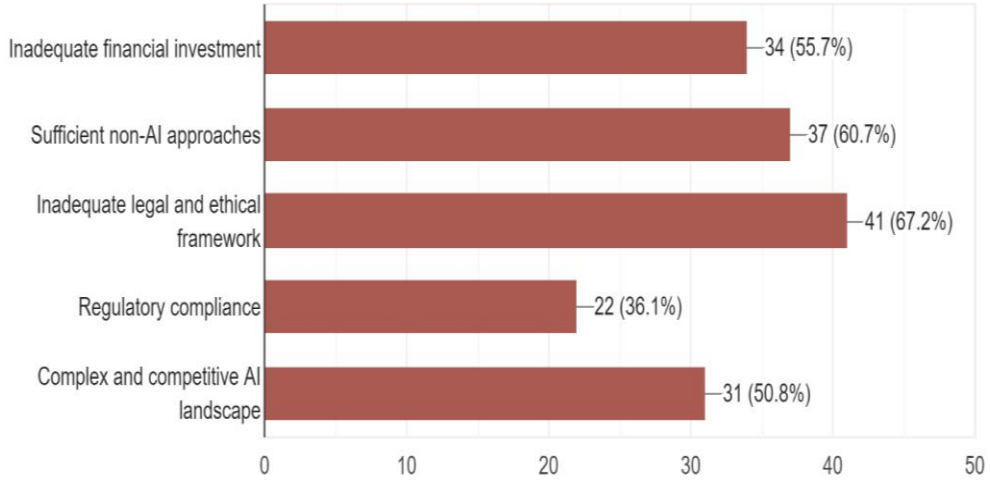
Participants (61 IT professionals) were asked to select their specific opinion regarding the greatest challenge to AI implementation in ORM in the IT Industry using a checkbox question with 13 possible answers. Identifying organizational obstacles five options were presented, as depicted in Fig. 12. To determine environmental difficulties, as shown in Fig.13, five options were presented. In Fig.14, there are three options for identifying technological challenges. The respondents indicated that internal culture and social components, transparency issues are the most significant organizational challenges when utilizing AI in an organization's operational risk management process. Insufficient financial investment, sufficient non-AI techniques, and insufficient legal and ethical framework are the most critical environmental challenges when deploying AI in the operational risk management process of the organization. Bias, inaccuracy, feedback, and algorithm misuse are the most significant technical challenges when integrating AI into the organization's operational risk management process.

The majority of respondents believe that artificial intelligence-based systems, programs, and applications pose no threat to operational risk management according to Fig. 15. When asked to explain the reasoning behind their opinion, they provided the reasons enumerated in Table 3. This demonstrates that, even though the majority of participants have a positive opinion of the capability of AI in ORM in the IT industry, it also has a negative opinion. The majority of respondents in Figure 16 are adamant that AI will have the greatest impact on how Bangladeshi IT organizations manage operational risk.



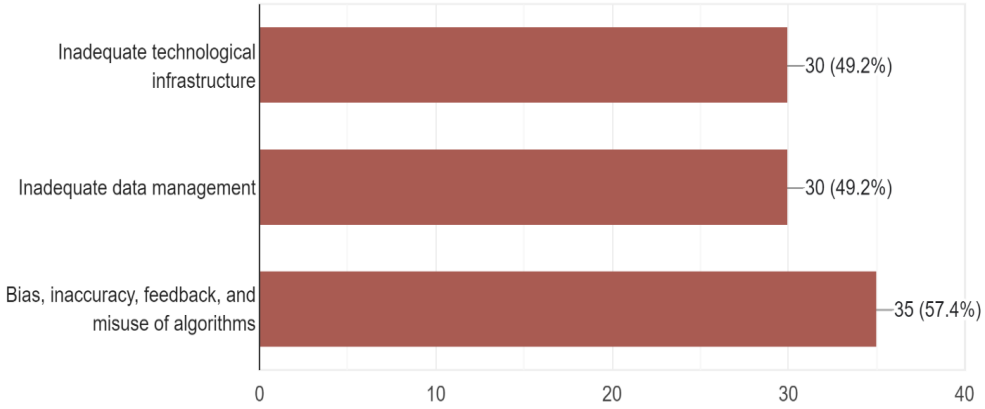
12. What are the primary organizational challenges in using AI in your organization's operational risk management process?

Fig. 12. Responses to Question No. 12 (own work)



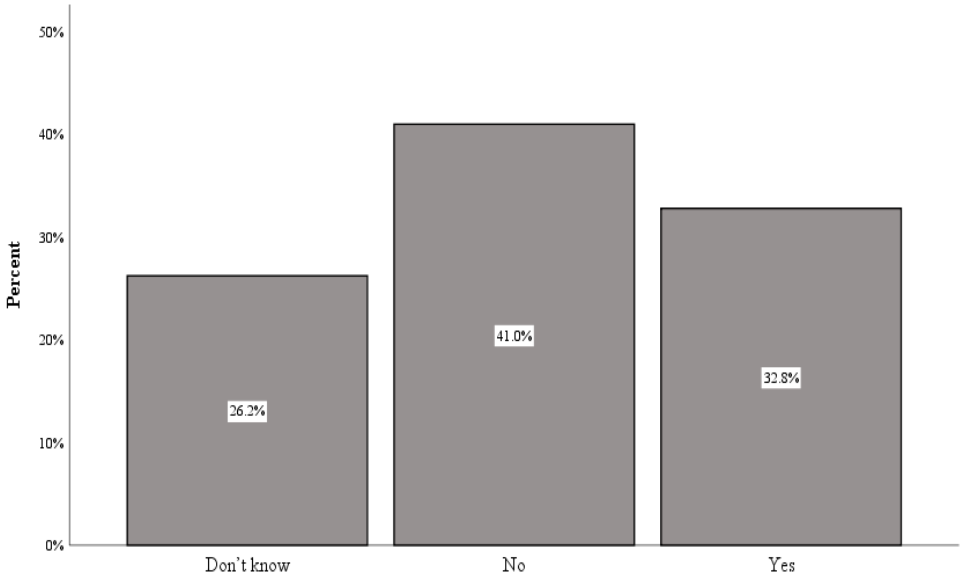
13. What are the primary environmental challenges in using AI in your organization's operational risk management process?

Fig. 13. Responses to Question No. 13 (own work)



14. What are the primary technological challenges in using AI in your organization's operational risk management process?

Fig. 14. Responses to Question No. 14 (own work)



11. Does an Artificial Intelligence-based system, program, or application pose a threat to Operational Risk Management?

Fig. 15. Responses to Question No. 11 (own work)

Table 3. Cross-tabulation of participant experience and perception of AI in ORM

2. How long have you been employed in your current field of work?
* 11. Does an artificial intelligence-based system, program, or application pose a threat to operational risk management? Cross-tabulation

			11. Does an artificial intelligence-based system, program, or application pose a threat to operational risk management?			Total
			Don't know	No	Yes	
2. How long have you been employed in your current field of work?	1-2 years	Count	2	8	8	18
		% within 2. How long have you been employed in your current field of work?	11.1%	44.4%	44.4%	100.0%
	3-5 years	Count	7	15	5	27
		% within 2. How long have you been employed in your current field of work?	25.9%	55.6%	18.5%	100.0%
	Less than 1 year	Count	7	1	2	10
		% within 2. How long have you been employed in your current field of work?	70.0%	10.0%	20.0%	100.0%
	More than 5 years	Count	0	1	5	6
		% within 2. How long have you been employed in your current field of work?	0.0%	16.7%	83.3%	100.0%
Total		Count	16	25	20	61
		% within 2. How long have you been employed in your current field of work?	26.2%	41.0%	32.8%	100.0%

Source: own work.

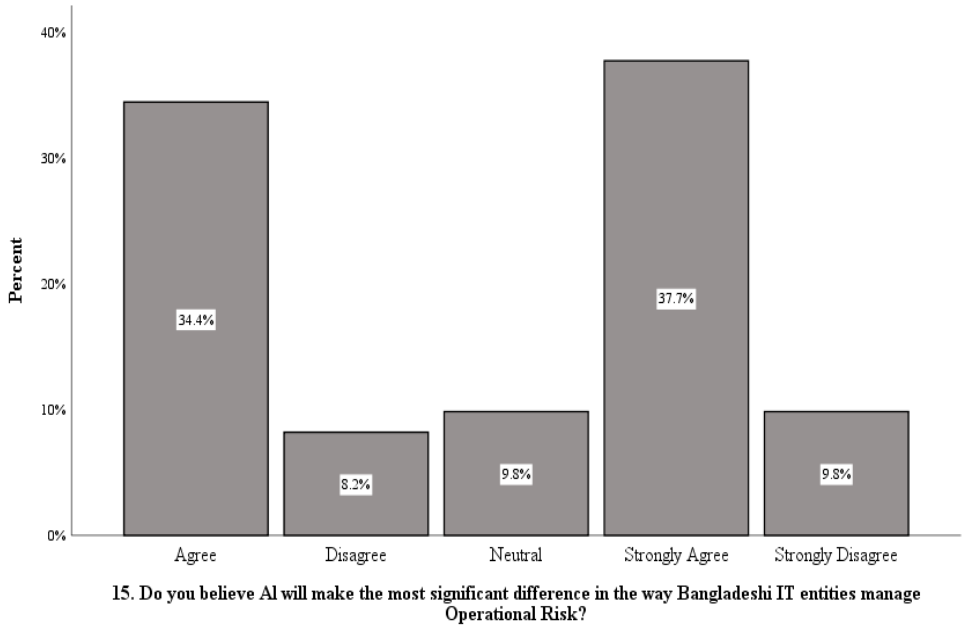


Fig. 16. Responses to Question No. 15 (own work)

5. CONCLUSIONS

The survey results provide a thorough understanding of the obstacles to AI adoption in operational risk management, as perceived by the company's professionals. The majority of staff have 3-5 years of expertise in their respective fields and rudimentary knowledge of AI technology. Few employees have a solid understanding of artificial intelligence, indicating that the organization should provide training or motivation to improve AI expertise. The majority of staff have some awareness of the ORM process. Familiarity with AI Technologies enables the intern to take the essential measures to increase domain expertise. The majority of the company's systems and software are AI-based. The majority of respondents are unaware of whether or not their business employs an AI-based system/software/application to mitigate the risks provided by its employees, indicating a communication gap in ORM. The majority of respondents are aware that their business employs an AI-based system, application, or software to mitigate any associated PROCESS risk. The majority of respondents are aware that the firm employs an AI-based system, application, or software to mitigate IT-related risks. The majority of respondents are optimistic about the application of AI in ORM. The majority of respondents are adamant that AI will have the

most influence on how IT businesses in Bangladesh manage operational risk. Viruses, inadequate system capacity, inappropriate data, and processing techniques are the most significant IT risks inside the organization. Currently, the firm employs AI-based systems/software/applications for IT system risk mitigation. Internal culture and social components, as well as transparency issues, are the most critical organizational challenges the organization has while using AI for operational risk management. Inadequate financial investment, sufficient non-AI techniques, and an inadequate legal and ethical framework are the most significant environmental challenges when adopting AI for operational risk management. The major technical challenges for incorporating AI into an organization's operational risk management process include bias, inaccuracy, feedback, and algorithm misuse.

This study has elucidated the company's present AI stance in operational risk management. The organization can give staff training and/or incentives to expand their AI skills. The organization may take the appropriate measures to reduce the obstacles to advancing AI technology in operational risk management.

This study has several limitations. The main limitation is the limited sample size, which may have affected the study's findings to some degree. Because this study was conducted on a single IT company, it cannot be generalized to comprehend and assess the obstacles that impede AI Implementation in the ORM in the Bangladeshi IT industry as a whole. Using an online survey methodology, this study focuses on a particular IT business. In the next step of this research, qualitative research using semi-structured questions may be explored to delve deeper into solutions for mitigating these AI deployment issues in Bangladesh’s IT industry.

REFERENCES

Alam, M.S. (n.d.). *National Strategy for Artificial Intelligence Bangladesh*. Retrieved from: https://www.academia.edu/44450021/National_Strategy_for_Artificial_Intelligence_Bangladesh (25.05.2023).

Arsic, V.B. (2021). Challenges of Financial Risk Management: AI Applications. *Management: Journal of Sustainable Business and Management Solutions in Emerging Economies*, 26(3), https://doi.org/10.7595/management.fon.2021.0015.

Awa, H.O., Ukoha, O., Emecheta, B.C. (2016). Using T-O-E theoretical framework to study the adoption of ERP solution. *Cogent Business & Management*, 3(1), 1196571, https://doi.org/10.1080/23311975.2016.1196571 (25.05.2023).

Aziz, S., Dowling, M. (2018). AI and Machine Learning for Risk Management. *SSRN Electronic Journal*, https://doi.org/10.2139/ssrn.3201337.

Baker, J. (2011). The Technology–Organization–Environment Framework. In: Y.K. Dwivedi, Michael R. Wade, S.L. Schneberger (Eds.), *Information Systems Theory*. Springer New York, 231-245, https://doi.org/10.1007/978-1-4419-6108-2_12.

de Carvalho, M.C.P. (2021). *The impact of artificial intelligence in operational risk management*. Retrieved from: https://repositorio.iscte-iul.pt/handle/10071/23075 (25.05.2023).

Daniotti, B., Gianinetto, M., Della Torre, S. (Eds.). (2020). *Digital Transformation of the Design, Construction and Management Processes of the Built Environment*. Springer Cham, https://doi.org/10.1007/978-3-030-33570-0.

Dogru, A.K., Keskin, B.B. (2020). AI in operations management: Applications, challenges and opportunities. *Journal of Data, Information and Management*, 2(2), 67-74, https://doi.org/10.1007/s42488-020-00023-1.

Dzhaparov, P. (2020). Application of Blockchain and Artificial Intelligence in Bank Risk Management. *Economics and Management*, 17(1), 43-57.

Ehsan, S. (2021). Artificial Intelligence and the Future of Labor Market in Bangladesh. In: A. Farazmand (Ed.), *Global Encyclopedia of Public Administration, Public Policy and Governance*. Springer Cham, https://doi.org/10.1007/978-3-319-31816-5_4359-1.

Fawcett, T., Haimowitz, I., Provost, F., Stolfo, S. (1998). AI Approaches to Fraud Detection and Risk Management. *AI Magazine*, 19(2), https://doi.org/10.1609/aimag.v19i2.1372.

Fernandez, A. (2019). Artificial Intelligence in Financial Services. Banco de Espana Article 3(19), https://doi.org/10.2139/ssrn.3366846.

Fernández-Martínez, C., Fernández, A. (2020). AI and recruiting software: Ethical and legal implications. *Paladyn, Journal of Behavioral Robotics*, 11(1), 199-216, https://doi.org/10.1515/pjbr-2020-0030.

Frederica, D., Murwaningsari, E. (2021). The Effect of the Use of Artificial Intelligence and Operational Risk Management on Banking Performance with the Implementation of Regulation as Moderation Variable. *DEGRES*, 20(1), 146-158, https://doi.org/10.1877/degres.v20i1.50.

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page Publishers.

Julies, B., Zuva, T. (2021). A Review on TAM and TOE Framework Progression and How These Models Integrate. *Advances in Science, Technology and Engineering Systems Journal*, 6(3), 137-145, https://doi.org/25046/aj060316.

Khan, A.M., Islam, R. (n.d.). *Aspects of Risk Management in Banking Sector of Bangladesh*.

Khan, S.U., Hasan, F., Islam, S., Hassan, S.M.T. (n.d.). *Artificial Intelligence in the Banking Sector of Bangladesh: Applicability and the Challenges*, 54.

Khatun, F., Nawrin, N. (2021). *Artificial Intelligence and its Impact on Information Technology (IT) Service Sector in Bangladesh*. Retrieved from: https://think-asia.org/handle/11540/14541 (25.05.2023).

Leone, P., Porretta, P. (2018). Introduction to the Work and Operational Risk. In: P. Leone, P. Porretta, M. Vellella (Eds.), *Measuring and Managing Operational Risk: An Integrated Approach*, https://doi.org/DOI/10.1007/978-3-319-69410-8_1.

Malhotra, Y. (2018). AI, Machine Learning & Deep Learning Risk Management & Controls: Beyond Deep Learning and Generative Adversarial Networks: Model Risk Management in AI, Machine Learning & Deep Learning: Princeton Presentations in AI-ML Risk Management & Control Systems (Presentation Slides). *SSRN Scholarly Paper*, 3167035, https://doi.org/DOI/10.2139/ssrn.3167035.

Mohammed, I.A. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *SSRN Electronic Journal*, 7(9), 172-176.

Moosa, I.A. (2007). *Operational Risk Management*. Palgrave Macmillan UK, https://doi.org/DOI/10.1057/9780230591486.

Mosteanu, N.R. (2020). Artificial Intelligence And Cyber Security – Face To Face with Cyber Attack – A Maltese Case of Risk Management Approach. *Ecoforum Journal*, 9(2). Retrieved from: http://www.ecoforumjournal.ro/index.php/eco/article/view/1059 (25.05.2023).

Singh, T., Pathak, N. (2020). Emerging Role of Artificial Intelligence in Indian Banking Sector. *Journal of Critical Reviews*, 7(16), 1370-1373.

Soni, V.D. (2019). Role of Artificial Intelligence in Combating Cyber Threats in Banking. *International Engineering Journal For Research & Development*. Retrieved from: https://www.academia.edu/43646442/ROLE_OF_ARTIFICIAL_INTELLIGENCE_IN_COMBATING_CYBER_THREATS_IN_BANKING (25.05.2023).

Thompson, C. (2021). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Enterprise Risk Management*. Kogan Page Ltd.

Wan Ismail, W.N.S., Mokhtar, M. (2016). Application of TOE framework in examining the factors influencing pre-and post-adoption of CAS in Malaysian SMEs. *International Journal of Information Technology and Business Management*, 49, 26-37.

Zaporowska, Z., Szczepański, M. (2022). Exploration of Lean Management Methods Used in Shared Services Centers, Drivers and Barriers to Process Selection for Improvements in the Light of Risk Management and ESG Reporting. *Sustainability*, 14(8), 4695, https://doi.org/DOI/10.3390/su14084695.

Žigienė, G., Rybakovas, E., Alzbutas, R. (2019). Artificial Intelligence Based Commercial Risk Management Framework for SMEs. *Sustainability*, 11(16), https://doi.org/DOI/10.3390/su11164501.

Zigiene, G., Rybakovas, E., Vaitkiene, R. (2020). Challenges in Applying Artificial Intelligence for Supply Chain Risk Management. *International Journal of Economics and Business Administration*, VIII, 299-318, https://doi.org/DOI/10.35808/ijeba/589.

CZYNNIKI ZAKŁÓCAJĄCE ROZWÓJ SZTUCZNEJ INTELIGENCJI W ZARZĄDZANIU RYZYKIEM OPERACYJNYM W SEKTORZE IT W BANGLADESZU – STUDIUM PRZYPADKU

Streszczenie

Pomimo niebywałego potencjału i korzyści płynących z implementacji sztucznej inteligencji w sektorze IT, Bangladesz nie zastosował jeszcze tej technologii w zarządzaniu ryzykiem operacyjnym. Podstawowym celem zaprezentowanych w tekście badań było określenie podstawowych barier uniemożliwiających wprowadzenie technologii AI w obszarze zarządzania ryzykiem operacyjnym na podstawie rozpoznań dokonanych przez przedstawicieli wybranych firm reprezentujących sektor IT w Bangladeszu. Wyniki badań zostały skonsultowane w ramach TOE (*Technology-Organization-Environment Framework*). Badanie niniejsze stanowi podsumowanie dotychczasowego wymiaru zastosowania sztucznej inteligencji w zarządzaniu ryzykiem w bangladeskich przedsiębiorstwach z branży IT. Ponadto artykuł zawiera – opartą na badaniach ankietowych, przeprowadzonych wśród przedstawicieli sektora IT z Bangladeszu – identyfikację podstawowych barier uniemożliwiających zastosowania sztucznej inteligencji w działaniach mających na celu określenie ryzyka operacyjnego. Metodologią badania

były badania ilościowe, które wykazały, iż na drodze do zastosowania sztucznej inteligencji w przestrzeni określania ryzyka operacyjnego w branży IT w Bangladeszu leży szereg problemów. Wśród nich należy wymienić: kulturę wewnętrzną zarządzania, czynniki społeczne, problemy związane z transparentnością, niewystarczające inwestycje finansowe. Ponadto wskazać należy na istnienie innych technik zarządzania, które nie wykorzystują sztucznej inteligencji. W Bangladeszu nie funkcjonują wystarczające ramy prawne i etyczne, a w przedsiębiorstwach często panuje stronniczość, niedokładność, a same algorytmy bywają używane w nieprawidłowy sposób. Wymienione kluczowe wyzwania mogą zostać przyporządkowane do trzech kategorii: barier organizacyjnych, środowiskowych oraz technicznych.

Słowa kluczowe: zarządzanie ryzykiem operacyjnym, sztuczna inteligencja, uczenie maszynowe, IT, Bangladesz

BY SA