African Journal of Inter/Multidisciplinary Studies 2025 **|** *7(1): 1-13* **|** *DOI:* https://doi.org/10.51415/ajims.v7i1.1543

RESEARCH ARTICLE:

Exploring the Risks Associated with Organisational Digitalisation in the Fourth Industrial Revolution: A Systematic Review

Elsabe Scholtz[1]

Received: 28 July 2024 **|** **Revised:** 30 June 2025 **|** **Published:** 20 August 2025

Reviewing Editor: Dr. Peggy Mthalane, Durban University of Technology

Abstract

The Fourth Industrial Revolution (4IR) ushered in the era of digitalisation, organisational transformation, and innovation of processes, strategies and operations. Integration of modern technology can provide opportunities for improvement, contributing to an organisation's productivity and efficiency, but also introduces risks that may influence organisational performance and success. To effectively integrate 4IR technology into organisational processes and functions, organisations must understand the new risks and how they can be mitigated. Despite the growing need to embrace digitalisation, the lack of clear guidelines remains challenging. This paper aims to address the gap by developing a theoretical model that identifies the risks encountered during organisational digitalisation and contributes to literature and understanding of the digitalisation risks during 4IR. A systematic literature review was conducted using four recognised databases to highlight the leading risk types that organisations face during the digitalisation of their operations. Ten risk types were identified, and a model was developed to indicate the risk items within each type and the relationships between them. This paper emphasises the importance of understanding and managing risks and adopting a comprehensive risk management approach, allowing organisations to ensure sustainable success in the digital era of the 4IR.

Keywords: *digitalisation; 4IR; risk; risk management competency; systematic literature review*

Introduction

The fourth industrial revolution (4IR) brought about the era of digitalisation, rapidly changing how the business world operates, delivers products and services and interacts with stakeholders. The revolution represented the rapid pace of technological advancements and increased complexity as technology is used within the organisation and integrated into all or most organisational activities (Alsufyani and Gill, 2022). Digitalisation influences every aspect of organisational operations, such as production, customer services, human resources and logistics. While this may result in a disruptive change, the benefits of digitalisation include increased productivity, cost reduction, customer service enhancement and decision-making capabilities (Ghadimi *et al.*, 2022; Etemadi, Van Gelder and Strozzi 2021). Prior research, consumer and business trends such as sustainability and a call to preserve the environment contribute to the pressure experienced by organisations to introduce digitalisation and digital elements. Although external pressures are felt, the organisation's specific needs for digitalisation should be clearly identified before deciding to digitalise to allow stakeholders' buy-in (Degryse, 2016). It is further pertinent that organisations realise and consider that implementing new processes, systems, and technologies also introduces new risks, uncertainty and disequilibrium, which may impact organisational design and performance (Tamvada *et al.*, 2022; de Mello and Ter-Minassian 2020; Valenduc and Vandramin, 2017) and with a lack of managerial guidelines on how organisations should digitalise, the likelihood that organisations will encounter risks increases (Fernando *et al.,* 2023; de Mello and Ter-Minassian, 2020; Birkel *et al.,* 2019; Ivanov, Dolgui and Sokolov, 2018).

Since the 18th century, technological advancements have transformed how humanity functions and became conceptually known as the Industrial Revolution. Each leap in technological advancements impacting

[1]University of South Africa, schole@unisa.ac.za | https://orcid.org/0000-0001-7849-7967

organisational and personal environments identifies a new phase of the Industrial Revolution (Britannica, 2024). The 4IR currently underway is characterised by the fusion of digital, physical, and biological systems facilitated by advanced technologies. These technologies, synonymous with the 4IR, include artificial intelligence (AI), the Internet of Things (IoT), big data, blockchain, and robotics (Ross and Mynard, 2021). 4IR is driving operational and production changes and altering how humanity interacts with one another. The scale and pace with which changes of the 4IR occur are also unprecedented, requiring society to instantly adapt to a world more interconnected and technologically advanced than before (Schwab, 2025; Ross and Mynard, 2021). The concept of digitalisation, particularly in the context of 4IR, has become a transformative force reshaping industries, societies, and economies worldwide (Alsufyani and Gill, 2022). Digitalisation includes adopting technology and fundamentally changing organisational strategy, processes, systems, and knowledge. It can be an opportunity to improve processes, enhance competitiveness or create new organisations (Schwab, 2016). Digitalisation requires strategists to develop a 'digital vision' capturing the digitalisation plan and expected results (Birkel *et al*., 2019); however, as sound digitalisation managerial guidelines are wanting, organisations are left exposed to risks that accompany the digitalisation process (Tamvada *et al*., 2022; de Mello and Ter-Minassian, 2020; Valenduc and Vandramin, 2017). Therefore, a risk management strategy should supplement the 'digital vision'. Managing risks encompasses planning, identifying, analysing, response planning, monitoring, and control (Aghimien *et al*., 2020). Understanding and managing the risks can allow organisations to develop competency in the digitalisation era (Strang and Vajjhala, 2022), contributing to organisational success and performance. A model is, therefore, imperative to understand the inherent risks of digitalising within an organisation so that policies and plans can be shaped to accommodate and mitigate these risks.

The study, therefore, aims to answer the research problem relating to the risks experienced during the adoption or implementation process of digitalisation, which negatively affects organisational operations and possibly its success. The paper aims to develop a theoretical model based on previous literature identifying these risks and showing the relationship between types of risks experienced during digitalisation in the 4IR.

Methodology

This research study used a systematic literature review (SLR) as a data collection method, allowing for a structured, systematic, and reproducible approach to summarising relevant literature (Munn *et al.,* 2018; Tranfield, Denyer and Smart, 2018). The SLR was guided by the study's research problem on the risks and challenges of digitalisation in the 4IR.

The guidelines of systematic review methodology posed by Tranfield *et al.* (2018) were used in this research together with the PRISMA Guidelines (2020). The SLR made use of four recognised databases (EBSCOhost, Scopus, Web of Science, ABI/Inform Complete) to search for academic literature on risks or challenges management experience during digitalisation adoption so that organisations can create a risk management competency within the era of digitisation and the 4IR. Only articles published from 2019 onward were included in the search. The rationale for excluding articles before 2019 was twofold. The first was to ensure the inclusion of the latest technological advancements since the conception of the 4IR. From 2018 onward, digitalisation and technological advancements such as AI, big data and automation were accelerated. Including only data from 2019 ensured relevant information regarding digitalisation was included, and information focussing on earlier revolutionary changes was curtailed. Secondly, as the 4IR progressed, new challenges and risks associated with digitalisation became apparent within organisations. Again, including information from articles published in 2019 onward ensured a better reflection of current organisational concerns. Based on the identified risks, a theoretical model was developed highlighting the relationship between different risk types of 4IR digitalisation. Key search terms were determined to define the search strings to be used. The search strategy used Boolean operators and included the search terms in Table 1.

Table 1: Search strings used

Digitalisation*	AND	Risk	AND / OR	Industry 4.0
Digitalise*		Risk management		4IR
Digital transformation		Challenge*		Technological revolution
Technology adoption		Threat*		Fourth Industrial Revolution
		Danger*		Automation revolution
		Vulnerability*		

To limit the large amount of literature, the search was limited to "validated knowledge" (Crossan and Apaydin, 2010), ensuring only peer-reviewed or scholarly articles were included. The search was narrowed further within each database using the filters indicated in Table 2.

Table 2: Database filters applied during the search

ABI/Inform Complete	EBSCOHOST	SABINET African Journals	Web of Science
Document title and abstract, full-text, peer-reviewed. Source type: scholarly journals. Document type: articles. Language: English. Published since 2019 **285 results**	Databases selected: Academic Search Ultimate; Africa Wide Information; Business Source Search in all fields. Full-text, peer-reviewed. Publication type: Academic journal. Document type: Article Language: English Published since 2019 **115 results**	Search: Anywhere. Language: English. Collection: Business and Finance Exclude calls for papers and trade magazine publications. Published since 2019 **310 results**	Search Topic (title, abstract, keyword). Document type: Article. Published since 2019 **360 results**

The search provided 1070 articles exported to the Mendeley reference management software. Using this software, duplicate entries were identified and excluded (n=1012). During the first pass review, the researcher excluded research titles irrelevant to the study (n=364). Articles were excluded based on their titles if they did not contain any search terms of the study and did not relate to the concepts researched in the study. Examples are articles regarding the quadruple helix model and sustainability and the 4th IR. Articles were also excluded if keywords were used in a context different from the one intended in the study. Terms such as digitisation, Internet of Things, emergent technologies, implementation, or competency were included pending the second pass review. A second pass review was conducted whereby the researchers analysed the abstracts of articles found relevant during the first pass review. Again, articles were excluded if it was found that the content did not apply to the current study. Although keywords were present in the title of some articles, the focus or context was irrelevant to the study and would not provide much value in developing the theoretical model. Most articles were excluded as they regarded positive iterations regarding the implementation of digitalisation with key success factors, organisational resilience, and efficiency researched, to name a few.

However, the study's viewpoint was focused on the risks of implementation, which is considered more of a negative narrative. Other articles had the view of implementing digitalisation but did not focus on challenges, barriers, or risks in implementation. Further examples of these excluded topics comprise organisational readiness for digitalisation, administration of information in a digitalised era, education in the 4IR or manufacturing of products. A full-text analysis was conducted on the articles remaining post-second pass review (n=21). After full-text analysis, four articles were excluded. First, an article was excluded as it did not speak to challenges or risks experienced due to digitalisation adoption but rather an ontology for the 4IR, which is not the focus of the study (n=20). Another article was excluded as it did not discuss the risks and challenges of adopting digitalisation in the 4IR but how digital risk management can assist in instances such as the COVID-19 pandemic (n=19). A third article was excluded as it focused on improving process safety and environmental impacts of 4IR but again did not discuss any risks or challenges associated with digitalisation (n=18). The final article was excluded as it discussed IoT adoption and project typology (n=17). The remaining 17 articles were included in the data analysis process. Figure 1 consists of a summary of the search process as a flow diagram.

To ensure transparency in the full-text analysis, the documents were loaded onto the Atlas.ti (v23) qualitative data analysis software to be coded and analysed. Inductive descriptive coding was used to organise the data meaningfully and produce themes. The researcher used a manifest approach, interpreting the literature as stated in the articles with no underlying interpretations. Upon concluding the first-cycle coding methods, 47 codes were identified. Thereafter, eclectic coding was performed to refine the coding, resulting in 10 code groups. These code groups were named risk types that occur during the digitalisation of organisations.

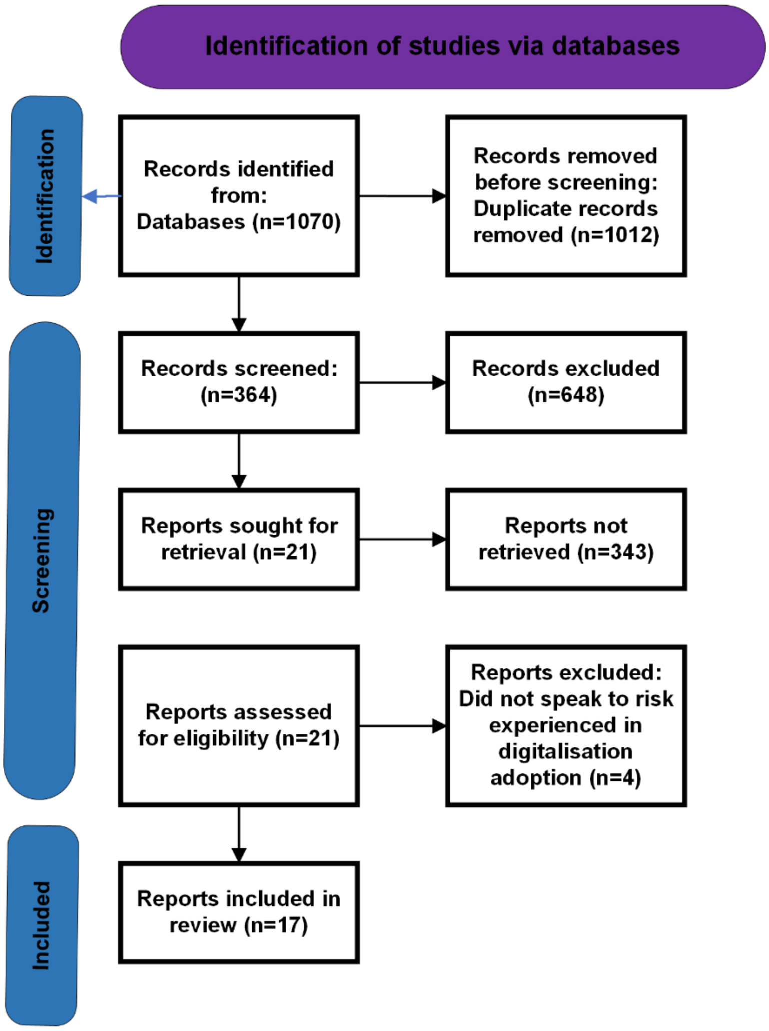
Identification of studies via databases
Identification
Screening
Included
Records identified from: Databases (n=1070)
Records removed before screening: Duplicate records removed (n=1012)
Records screened: (n=364)
Records excluded (n=648)
Reports sought for retrieval (n=21)
Reports not retrieved (n=343)
Reports assessed for eligibility (n=21)
Reports excluded: Did not speak to risk experienced in digitalisation adoption (n=4)
Reports included in review (n=17)

Figure 1: Systematic review flow diagram

After coding the documents, a code-document analysis was conducted to determine which articles identified which risk type. The result of this analysis is summarised in Table 3 and reviewed in the discussion section. Following the code-document analysis, a co-occurrence analysis was conducted to determine whether a relationship exists between the main risk types. Based on this analysis, a theoretical model was developed. The model is depicted in Figure 2 and shows the risk items within each risk type and the relationships among the risk types. A further discussion can be found in the results section.

Findings and Discussion

The systematic literature review identified ten risk types (as indicated in Table 3 and Figure 2). The code-document analysis shows that the ten risk types are discussed across the analysed articles. Technological and Social risks were identified as the most discussed among the articles, indicating their importance and the many times these risks occurred within research. Strategic, logistics, operational, and legal risk types are discussed often. While these risk types can be regarded as more visible in the study, it is not to say that these risks will increase the risk of unsuccessful digitalisation adoption more than risk types less discussed. Each risk type should be considered significant, with mitigating each possible risk a vital aspect of digitalisation.

Figure 2 depicts the ten identified risk types, the risk items included within each type, and the relationships among the risk types. In this section, each risk type will be discussed.

Table 3: Summary of code-document analysis

	Data and Storage	**Ecological**	**Financial**	**Integration**	**Legal**	**Logistics and Operational**	**Security**	**Social**	**Strategic**	**Technological**
Aviles-Sacoto *et al*., 2019			√					√		√
Birkel *et al*., 2019	√	√	√		√	√	√	√	√	√
Dixit and Verma 2022	√		√	√	√	√	√	√	√	√
Etemadi *et al*., 2021		√			√	√	√		√	√
Fernando *et al*., 2023			√		√	√	√	√	√	√
Gadekar *et al*., 2022	√	√	√		√	√	√	√	√	√
Ghadimi *et al*., 2022	√		√	√	√	√		√	√	√
Herceg *et al*., 2020			√	√		√		√	√	√
Jain *et al*., 2023			√		√	√	√	√	√	√
Javaid *et al*., 2022				√	√	√		√	√	√
Karadayi-Usta 2020						√		√	√	√
Machado *et al*., 2021	√		√		√	√	√	√	√	√
Popescu *et al*., 2020					√			√		√
Rodriquez-Espindola *et al*., 2022			√	√	√	√	√	√	√	√
Blose and Okeke-Uzodike 2020								√		
Tamvada *et al*., 2022		√	√		√	√	√	√	√	√
Virmani *et al*., 2023					√	√	√	√	√	√

Strategy risk

Strategic risk can be seen as failing to reconstitute strategic priorities regarding the 4IR. Organisations require developing a digital strategy to take full advantage of the benefits of 4IR. This could require revision of the business model concerning the architecture, structure, strategic focus, and priorities, fundamentally changing how the organisation functions. Classical planning and management philosophies should be replaced with a decentralised organisational architecture (Dixit and Verma, 2022; Birkel *et al.,* 2019). A decentralised architecture does, however, require increased communication processes between departments, posing a social risk for the organisation. There is also a risk in strategic alignment between organisational priorities and technological needs, which could affect the success of the organisation's intent (Rodriquez-Espindola *et al.,* 2022). Implementing a new business model brings a lot of uncertainty, which could increase organisational resistance and interruptions to the established logistics and operational processes (Ghadimi *et al.,* 2022). Data-driven business models also require expertise, which may be lacking in some organisations. This will require outsourcing tasks or reskilling of staff, which could be costly and increase organisational resistance (Ghadimi *et al.,* 2022). While digitalisation adoption already comes at a high cost, it is undetermined whether an even higher investment, with outsourcing, reskilling, or additional expenditure in terms of integration, will mean better success for the organisation (Ghadimi *et al.,* 2022; Birkel *et al.,* 2019). Uncertainty about digitalisation implementation is heightened for models, such as the digitalised business model, that have not been extensively tested in numerous organisational contexts and for which implementation guidelines and standards are not readily available (Fernando *et al.,* 2023; Birkel *et al.,* 2019). Further, technology is uncertain (Birkel *et al.,* 2019), complicating digitalisation. However, the risk of incorporating 4IR technology in organisational processes increases as process complexities increase.

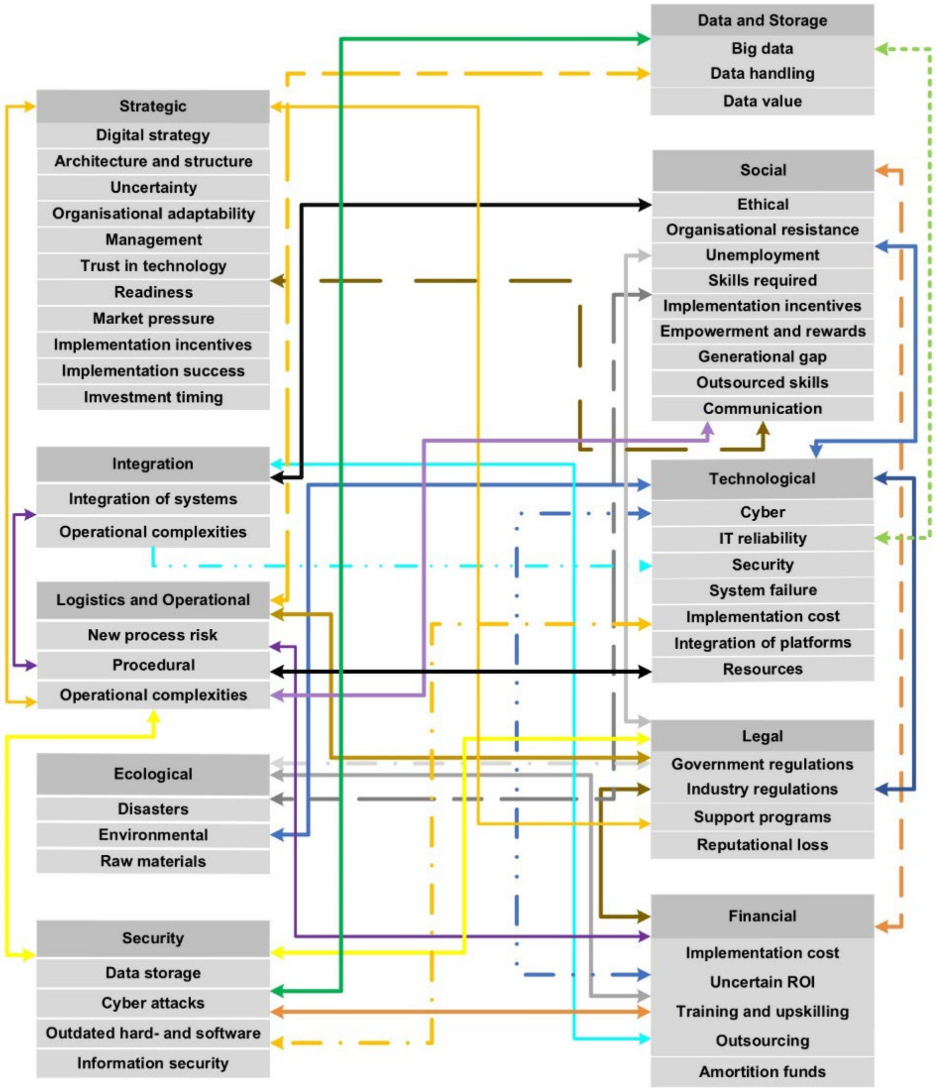

Figure 2: Theoretical model of ten risk types and their relationships

Many organisational processes also function across entities in the value chain, which require additional integration of technological platforms, which may be difficult (Dixit and Verma, 2022). In the manufacturing industry specifically, integration will be of more significant concern as incorporation is needed between mechanical and technical systems across numerous stakeholders within a supply chain (Birkel *et al.,* 2019). Strategically, implementing digitalised systems could improve organisational adaptability regarding environmental changes and customer wants (Birkel *et al.*, 2019). These environmental changes are, however, difficult to predict, and organisations cannot implement the correct technology and use it effectively, which might run considerable risks in terms of adaptability and the organisation's success (Birkel *et al.*, 2019). However, this requires strategic planning and commitment from management and employees to implement the new business model successfully. Fernando *et al.* (2023) indicate that managers often do not understand the strategic value of digitalisation, which could be detrimental to the success of digitalisation implementation. Management thinking, planning skills and practices should be adapted to the digitalised organisation (Fernando *et al.,* 2023; Tamvada *et al.,* 2022). New skills should be adopted to not only support staff through the implementation of technology (Tamvada *et al.*, 2022; Herceg *et al.,* 2020) but also take full advantage of the competencies and abilities digitalisation could provide the organisation with.

With all new technology, there is an element of distrust, which increases implementation risk. This distrust, coupled with a lack of guidelines, policies and regulations for implementation, could pose a significant risk to organisations. Trust in technology further relates to the reliability of information captured and the safety and security thereof. In digitalised organisations, data is often stored and managed by a central authority, which should be fully trusted to protect the information and maintain accessibility (Etemadi *et al.,* 2021). Organisations should be on guard to not only digitalise their organisation due to market pressures or customer wants (Rodriquez-Espindola *et al.,* 2022; Birkel *et al.,* 2019) but ensure readiness for implementation (Rodriquez-Espindola *et al.,* 2022; Etemadi *et al.,* 2021). Readiness can be seen as financial capacity, buy-in from management and employees, revision of the organisation's strategies to incorporate a digital strategy and so on. Government support could pose an additional risk as a lack of governmental infrastructure could impede the organisation's ability to digitalise successfully. The lack of governmental regulations, guidelines, and standards regarding ecological conservation and data protection could pose a further risk should future regulations impede technological implementation (Fernando *et al.,* 2023; Rodriquez-Espindola *et al.,* 2022). Few incentives are also awarded to organisations, especially in developing countries where adopting technology could harm the unskilled job market reliant on blue-collar work. Strategically, it is also essential to consider the timing of investing in digitalisation. As the cost of digitalisation could be overwhelming for organisations, and technology is ever evolving, the risk exists that by the time the funds are available, the implemented technology may have been rendered obsolete, also referred to as false investments (Ghadimi *et al*., 2022; Birkel *et al.,* 2019). The risk of late investment arises when organisations must move with trends to position themselves in the market and ensure organisational success (Birkel *et al*., 2019). With the tremendous financial investment required, the risk also exists that organisations will not know whether there will be economic benefits in implementation as the implementation and amortisation period can be long (Tamvada *et al.,* 2022).

Social risk

When changes are made within an organisation, there is always a question of the *ethical* challenges in its implementation. This is also true with digitalisation, as technology integration will significantly affect the organisation's human resources. With the implementation of new technology, there will also be a need for *new expertise* (Fernando *et al*., 2023; Virmani *et al.,* 2023; Ghadimi *et al*., 2022; Javaid *et al*., 2022; Rodriquez-Espindola *et al*., 2022; Tamvada *et al*., 2022; Herceg *et al*., 2020; Aviles-Sacoto *et al*. (2019). This poses a social risk to the organisation as employees who do not have technological skills or abilities will have to be *reskilled*, placing an additional burden on the organisation, either financially in the form of external training or in terms of productivity when implementing on-the-job training (Fernando *et al*., 2023). Besides this, it needs to be determined whether employees can adapt to the technological skills demanded (Fernando *et al*., 2023).

Many aspects of digitalising the organisational environment may cause *organisational resistance* (Fernando *et al*., 2023; Virmani *et al*., 2023; Gadekar, Sarkar and Gadekar, 2022; Ghadimi *et al*., 2022; Tamvada *et al*., 2022; Machado *et al*., 2021; Herceg *et al*., 2020; Birkel *et al*., 2019). As new skills will be needed, employees will be required to undergo training, increasing their workload and responsibilities. As the organisation becomes more digitised, changes in the working environment may also occur (Fernando *et al*., 2023). Finally, employees may fear the possible loss of jobs due to machines replacing or taking over mundane and repetitive tasks (Tamvada *et al*., 2022). These factors could all cause a rift between employees and management, as employees feel uncomfortable with the uncertainty the changes will bring. *Open communication* and transparency are required to ensure employee buy-in is obtained and kept throughout the planning and implementation of digitalisation. One of the fears causing organisational resistance is the fear of job losses or *unemployment* (Tamvada *et al*., 2022). Depending on the industry, this could be an unfortunate reality as machinery can not only replace human resources, rendering them obsolete and causing job losses, but the demand for narrow and niche skills to manage or maintain the machinery will also increase (Gadekar *et al.,* 2022; Tamvada *et al*., 2022; Birkel *et al*., 2019).

A *generational gap* is occurring in terms of customers as well as employees. Younger customers increasingly focus on product and service capabilities, while others would not want to pay the additional cost of additional features or capabilities. Therefore, implementing digitalisation might risk alienating customers who are unwilling to pay for new technologies and losing their revenue. Similarly, with employees, implementing technology that older generations do not know or experience could cause isolation of these individuals, further heightening resistance to the changes (Birkel *et al.,* 2019). Management also risks not providing sufficient support while implementing 4IR technology, which would hinder employee commitment. Support can be provided through stipulated compliance, and standards employees should adhere to as this can improve the confidence and level of information an employee has (Rodriquez-Espindola *et al*., 2022), delegating authority and empowering employees within the decentralised architecture so that quick decisions can be taken to resolve matters as they arise. Finally, employees need to be *recognised and rewarded* for achievements in implementing new processes or procedures to keep employees motivated and committed to the digitalisation strategy (Virmani *et al*., 2023). Should organisations deem the reskilling of employees as a time-consuming or costly process, *outsourcing* is another option for obtaining the niche skills needed. However, this places additional financial strain on the organisation and creates a high dependency on external partners (Birkel *et al*., 2019). With the sudden shift in technological reliance, a scarcity of IT skills exists, which places additional risk on the ability of an organisation to obtain the needed skills (Virmani *et al*., 2023; Ghadimi *et al.,* 2022; Javaid *et al*., 2022; Birkel *et al*., 2019).

Technological risk

With digitalisation adoption, new systems are implemented to conform to the digital strategy. The new systems pose *a systemic risk to organisations (*Jain *et al*., 2023) that do not possess the technical know-how and innovative engineering programs (Fernando *et al*., 2023) to ensure effective and proficient implementation. In many cases, 4IR technologies are still immature, which increases systemic risk as guidelines on implementation, expertise, and support may still be in their developmental stages (Tamvada *et al.,* 2022).

In many organisations, it is not only the technology that requires updating with digitalisation adoption but also their manufacturing sites and infrastructure to ensure sufficient IT facilities. Again, this raises the risk of unsuccessful implementation as it burdens the organisations' finances and ability to operate (Virmani *et al*., 2023). Updating *infrastructure* is also essential to ensure systems such as servers can handle the increase in data without constantly overloading the server (Dixit and Verma, 2022; Ghadimi *et al*., 2022; Birkel *et al*., 2019). A digital ecosystem should be in place to cope with the demands and operations of the new digitalised strategy (Fernando *et al*., 2023). Again, expertise is needed to ensure correct data handling and secure and reliable information management (Gadekar *et al*., 2022; Birkel *et al*., 2019). Government infrastructure could also pose a risk for digitalisation as crucial resources such as network accessibility, reliability, and electricity may be lacking (Tamvada *et al.,* 2022; Birkel *et al*., 2019). With digitalisation, organisations will be more interconnected and dependent on technology (Ghadimi *et al*., 2022; Birkel *et al*., 2019). Again, this is why updated, and sufficient infrastructure is so critical, as it will keep the organisation running and operational and, with high-speed data capturing and analysis, will allow organisations to adapt quickly to changes in customer demands. Although organisations will be more interconnected and dependent on technology after digitalisation, human error will remain a risk. This could be human resources operating the technology or experts maintaining it (Etemadi *et al*., 2021). For organisational processes that are not digitalised, human error could also affect the information stored, which could cause problems throughout the operation or production process.

With an increase in the technical complexity of system operations, the risk of *unreliable IT* could halt or reduce operations, produce lower-quality products or create a lack of accessibility or security regarding data storage. Proper platforms should be acquired to accommodate diverse technologies and applications (Dixit and Verma, 2022) across different organisational departments, ensuring cooperation between various systems and processes that are difficult to manage (Jain *et al*., 2023; Tamvada *et al*., 2022). IT interface problems could be prevented with the correct platforms and effective integration of these platforms, IT interface problems (Tamvada *et al*., 2022). Digitalisation of organisations or processes increases the data captured within that organisation. The management of this information is of utmost importance as it should always be accessible, and the s*ecurity* of the information should continuously be ensured (Gadekar *et al*. 2022; Etemadi *et al*., 2021). Cyber threats and terrorism (Etemadi *et al*., 2021) could harm the organisation in many ways. If information is made inaccessible, organisations could lose control of their operations and processes or the ability to communicate with internal and external stakeholders. Cloud deployments, where data is stored in a centralised place online, are also challenging to manage and could increase the organisation's susceptibility to cyber-attacks and terrorism (Jain *et al*., 2023). Lack of resources (Karadayi-Usta, 2020) to fully adopt and integrate technological systems and invest in the needed expertise to run and maintain the technology could pose a risk to the operations (Virmani *et al*., 2023; Tamvada *et al*., 2022). Some organisations implement digitalisation in various stages as finances permit; however, the reliability of the digitalised network will only be known when the whole system is tested as a closed system (Ghadimi *et al*., 2022).

The risk also exists that organisations *invest in technology* without knowledge of the technology required to produce the same or new products and services at the necessary quality and quantity (Fernando *et al*., 2023). Business interruption could further pose a risk to the organisation and can occur due to various reasons already discussed (Etemadi *et al*., 2021). Unreliable infrastructure and IT, human error, inaccessibility of information, and system failure could all cause a standstill in organisational operations, negatively affecting the success and profitability of the organisation.

Financial risk

For organisations to migrate from their 'as-is' state to a digitalised organisation could pose a financial risk. *High costs involve obtaining the required technology and integrating* current and new processes and technologies (Fernando *et al*., 2023; Aviles-Sacoto *et al*. 2019; Birkel *et al*., 2019). Again, integration requires skills which the organisation does not necessarily possess. The cost of outsourcing the integration and/or maintenance of technology or reskilling employees could further contribute to the financial burden that might not have been realised at the start of the digitalisation process (Fernando *et al*., 2023). Organisations could opt to implement digitalisation in stages not to put financial strain on the organisation. However, the system's reliability will only be known once implemented and integrated fully (Gadekar *et al*., 2022). Due to the long and uncertain *amortisation period* of digitalisation, the financial and economic benefits might not be known for some time after implementation (Ghadimi *et al*., 2022; Tamvada *et al*., 2022). During this period, the organisation should still be able to cover any financial expenditure and ensure the continuation of operations (Birkel *et al*., 2019). The successful implementation of digitalisation will also only be known after the amortisation period, which could mean the financial investment was unsuccessful (Ghadimi *et al*., 2022). Therefore, it is only after the amortisation period that organisations will know whether there is *return on investment* (ROI) from digitalisation (Fernando *et al*., 2023; Ghadimi *et al*., 2022; Tamvada *et al*., 2022; Birkel *et al*., 2019). Finally, with new technologies, new skills and expertise are required. If these skills are unavailable within the organisation, the organisation will need to train employees to allow them to adopt new expertise (Rodriquez-Espindola *et al*., 2022). Training will be an additional expense for an organisation to invest in above and beyond the investment in technology. Should employees not have the ability to adopt the required skills, the organisation could outsource these skills, which again will add to the financial burden (Birkel *et al*., 2019).

Integration risk

Interoperability is "the ability of two or more systems or components to exchange information and to use the information that has been exchanged" (Etemadi *et al*., 2021), which is crucial when an organisation is digitalised. Departments and sections within the organisation must be able to communicate with one another as well as external partners and stakeholders such as suppliers. Technological integration could pose a risk for organisations when processes are not unified or standardised (Fernando *et al*., 2023; Birkel *et al*., 2019). *Integration* is even more crucial in industries with increased *operational complexities* (Birkel *et al*., 2019). Failure to integrate processes and systems effectively could result in loss of revenue as there could be missing data, data inaccessible to some departments, or disruptions in operations.

Legal risk

Legal risk was regarded as regulatory or criminal risks when adopting digitalisation. The lack of overall guidelines and poor regulatory provisions on adopting digitalisation (Jain *et al*., 2023; Ghadimi *et al*., 2022; Rodriquez-Espindola *et al*., 2022; Etemadi *et al*., 2021) increases the risk of digitalisation adoption. Legal risk occurs on the organisational level as successful implementation of digitalisation is less likely to happen without clear implementation actions and standards to guide management and employees. This risk also occurs nationally as government regulations could hinder investment and funding possibilities for digitalisation but could also prevent technology implementation (Ghadimi *et al*., 2022; Rodriquez-Espindola *et al*. 2022) when considering ecological conservation. Regulatory guidance and governmental policies will also increase the ease of using employee confidence and understanding of implementation, which could decrease the risk of organisational resistance and success of implementation (Rodriquez-Espindola *et al*., 2022). The lack of regulations and policies also increases the risk of data exploitation. Cybersecurity remains a risk of digitalisation (Gadekar *et al*., 2022; Ghadimi *et al*., 2022), which, in essence, means data sharing is also a risk. Standardisation of management and security systems, along with data sharing regulations (Ghadimi *et al*., 2022), is required for data sharing to allow secure and reliable data management (Gadekar *et al*., 2022; Ghadimi *et al*., 2022). Should breaches in security arise, it could negatively affect an organisation's *reputation* (Dixit and Verma, 2022). This could be due to information stolen and distributed, placing the organisation in a bad light or causing reputation loss due to the organisation's inability to operate due to the breach. Currently, the lack of support programs does not influence the implementation risk. However, redevelopment of the current curriculum could include digitalisation skills and upskill programs (Fernando *et al*., 2023), which could decrease the risk of insufficient expertise and organisational resistance as the fear of new technology decreases.

Ecological risk

Waste and emissions are bound to increase during digitalisation. Although machinery was used within an organisation before the adoption, different technologies will be needed. This means that while some machinery can be retrofitted, there will still be waste from the existing machinery. Failing to adapt machinery to meet new needs will cause the machinery to be wasted. Further, with a greater need for technology, a greater need exists for alternative resources, such as electricity, which hurts *the environment* (Machado *et al*., 2021; Birkel *et al*., 2019). Implementation and use of digitalisation also require limited raw materials. Organisations, therefore, run the risk of unavailability or the cost of these materials as their scarcity increases, threatening technology implementation (Birkel *et al*., 2019). Customers increasingly demand customised and high-quality products, which not only require technology but also require the use of specific materials which may cause harm to the environment when disposed of (Gadekar *et al*., 2022). Customised products also decrease the ability for products to be reused or repurposed and would go to landfills. Natural and manufactured disasters such as earthquakes, hurricanes, and floods (Etemadi *et al*., 2021) could hinder the organisation's ability to operate if infrastructure or the work environment is damaged. While technology may assist in keeping the organisation operational in specific industries (where working from home is possible), organisations dependent on physical spaces and systems could be interrupted for some time during repairs.

Logistics and operational risk

With the implementation of *new systems and new processes*, it can be expected that there will be interruptions in the operation of the organisation. Business interruption and potential delays when implementing digitalisation systems will likely occur (Ghadimi *et al*., 2022; Etemadi *et al*., 2021), reducing the organisation's ability to produce products or deliver a service because of these implementation delays (Etemadi *et al*., 2021). Increasing *operational complexity* due to additional technology and integrating mechanical and technological systems (Birkel *et al*., 2019) will also increase *procedural* uncertainty and complexity. Often, no standardised policies or certification is available to specify how organisations should operate during and after adopting a digitalised strategy (Ghadimi *et al*., 2022). There is also a lack of information and communication systems that allow for existing policies and procedures to be communicated among employees (Virmani *et al*., 2023). This and the procedural and technical complexities of operation could harm an organisation's productivity and profitability. Finally, digitalisation could increase the vulnerabilities in the production process, leading to further production delays (Ghadimi *et al*., 2022).

Security risk

The most crucial consideration of security risk is information integrity risk (Jain *et al*., 2023). Organisations need an information management strategy (Rodriquez-Espindola *et al*., 2022) to ensure that the data captured daily is stored securely and can be accessed when needed (Jain *et al*., 2023). Big data is collected from sources around the organisation and external stakeholders and is then "transferred, integrated, processed, transformed and stored", comprising lengthy processes and inciting risks within each process (Gadekar *et al*., 2022). Safe and secure storage of data is therefore crucial (Birkel *et al*., 2019; Machado *et al*., 2021); however, universal standards and protocols for interfacing and networking devices to ensure security are lacking (Gadekar *et al*., 2022) create security uncertainty (Etemadi *et al*., 2021). The increase in data once an organisation digitalise is also a risk, as it may impede the organisation's functioning due to infrastructural insufficiency (Gadekar *et al*., 2022; Dixit and Verma, 2022). It is, therefore, essential to ensure that infrastructure is upgraded, preventing *outdated hardware or software* from causing operational difficulties and decreasing the security risk. Organisations, especially SMMEs, are unwilling to share information, which speaks to mistrust of the Internet and the security and accessibility of information using this channel (Fernando *et al*., 2023). It is found daunting to store information digitally for fear that their trade secrets will be discovered during a cyber-attack, and they will lose their competitive edge (Birkel *et al*., 2019). The increase in reliance on technology after the global pandemic, such as cash-less transactions and remote working policies (Jain *et al*. 2023; Tamvada *et al*., 2022), makes it difficult to stay completely offline, meaning that organisations need to incorporate technology as securely as possible. Cybercrimes are one of the most significant risks for digitalised organisations, as they can take many forms. Cyber-attacks can include malware denial-of-service attacks, device hacks, and data exploitation or sharing (Fernando *et al*., 2023; Jain *et al*., 2023; Virmani *et al*., 2023; Gadekar *et al*., 2022; Tamvada *et al*. 2022; Etemadi *et al*., 2021). Cyber protection costs money, and although awareness can be created across multiple processes and platforms, thus preventing attacks, organisations are still left vulnerable to theft by internal and external stakeholders (Tamvada *et al*., 2022).

Data and storage risk

When organisations digitalise, it should be understood that with digitalisation comes large amounts of data, referred to as *Big Data* (Dixit and Verma, 2022; Ghadimi *et al*., 2022). As all or most activities will be done using technology, this data will increase daily and needs to be stored (Ghadimi *et al*., 2022) and readily available. Data that can be collected from numerous sources will also need to be integrated, processed, and, at times, analysed (Dixit and Verma, 2022). At each stage of *data handling,* errors can occur and pose a risk to organisational operations (Gadekar *et al*., 2022). With new data and new operations, data handling competencies are crucial. The collection process and storage of the data are only meaningful if the value can be derived from the data (Ghadimi *et al*., 2022).

Conclusion

The systematic literature review identified that previous authors identified ten main risk types. Not only are there ten main risk types, but from the results, it is clear that they have an interconnected relationship as the discussions of the risk items often overlap between risk types. Adopting digitalisation in an organisation will not come quickly but considering the risks that may cause failure of implementation and finding paths to mitigate or prevent these risks from occurring could ease the organisation’s implementation journey. The study's limitations include the time frame chosen for the literature review and the limitations of the databases used. To ensure a manageable number of articles and the focus remained on the current concerns regarding organisational digitalisation within the 4IR, the literature search was conducted between 2019 and 2024. Although more than a thousand sources were identified and sorted with the four-year limitation, the study did not include any data from 2011 (the inception of the 4IR) until 2018. Excluding articles published during the early stages of the 4IR may have impacted the article’s findings as historical context, and the evolution of digitalisation risks within the 4IR may have been lost. Understanding how some risks may have evolved or been mitigated may be lacking in the article’s discussion. Another limitation of the study is the use of only four databases, excluding all other sources of information. Within these databases, sources of information were also limited to peer-reviewed articles, possibly limiting the research perspectives available.

Practical implications from the research include that organisations open themselves up to several risks during the process of digitalisation adoption, some still unfamiliar within this new era of business. However, incorporating sound risk management processes will set the organisation up for success as it aids the identification, prevention, or mitigation of consequences that may arise from digitalisation. The information in the theoretical model can help digitalised organisations or those preparing to adopt digitalisation realise the importance of risk management and how it can aid organisations in becoming more resilient. The theoretical implications encompass a contribution to the theory of digitalisation and the 4IR by providing a systematic overview of the literature concerning risks, digitalisation and the 4IR. The literature search highlighted the different risk types and their relationship, which is essential for risk management within this digitalisation era through the theoretical model's development. Future research can always be identified to further theoretical knowledge of a subject. With the 5th IR coming of age, the model for risk in the 4th IR can be repeated to include additional risks that are prevalent in technology adoption within the 5th IR. Research could also determine how to overcome the identified risk types to implement digitalisation in organisations successfully. As this study only included articles published in 2019, a more in-depth analysis can be conducted to include sources from 2011, the onset of the 4IR. Finally, the 4IR implementation is very focused on SCM. More research can be conducted in other sections of management to allow for a more complete visualisation of implementation challenges and risks for organisations. In conclusion, this study proposed a risk model based on previous literature to indicate the risks which may occur during the digitalisation process.

Declarations

Interdisciplinary Scope: The article aimed to determine the main risks organisations should consider when digitalising. This paper adopts an interdisciplinary approach to examine the strategic risks associated with digitalisation and the management of these risks. Ten types of digitalisation risks were identified, as well as the interrelationships between them.

Author Contributions: Sole authored.

Conflict of Interest: The author declares no conflict of interest related to this study.

Funding: The study was not funded by any organisation.

Availability of Data: All relevant data is included in the article.

References

Aghimien, D., Aigbavboa, C., Meno, T. and Ikuabe, M. 2020. Unravelling the Risks of Construction Digitalisation in Developing Countries. *Construction Innovation*, 21(3): 456-475.

Alsufyani, N. and Gill, A. Q. 2022. Digitalisation Performance Assessment: A Systematic Review. *Technology in Society*, 68(February): 1-18.

Aviles-Sacoto, S. V., Aviles-Gonzalez, J. F., Garcia-Reyes, H., Bermeo-Samaniego, M. C., Canizares-Jaramillo, A. K. and Izquierdo-Flores, S. N. 2019. A Glance of Industry 4.0 at Supply Chain and Inventory Management. *International Journal of Industrial Engineering – Theory Applications and Practice*, 26(4): 486-506.

Birkel, H. S., Veile, J. W., Muller, J. M., Hartmann, E. and Voigt, K. I. 2019. Development of a Risk Framework for Industry 4.0 in the Context of Sustainability for Established Manufacturers. *Sustainability*, 11(2): 384-411.

Blose, S. and Okeke-Uzodike, O. E. 2020. Pre-Fourth Industrial Revolution: Challenges for Small, Medium and Micro Enterprises in a Transforming Economy. *Journal of Contemporary Management*, 17(2): 67-90.

Britannica. 2024. Industrial Revolution. Available: https://www.britannica.com/event/Industrial-Revolution (Accessed 14 January 2025).

Crossan, M. M., and Apaydin, M. 2010. A Multi-Dimensional Framework of Organisational Innovation: A Systematic Review of the Literature. *Journal of Management Studies*, 47(6): 1154-1191.

De Mello, L. and Ter-Minassian, T. 2020. Digitalisation Challenges and Opportunities for Subnational Governments. Available: https://ideas.repec.org/s/oec/ctpaab.html (Accessed 14 January 2025).

Degryse, C. 2016. *Digitalisation of the Economy and Its Impact on Labour Markets.* Brussels: European Trade Union Institute.

Dixit, V. and Verma, P. 2022. Identification, Assessment, and Quantification of New Risks for Logistics 4.0. *International Journal of Logistics-Research and Applications*, 27(6): 1-25.

Etemadi, N., Van Gelder, P. and Strozzi, F. 2021. An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains Towards Cybersecurity. *Sustainability*, 13(9): 1-28.

Fernando, Y., Wahyuni-T, D. I. S., Gui, A., Ikhsan, R. B., Mergeresa, F. and Ganesan, Y. 2023. A Mixed-Method Study on the Barriers of Industry 4.0 Adoption in the Indonesian SMEs Manufacturing Supply Chains. *Journal of Science and Technology Policy Management*, 14(4): 678-695.

Gadekar, R., Sarkar, B. and Gadekar, A. 2022. Investigating the Relationship Among Industry 4.0 Drivers, Adoption, Risks Reduction, and Sustainable Organizational Performance in Manufacturing Industries: An Empirical Study. *Sustainable Production and Consumption*, 31: 670-692.

Ghadimi, P., Donnelly, O., Sar, K., Wang, C. and Azadnia, A. H. 2022. The Successful Implementation of Industry 4.0 in Manufacturing: An Analysis and Prioritization of Risks in Irish Industry. *Technological Forecasting and Social Change*, 175: 1–13.

Herceg, I. V., Kuc, V., Mijuskovic, V. M. and Herceg, T. 2020. Challenges and Driving Forces for Industry 4.0 Implementation. *Sustainability*, 12(10): 1-22.

Ivanov, D., Dolgui, A., and Sokolov, B. 2018. 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.

Jain, R., Kumar, S., Sood, K., Grima, S. and Rupeika-Apoga, R. 2023. A Systematic Literature Review of the Risk Landscape in Fintech. *Risks*, 11(2): 36-52.

Javaid, M., Khan, S., Haleem, A. and Rab, S. 2022. Adoption of Modern Technologies for Implementing Industry 4.0: An Integrated MCDM Approach. *Benchmarking – An International Journal*, 30(10): 1-38.

Karadayi-Usta, S. 2020. An Interpretive Structural Analysis for Industry 4.0 Adoption Challenges. *IEEE Transactions on Engineering Management*, 67(3): 973-978.

Longo, F., Mirabelli, G., Nicoletti, L. and Solina, V. 2022. An Ontology-Based, General-Purpose and Industry 4.0-Ready Architecture for Supporting the Smart Operator (Part I–Mixed Reality Case). *Journal of Manufacturing Systems*, 64: 594-612.

Machado, E., Scavarda, L. F., Caiado, R. G. G. and Thome, A. M. T. 2021. Barriers and Enablers for the Integration of Industry 4.0 and Sustainability in Supply Chains of MSMEs. *Sustainability*, 13(21): 1-31.

Munn, Z., Peters, M. D. J., Stern, C., Tufanaru, C., McArthur, A. and Aromataris, E. 2018. Systematic Review or Scoping Review? Guidance for Authors When Choosing Between a Systematic or Scoping Review Approach. *BMC Medical Research Methodology*, 18(1): 1-7.

Popescu, S., Santa, R., Teleaba, F. and Ilesan, H. 2020. A Structured Framework for Identifying Risk Sources Related to Human Resources in a 4.0 Working Environment Perspective. *Human Systems Management*, 39(4): 511-527.

PRISMA. 2020. Welcome to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Available: http://www.prisma-statement.org/?AspxAutoDetectCookieSupport=1 (Accessed 03 August 2023).

Rodriquez-Espindola, O., Cuevas-Romo, A., Chowdhury, S., Diaz-Acevedo, N., Albores, P., Despoudi, S., Malesios, C. and Dey, P. 2022. The Role of Circular Economy Principles and Sustainable-Oriented Innovation to Enhance Social, Economic and Environmental Performance: Evidence from Mexican SMEs. *International Journal of Production Economics*, 248: 1-18.

Ross, P. and Mynard, K. 2021. Towards a 4th Industrial Revolution. *Intelligent Buildings International*, 13(3): 159–161.

Schwab, K. 2016. *The Fourth Industrial Revolution*. New York: Crown Business.

Schwab, K. 2025. The Fourth Industrial Revolution. Available: https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 (Accessed 14 January 2025).

Strang, K. D. and Vajjhala, N. R. 2022. Testing Risk Management Decision Making Competency of Project Managers in a Crisis. *Journal of Modern Project Management*, 10(1): 53-71.

Tamvada, J. P., Narula, S., Audretsch, D., Puppala, H. and Kumar, A. 2022. Adopting New Technology is a Distant Dream? The Risks of Implementing Industry 4.0 in Emerging Economy SMEs. *Technological Forecasting and Social Change*, 185: 1-17.

Tranfield, D., Denyer, D. and Smart, P. 2003. Towards a Methodology for Developing Evidence-Informed Management Knowledge by Means of Systematic Review. *British Journal of Management*, 14(3): 207-222.

Valenduc, G. and Vendramin, P. 2020. Digitalisation, between Disruption and Evolution. *Transfer: European Review of Labour and Research*, 23(2): 1-14.

Virmani, N., Salve, U. R., Kumar, A. and Luthra, S. 2023. Analyzing Roadblocks of Industry 4.0 Adoption Using Graph Theory and Matrix Approach. *IEEE Transactions on Engineering Management*, 40(2): 454-463.