Electronic Markets (2025) 35:104
https://doi.org/10.1007/s12525-025-00844-1

RESEARCH PAPER

Supply chain risk management automation: A literature review

Suman Kumar Das[1] · **Marco Perona**[1]

Received: 2 August 2024 / Accepted: 23 September 2025 / Published online: 29 November 2025

Abstract
In today's highly perturbed supply chains, it is crucial to effectively manage the risk of interrupting business continuity. In recent years, an expanding body of literature has emerged on how to automate supply chain risk management (SCRM) by applying Industry 4.0 technologies. This paper provides a first systematic review of SCRM automation (SCRMA) literature. We firstly conducted a structured review of 171 papers to support a descriptive analysis, which was further narrowed to 51 papers to support our content analysis. We analyzed which of the five stages of SCRMA, namely risk detection, assessment, mitigation, monitoring, and handling, is supported by which of the nine different technology groups. Overall, it emerges that SCRMA implementation is still at a very early stage: this provides a broad range of developments to researchers, but it also suggests managers to invest carefully in those technologies that do not seem fully mature for practical utilization, yet. Finally, this review uncovers under-investigated areas in current SCRMA research and outlines promising future research directions.

Keywords Artificial Intelligence · Industry 4.0 · Literature review · Risk automation · Supply chain management · Supply risk

Introduction

A supply chain (SC) is an ecosystem of actors interacting through a set of networked processes to fulfill customers' needs (Cooper & Ellram, 1993). Supply chain management (SCM) is the coordination of the flows of goods, information, and cash within the SC. Cigolini et al. (2004) described four fundamental types of SCs, the goals they pursue, and the coordination strategies they employ. SC continuity is a SC's ability to remain in business despite disruptions: following Blos et al. (2015), it is important because it keeps the business running and also because it protects the firm's reputation.

This paper builds on the enterprise risk model proposed by the ISO 2002 norms, following which industrial risks are modelled by their occurrence probability and the magnitude of their consequences (Krolas & Krolas, 2010). This model is applied to SC risks, by considering the probability that a specific supplier interrupts its supplies and the economic damage generated. Ho et al. (2015) set a first step in SC risk management (SCRM) research by defining SC risk as "the likelihood and impact of unexpected events or conditions that adversely influence a supply chain, leading to operational, tactical, or strategic failures" and SCRM as "an inter-organizational collaborative endeavor utilizing quantitative and qualitative risk management methodologies to identify, evaluate, mitigate and monitor unexpected events or conditions."

Ivanov et al. (2019) and Ivanov and Dolgui (2021) proposed adopting a digital SC twin as a tool to manage SC disruptions. By joining modelling with real-time data, they considered that it is possible to investigate how perturbations propagate in the SC, how long a transient would take to return to the steady state, and which features can make a specific SC more resilient by design. In their view, since SC risk data are typically online and dynamic, it is limiting to shape risk-management decisions based on offline and static data and decisions. Complementing these approaches, Siemens has developed a Digital Risk Twin to simulate supply chain disruptions and assess safety and risk exposure. Through scenario modelling, the tool identifies structural vulnerabilities and supports the design of targeted mitigation strategies, thereby reinforcing supply chain robustness (Siemens,

Responsible Editor: Andrea Patrucco

✉ Marco Perona
marco.perona@unibs.it
https://www.unibs.it/it

[1] Department of Mechanical and Industrial Engineering, University of Brescia, Via Branze 38, 25123 Brescia, Italy

2025). Accordingly, the second standpoint adopted by this paper is that SCRM can be enhanced through digitalization by integrating real-time and dynamic data with predictive analytics.

Hence, digital technologies can support SCRM by enhancing operational efficiency, improving visibility, and enabling proactive decision-making through the timely capture, transfer, and analysis of information. We can narrow our focus from this broad spectrum to Industry 4.0 technologies, addressing intelligent process automation, interconnected systems, and real-time data to drive SCRM practices transformation. This synergy between Industry 4.0 and SCRM has been widely recognized by other studies (Spieske & Birkel, 2021). We call this new approach *Supply Chain Risk Management Automation* (SCRMA): in other words, SCRMA is the discipline that combines SCM, enterprise risk management (ERM), and Industry 4.0 (I4.0). SCRMA is a novel approach that promises to revolutionize SCRM, much as I4.0 changed manufacturing by linking real-time data, operations technology, and information technology.

Yet, to date, there appear to be only isolated studies that propose the automation of specific SCRM stages or explore the use of particular technologies to automate SCRM, while we lack a comprehensive and holistic overview of the knowledge accumulated to date on SCRMA, owing on the one side to the novelty of SCRMA as a research discipline and on the other on the difficulty of blending three such well-established research domains as SCM, ERM and I4.0.

Thus, in this paper, we provide a systematic literature review of SCRMA. We considered it highly relevant and appropriate to fill this gap, especially during a period in which several innovative digital technologies are rapidly developing, alongside the growing opportunity to gather extensive online data. Accordingly, this study develops a structured analysis of the extant SCRMA literature (Durach, et al., 2021; Wong, 2021; Ketchen & Craighead, 2023), by trying to answer three research questions. The first research question pursues a process view of SCRM, by asking: *which stage or activity within SCRM is most and least affected by which I4.0 technologies*? By the same token, the second research question applies a technology-oriented view: *which of the I4.0 technologies are of most use to support which stage or activity within SCRM*? Finally, the third, and main research question that guided our work is: *which is the level of maturity achieved by the implementation of I4.0 technologies to improve SCRM*?

By highlighting the transformations that I4.0 technologies are inducing in SCRM, our literature review can help identify issues on which the SCRMA body of literature is well developed and consistent, which we can address as "solved" problems, and other issues where the knowledge accumulated to date could leave space for further research either because the extant research does not fully agree or because they are under-investigated topics. Note that this paper is not aimed at deepening our understanding of specific technologies *per se*, but rather we are interested in investigating the broader contribution that I4.0 technologies as a whole can achieve for businesses in the SCRM domain.

To this purpose, the "Background" section illustrates our study's background; the "Methodology" section presents the methodology applied in this study; and the "Descriptive analysis" section presents the descriptive analysis emerging from a long list of 171 papers; the analytical description of the main empirical findings from a short list of 51 papers is then reported in the "Content-based analysis" section. The "Discussion" section discusses the main implications of our findings by answering the research questions in the light of a managerial, technological and business viewpoint. Finally, a concluding remarks section closes the paper by discussing the main takeaways and implications of our research.

Background

The idea that ERM could be applied to SC was first considered in the early years of the last century, but research in this domain started developing only in the last 25 years (Sodhi et al., 2012), on the ground of companies' expectation that their SCs' vulnerability could increase in the next years (Jüttner, 2005). A first exploratory study was proposed by Zsidisin et al. (2000) and Zsidisin (2003), who discovered that purchasing organizations often create contingency plans and implement process-improvement and buffering strategies in response to supply risks. Despite acknowledging SCRM's importance, many managers believed that their organizations were not doing enough to mitigate supply risks and disruptions.

Once SC risk's relevance was achieved, researchers set out to analyze and assess corporate risks: Hallikas et al. (2002, 2004) were among the first to discuss this. They highlighted that firms' exposure to risks generated by other firms increases with the dependency between companies. This is a possible explanation of the increase in risk perceived by companies, as confirmed by Harland et al. (2003), who highlighted that the growing complexity of supply networks is one major driver of the increase in firms' vulnerability.

The policies most suited to reduce SC risk were the next main topic investigated: for instance, Ojala and Hallikas (2006) examined what are the main risks related to investing in a network context and how to manage these risks. Micheli (2008) and Micheli et al. (2008, 2009) investigated the relation between suppliers and supply risk. They proposed a critical supplier selection approach based on a total cost profile. By the same token, Hult et al. (2010) provided evidence that options operate differently in SCs than they do in firms when facing high levels of uncertainty by using the

lens of Real Options Theory. Wagner and Bode (2006) had previously confirmed this result through a survey of German executives showing that a firm's exposure to supply risk depends on supplier selection, single vs. multiple sourcing, and global vs. local sourcing. Thun and Hoenig (2011) surveyed 67 German automotive plants, finding that firms implementing supply risk assessment tools are better off in SC performance than their peers that do not. Wang et al. (2010) confirmed that, by activating multiple sourcing, firms experience less supply risk and a more reliable SC. Overall, this body of research confirms that sourcing policies affect supply risk.

On these grounds, researchers went further to investigate if the structural characteristics of a SC have an impact on its vulnerability to risks and disruptions. Two such aspects are robustness (the capability to cope with perturbations proactively, for instance by preparing *ex-ante* contingency plans) and agility (the ability to react quickly and effectively): following Wieland and Wallenburg (2012) both are important in improving SC performance, yet while agility improves only SC's customer value, robustness has a positive effect on the firm's business performance as well. Pettit et al. (2013) were the first to define the concept of resilience: their research proposed a positive correlation between resilience and SC performance by describing hundreds of resilience levers. Furthermore, Heckmann et al. (2015) were among the first to propose quantitative SCRM approaches.

Next came the investigation of the SC risk mitigation levers' effectiveness: Wiengarten et al. (2016), through an international survey, found that supplier integration can improve SC performance and decrease risk. Another empirical study conducted with a set of Finnish firms by Hallikas and Lintukangas (2016) confirmed that supplier collaboration and integration reduce SC risk. Mishra et al. (2016) also considered inbound inventory buffering and supplier collaboration as risk mitigation levers in an empirical study of 184 Indian firms. In 2017, Revilla and Saenz examined how firms manage SC risks, confirming that firms more oriented towards inter-organizational collaboration achieve the lowest levels of SC perturbations. Overall, this research streams outlined customer–supplier collaboration's role as an effective policy to control disruptions (Shekarian & Mellat Parast, 2021).

Another fundamental contribution to SCRM research was normative and definitory: El Baz and Ruel (2021) proposed four main steps of SCRM: risk identification, assessment, mitigation, and control. They found that agility is positively connected to all four phases, while robustness only impacts risk identification and control. By the same token, Emrouznejad et al. (2023) reviewed a list of 53 literature reviews on SCRM and identified three categories of risk sources in SCs, namely environmental, network-related, and organizational. The advancements in SCRM research reported by these studies are significant; however, the rise of I4.0 demanded new approaches to manage and mitigate real-time and multi-tier risk.

One of the first contributions to SCRMA is the 2017 paper by Schlüter et al., proposing a simulation-based approach as part of creating a smart SCRM platform. They build on finite-event simulation to model the material flow and Monte-Carlo simulation to model risks. Following their analysis, the usage of cyber-physical systems (CPS) in SCRMA can lead to "the integration of technology (sensors, actuators, connectivity, analytics) along SC processes to improve risk identification, analysis, assessment, mitigation and monitoring by processing real time SC risk information." Integration of I4.0 technologies into SCM thus leads to smart SCRM, which combines multiple independent data analytics, historical data repositories, and real-time data streams. Through this embedded intelligence, SCRM moves from decision-support to predictive and ultimately to prescriptive.

Another step in SCRMA was achieved in 2018 when Ivanov et al. investigated the impact of digitalization and I4.0 on the ripple effect and disruption control analytics in the SC for the first time. Their research combines two separate analyses, namely the impact of digitalization on SCM and the impact of SCM on the ripple effect control. They analyze and discuss the overall impact of big data analytics (BDA) and advanced track and trace systems on SC disruptions and find that each of these determinants can have both beneficial and negative effects. For instance, BDA can reduce risk by improving SC visibility, while at the same time, it can increase it by exposing firms to greater coordination complexity and more severe data safety issues. Finally, Ivanov and Dolgui (2021) advocate the usage of a digital SC twin, a computerized model that can represent network states at any given time, as a significant tool to address these risks by uncovering the interrelation of risk data, disruption modelling, and SC performances.

Methodology

This study employs a four-stage systematic literature review (SLR) process to analyze the current state of SCRMA, detailed as follows:

Stage 1: *Background study*—we selected 30 highly relevant articles based on journal impact factors and citation rates to form our core literature base. The objective of this stage was to map SCRMA knowledge and synthesize key findings. This foundational step guided the following review's direction.

Stage 2: *Systematic literature review*—we employed a SLR as our primary methodology to identify and col-

lect relevant papers. SLR is widely recognized for its effectiveness in identifying, evaluating, and synthesizing pertinent literature (Tranfield et al., 2003). We utilized the PRISMA protocol to establish our research objectives (Ketchen & Craighead, 2023; Wong, 2021), as illustrated in Fig. 1. We chose the Scopus database to identify relevant studies. We then followed the three characteristic steps of the PRISMA method.

During the *identification* phase, a systematic approach was adopted to develop a comprehensive set of keywords categorized into two thematic groups. The first group focused on core concepts, including SCM, SCRM, and ERM principles. The second group encompassed keywords specific to I4.0 technologies. We adopted the I4.0 technology classification by (Frank et al., 2019; Lu, 2017; Russmann, 2015) by considering nine digital technolo-

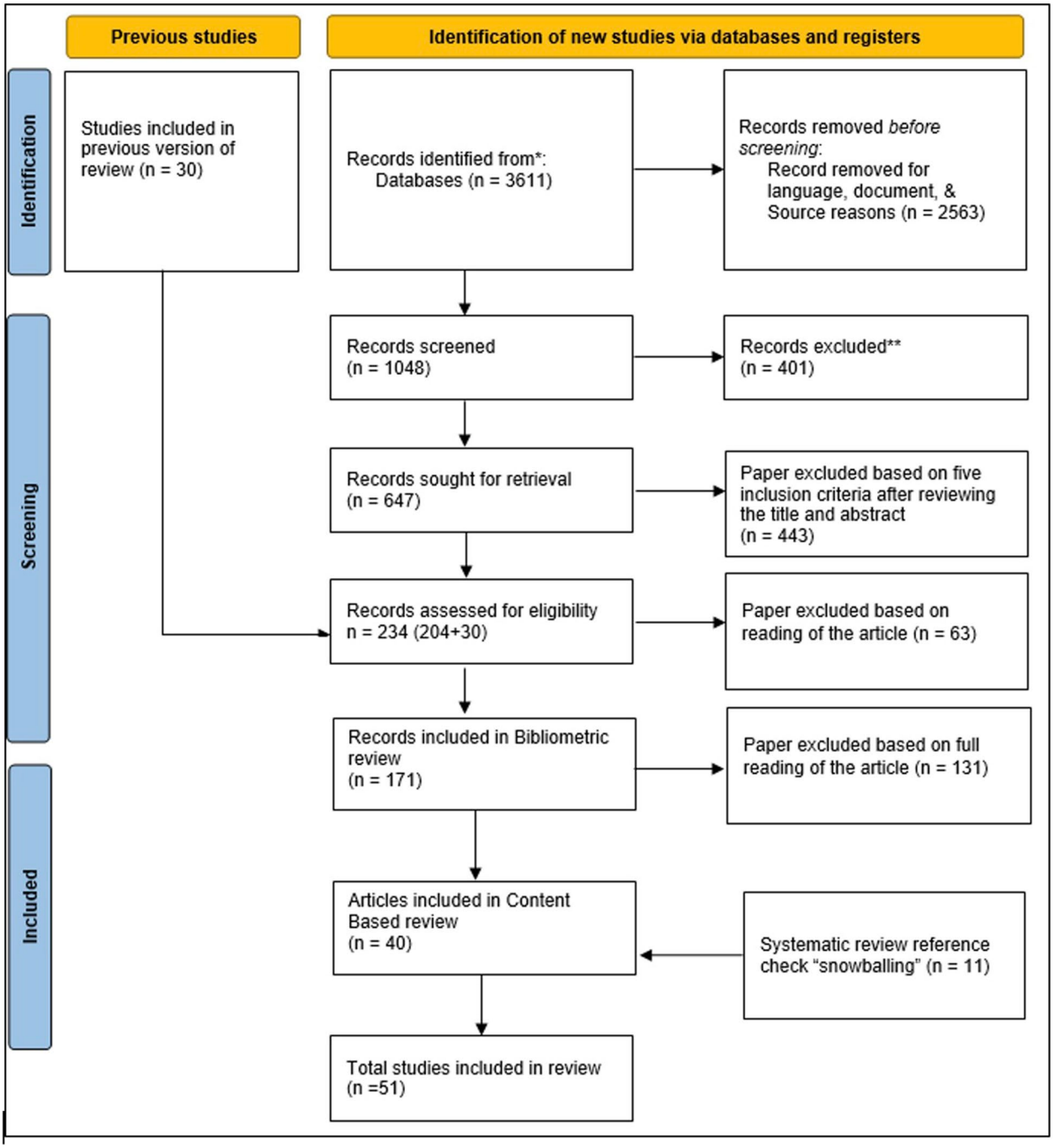

Fig. 1 PRISMA method flow diagram

gies groups, namely: Internet of Things (IoT), Big Data and Analytics (BDA), Cloud Computing (CC), Artificial Intelligence/Machine Learning (AI/ML), Additive manufacturing/3D Printing (AM), Blockchain (BC), Cyber-physical systems (CPS), Industrial Robotics (IR), and Digital Twins and simulation (DTS). These I4.0 technology groups are defined in Appendix I, and were integrated to construct the search string, as depicted in Fig. 2. The selection process was confined to peer-reviewed articles presented in academic journals and published in English between 2000 and 2023, which resulted in a total of 3611 articles.

Stage 3: *Screening for quality and relevance*—2563 papers belonging to unrelated research areas were excluded, leaving 1048 articles. Next, we reviewed the titles, removing 401 unrelated papers and retaining 647. A double-blind review process was then conducted by the two authors, who independently evaluated the abstracts and categorized each paper as "keep," "maybe," or "scrap." Only papers labelled as "double keep" were retained, resulting in the inclusion of 204 articles. Further, for the background study, 30 papers were incorporated, yielding a total of 234 relevant papers. Using again the previous "double-blind" method on the full text of the papers, the authors rejected 63 more papers, leaving 171 articles that formed the basis for our descriptive analysis below described.

Stage 4: *Refinement of selection*—we further selected articles based on the number of citations per year (as stated by SCOPUS) and the journal impact factor (as stated by WOS). This approach aligns with methodologies previously employed by Durach et al. (2021) and Shah et al. (2021). We computed the median of these two bibliometric indices across the sample of 171 papers and considered only papers and journals ranked above both medians, leading to the exclusion of 131 papers, resulting in a refined set of 40 highly relevant articles. To further ensure comprehensiveness, the "snowball" cross-referencing method was applied, incorporating 11 additional articles, culminating in a final corpus of 51 papers that formed the basis for our detailed content-based analysis below described.

Descriptive analysis

By building on the long list of 171 papers emerging from PRISMA's stage 3, we explored the trend of SCRMA papers, as shown in Fig. 3: despite its growing prominence, research in this area was rather limited until 2018.

Starting with 2019, there has been an increase in research, particularly on supplier disruption, risk mitigation, and risk assessment. Following the COVID-19 pandemic, papers per year have skyrocketed, and research has expanded to include digital technologies such as AI, ML, BDA, and DTS, accommodating concepts as resilience, recovery, learning, and disruption.

Figure 4 depicts the Pareto A class of journals that published SCRMA articles: IJPE and IJPR are by far the major contributors, with 51 papers combined. Nine out of 10 top journals and most of the others are related to operations. However, the appearance of Computers and Industrial Engineering in the top 10 means that SCRMA is attracting increasing attention from researchers in computer and decision sciences too.

Fig. 2 Keyword and inclusion criteria for PRISMA

Criteria	Description
Applied keywords for searching	("Supply chain management") AND ("Risk" or "Supply risk" or "Supply chain risk" or "Supply chain risk management") ("Internet of things" OR "Machine Learning" OR "ML" OR "AI" OR "Artificial Intelligence" OR "Cloud computing" OR "Industrial robotics" OR "Big Data analy*" OR "Additive manufacturing" OR "3D printing" OR "CPS" OR "Cyber Physical System" OR "Digital twin" OR "Block Chain" OR "Industry 4.0")
Inclusion Criteria	**1.Research should focus on supply chain risk or supply chain risk management.** **2. The research should emphasize the importance of technology, especially any industry 4.0 technology as key component.**

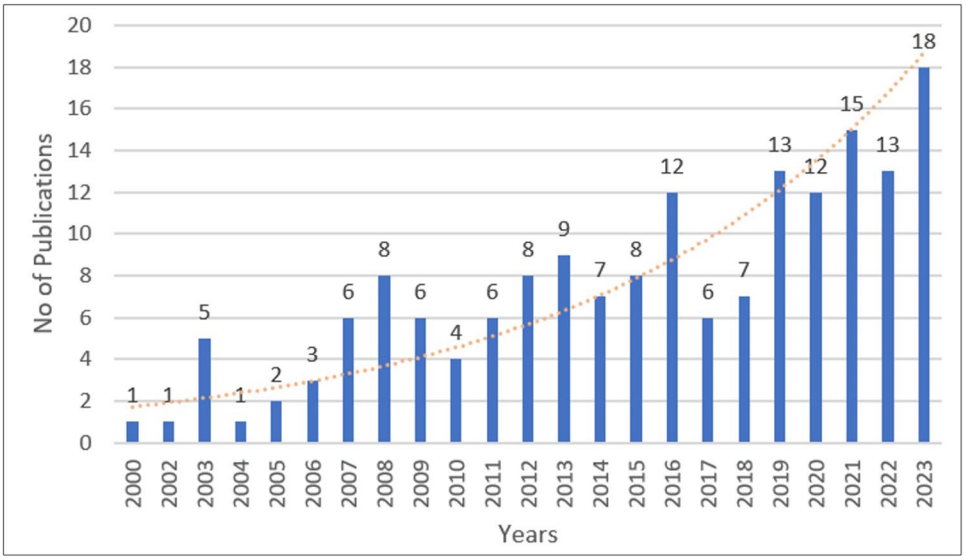

Fig. 3 The number of articles published on SCRMA over the years 2000–2023

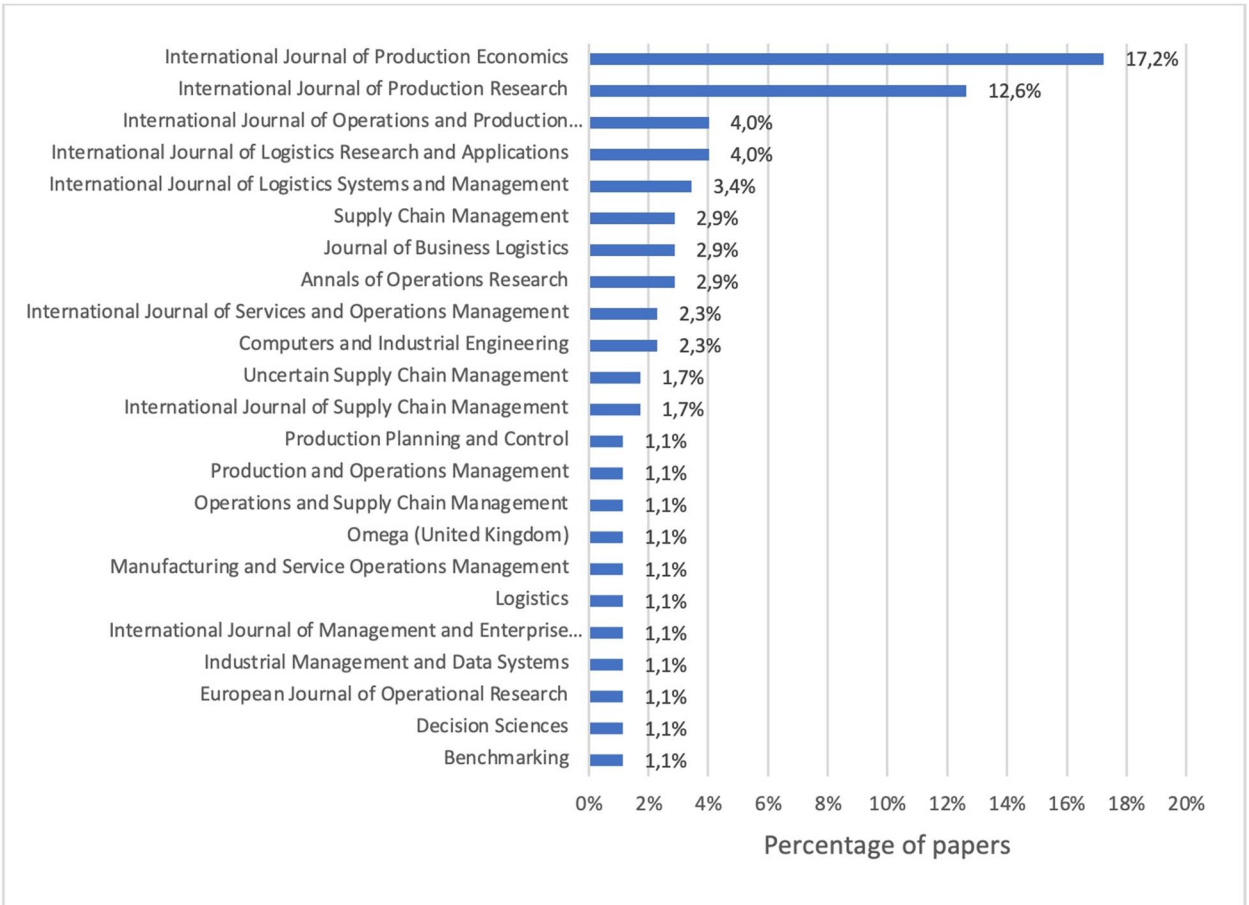

Fig. 4 The number of articles published on SCRMA by selected journals

Content-based analysis

Structure

SCRM consists of five main phases (Aqlan & Lam, 2015b; Blome & Schoenherr, 2011; Deiva Ganesh & Kalpana, 2022a; Hallikas et al., 2004; Rangel et al., 2015; and Schlüter et al., 2017): the detection, assessment, mitigation, monitoring, and handling of risks. Figure 5 illustrates the main aspects of each of them.

Risk detection entails the identification of all potential risks and their causes. This involves identifying which suppliers could disrupt the primary process, and what the potential causes are, such as financial default, geopolitical implications, or equipment failures. Another function of this phase is to categorize causes into homogenous classes. Because it needs to detect any possible cause of disruption, this phase typically acts on all direct suppliers and considers any causal factor that could possibly trigger disruptions. Because of the volatility of the business environment, risk detection is conducted at fixed intervals, such as yearly or quarterly.

Risk assessment evaluates how serious each risk is. It requires an estimate of how likely each event is to occur and its potential impact in terms of economic damage (Hallikas et al., 2002; Harland et al., 2003). For instance, by examining the suppliers' financial statements, it is possible to estimate their financial default likelihood; likewise, by taking into consideration the volumes and use of each supply, we can estimate the costs resulting from its sudden interruption (Blome & Schoenherr, 2011). Given its goal, the risk assessment phase follows the patterns and frequency of risk detection.

Risk mitigation encompasses all ex-ante actions that can reduce SC risk. It is composed of two fundamentally different types of levers: *prevention*, aimed at reducing the likelihood of risky events, and *protection*, which aims to reduce events' impact when they occur (Hallikas et al., 2004; Hoffmann et al., 2013; Hsu et al., 2022; Wiengarten et al., 2016). For example, replacing a high-risk supplier with a lower-risk

Fig. 5 SCRM's five main phases

one is a preventive action, whereas purchasing an insurance contract to safeguard a company from its high-risk suppliers is a protective action. Since risk mitigation is aimed at reducing risk *ex-ante*, it specifically focuses on those suppliers that were found particularly risky in the assessment phase, either because they are particularly likely to interrupt supplies, or because this event could determine large damages. Hence, prevention is continuously done until the overall risk exposure is deemed acceptable.

Risk monitoring takes into consideration all risky suppliers where it was either impossible or too expensive to perform any mitigation action (Blome & Schoenherr, 2011; Hallikas et al., 2002). By focusing on rather few, very risky suppliers, risk monitoring can be a more detailed risk analysis than risk assessment. In the case of suppliers with a high failure probability, it requires to increase the evaluation frequency, for instance by checking relevant information every week or even in real time. When a supplier's failure could be particularly costly, the focal company could be interested in deepening information on that firm's control structure, management team, development plans, etc. (Spieske & Birkel, 2021).

Finally, *risk handling* actions manage unwelcome events once they occur. If the customer is caught unprepared, the reaction is inevitably both inefficient and ineffective: this is why Emrouznejad et al. (2023) and Shah et al. (2023) suggest developing ex-ante contingency plans in a way that the ex-post reaction can be more rational and coordinated: accordingly, this is the only SCRM phase that is performed, partially, ex post.

The five following sections present the findings of our content analysis based on the 51 final papers selected as described in the "Methodology" section, arranged by these 5 SCRM process phases. A resume of our findings is presented in Tables 1 and 2.

Risk detection

According to Deiva Ganesh and Kalpana (2022b) and Ivanov et al. (2019), modern SCs are increasingly vulnerable, especially if they are global, de-verticalized, and lean. However, the dynamic and interconnected nature of these risks complicates the detection process (Kassa et al., 2023). Various studies outline several different SC risk classifications and interpretations: some were proposed by academics, while others have emerged from industry (Aljabhan, 2023; Duong et al., 2023). A vast amount of literature (26 articles) follows a basic risk classification as either exogenous or endogenous (Hallikas et al., 2004; Rauniyar et al., 2023; Samvedi et al., 2013; Schroeder & Lodemann, 2021; Wiengarten et al., 2016). Baryannis et al. (2019a), Baryannis et al. (2019b), and Kumar and Sharma (2023) focus on the SC phase affected, defining supply-side, demand-side, operational, environmental, and process-related risks. Another popular approach is simply to categorize SC risks by their origin: for instance, Hallikas et al. (2002) and Thun and Hoenig (2011) categorize financial, supply, demand, or logistic risks.

Traditional risk detection approaches include quantitative methods like fuzzy-sets (Aqlan & Lam, 2015a), AHP (Samvedi et al., 2013), multi-criteria decision making (MCDM) (Hsu et al., 2022), knowledge-based systems (Hult et al., 2010), and SC vulnerability maps (Tukamuhabwa et al., 2017), alongside qualitative methods such as the Delphi Technique (Meyer et al., 2022), cause-effect diagrams (Pournader et al., 2020), structured interviews, and surveys. By expanding the scope of traditional risk detection methods, I4.0 is redefining risk identification mechanisms in qualitative, quantitative, and hybrid ways. For example, BASF, UCB Biopharma, and Dover Chemical adopted Predictive Sourcing AI, a machine learning approach to analyze supplier pricing, detect quote anomalies, and support risk-informed procurement policies. These capabilities enable firms to respond more effectively to market volatility and supplier uncertainty (Arkestro, 2021).

BDA enhances SC visibility and traceability, ensuring information is more available, timely, complete, and accurate, thus enabling organizations to make more informed decisions (De Assis Santos & Marques, 2022; Yang et al., 2023), while data accessibility remains a significant barrier, as highlighted by Rezki and Mansouri (2023), especially by leveraging technologies such as AI/ML and BDA firms can achieve the ability to gather and process vast amounts of real time and dynamic data from suppliers' financial reports (S. M. Shah et al., 2021), public databases for default risk exposure, territorial exposure to extreme natural events, and online resources regarding geopolitical risks (Meng, 2021; Toorajipour et al., 2021).

Analytical techniques such as data mining, text mining, decision trees, support vector machines, and neural networks are used to uncover hidden patterns, relationships, and trends within different data sources (Raman et al., 2023). They can collect and analyze large amounts of information to identify environmental hazards, natural disasters, financial fluctuations, and political instabilities (Chu et al., 2020; Shah et al., 2021). Baghalzadeh et al. (2024), Handfield et al. (2020), and Baryannis et al. (2019b) report gathering a continuous flow of frequently updated information from open platforms like Google and Yahoo, social media, and open-access data. Handfield et al. (2020) used newsfeed data and textual analysis to identify political unrest or natural disasters. Further, Al Ayed & Al Tit (2023) and Gao et al. (2020) discussed how the integration of IoT devices with ERP systems can facilitate automatic internal risk identification. Data from corporate ERP and CRM systems has been leveraged to identify risks in the textile sector (Rafi et al., 2024); likewise, Chenger and

Table 1 Papers included in our content analysis by the SCRMA phase

#	Authors	Title	Detection	Assessment	Mitigation	Monitoring	Handling
1	Baghalzadeh Shishehgarkhaneh M.; Moehler R.C.; Fang Y.; Aboutorab H.; Hijazi A.A	Construction supply chain risk management	X	X	X		X
2	Rafi-Ul-Shan P.; Bashiri M.; Kamal M.M.; Mangla S.K.; Tjahjono B	An Analysis of Fuzzy Group Decision-Making to Adopt Emerging Technologies for Fashion Supply Chain Risk Management	X	X	X		
3	Jegan Joseph Jerome J.; Sonwaney V.; Bryde D.; Graham G	Achieving competitive advantage through technology-driven proactive supply chain risk management: an empirical study	X	X	X		
4	Wu, Mengna; Fu, Changxin; Holguin-veras, Jose; Enz, Matias G.; Mondy, Christopher	The impact of digital technology deployment on mitigating supply chain disruptions: Evidence from Chinese automotive manufacturers during the COVID-19 crisis			X		X
5	Mittal U.; Panchal D	AI-Based Evaluation System for Supply Chain Vulnerabilities and Resilience Amidst External Shocks: An Empirical Approach	X	X	X		X
6	Yang M.; Lim M.K.; Qu Y.; Ni D.; Xiao Z	Supply chain risk management with machine learning technology: A literature review and future research directions	X	X	X	X	
7	Kumar S.; Sharma S.C	Integrated Model for Predicting Supply Chain Risk through Machine Learning Algorithms	X	X	X		
8	Kalbouneh N.Y.; Bataineh K.A.; Al-Hamad A.A.-S.A.; Dwakat M.K.A.; Abualoush S.; Almasarweh M.S.; Al-Smadi R.W	The effects of the blockchain technology and big data analytics on supply chain performance: The mediating effect supply chain risk management	X		X		X
9	Yang Y.; Peng C.; Cao E.; Zou W	Building Resilience in Supply Chains: A Knowledge Graph-Based Risk Management Framework	X	X	X	X	X
10	Chenger D.; Pettigrew R.N	Leveraging data-driven decisions: a framework for building intracompany capability for supply chain optimization and resilience	X	X	X		
11	Spieske A.; Gebhardt M.; Kopyto M.; Birkel H.; Hartmann E	The future of industry 4.0 and supply chain resilience after the COVID-19 pandemic: Empirical evidence from a Delphi study	X	X	X		X
12	Raman P.; Seetha R.; Sankar S.; Suresh K.; Arunkumar R.; Mohanaprakash T.A	CUCKOO SEARCH SUPPORT VECTOR MACHINE FOR SUPPLY CHAIN RISK MANAGEMENT	X	X			X
13	Shah H.M.; Gardas B.B.; Narwane V.S.; Mehta H.S	The contemporary state of big data analytics and artificial intelligence towards intelligent supply chain risk management: a comprehensive review	X	X	X	X	
14	Rauniyar K.; Wu X.; Gupta S.; Modgil S.; Lopes de Sousa Jabbour A.B	Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology	X		X	X	X
15	Rezki N.; Mansouri M	Improving supply chain risk assessment with artificial neural network predictions		X			X
16	Wyrembek M	The application of adaboost.m1 based on ant colony optimization to classify the risk of delay in the pharmaceutical supply chain	X	X			

Table 1 (continued)

#	Authors	Title	Detection	Assessment	Mitigation	Monitoring	Handling
17	Wong W.P.; Saw P.S.; Jomthanachai S.; Wang L.S.; Ong H.F.; Lim C.P	Digitalization enhancement in the pharmaceutical supply network using a supply chain risk management approach	X				
18	Al-Ayed S.I.; Al-Tit A.A	The effect of supply chain risk management on supply chain resilience: The intervening part of Internet-of-Things	X	X			X
19	Aljabhan B	Economic strategic plans with supply chain risk management (SCRM) for organizational growth and development	X	X	X	X	
20	Li L.; Gong Y.; Wang Z.; Liu S	Big data and big disaster: a mechanism of supply chain risk management in global logistics industry	X		X		X
21	Giudici, Paolo; Centurelli, Mattia; Turchetta, Stefano	Artificial Intelligence risk measurement		X			
22	Kassa, Adane; Kitaw, Daniel; Stache, Ulrich; Beshah, Berhanu; Degefu, Getachew	Artificial intelligence techniques for enhancing supply chain resilience: A systematic literature review, holistic framework, and future research	X	X	X		X
23	Aljohani, Abeer	Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility			X		X
24	Deiva Ganesh A.; Kalpana P	Supply chain risk identification: a real-time data-mining approach	X				
25	Meyer M.M.; Glas A.H.; Eßig M	A Delphi study on the supply risk-mitigating effect of additive manufacturing during SARS-COV-2			X		
26	Kosasih E.E.; Margaroli F.; Gelli S.; Aziz A.; Wildgoose N.; Brintrup A	Towards knowledge graph reasoning for supply chain risk management using graph neural networks		X		X	
27	de Assis Santos L.; Marques L	Big data analytics for supply chain risk management: research opportunities at process crossroads	X	X	X		X
28	Park M.; Singh N.P	Predicting supply chain risks through big data analytics: role of risk alert tool in mitigating business disruption	X	X	X		
29	Deiva Ganesh A.; Kalpana P	Future of artificial intelligence and its influence on supply chain risk management – A systematic review	X	X	X	X	X
30	Žigienė G.; Rybakovas E.; Vaitkienė R.; Gaidelys V	Setting the Grounds for the Transition from Business Analytics to Artificial Intelligence in Solving Supply Chain Risk	X	X		X	
31	Schroeder M.; Lodemann S	A Systematic Investigation of the Integration of Machine Learning into Supply Chain Risk Management	X		X		
32	Meng L	Using iot in supply chain risk management, to enable collaboration between business, community, and government			X	X	X
33	Li S.; Sun Q.; Liu S	Risk assessment for supply chain based on Cloud model	X	X			X
34	Shah S.M.; Lütjen M.; Freitag M	Text mining for supply chain risk management in the apparel industry	X				
35	Ivanov, Dmitry; Dolgui, Alexandre	A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0				X	X
36	Spieske, Alexander; Birkel, Hendrik	Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic	X		X	X	X

Table 1 (continued)

#	Authors	Title	Detection	Assessment	Mitigation	Monitoring	Handling
37	Gao Q.; Guo S.; Liu X.; Manogaran G.; Chilamkurti N.; Kadry S	Simulation analysis of supply chain risk management system based on IoT information platform	X		X	X	
38	Handfield R.; Sun H.; Rothenberg L	Assessing supply chain risk for apparel production in low cost countries using newsfeed analysis	X	X			
39	Chu C.-Y.; Park K.; Kremer G.E	A global supply chain risk management framework: An application of text-mining to identify region-specific supply chain risks	X	X	X		
40	Birkel H.S.; Hartmann E	IoT – the future of managing supply chain risks	X		X		
41	Er Kara M.; Oktay Fırat S.Ü.; Ghadge A	A data mining-based framework for supply chain risk management	X				
42	Messina, Dario; Barros, Ana Cristina; Soares, António Lucas; Matopoulos, Aristides	An information management approach for supply chain disruption recovery					X
43	Fischer-pre, Diana; Eismann, Kathrin; Fischbach, Kai	Information technology and risk management in supply chains	X	X	X	X	
44	Baryannis G.; Validi S.; Dani S.; Antoniou G	Supply chain risk management and artificial intelligence: state of the art and future research directions	X	X	X		
45	Singh N.P.; Singh S	Building supply chain risk resilience: Role of big data analytics in supply chain disruption mitigation	X		X		X
46	Ivanov D.; Dolgui A.; Sokolov B	The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	X	X	X		X
47	Baryannis G.; Dani S.; Antoniou G	Predicting supply chain risks using machine learning: The trade-off between performance and interpretability		X			X
48	Qazi, Abroon; Dickson, Alex; Quigley, John; Gaudenzi, Barbara	Supply chain risk network management: A Bayesian belief network and expected utility based approach for managing supply chain risks	X	X	X		X
49	Mani, Venkatesh; Delgado, Catarina; Hazen, Benjamin T.; Patel, Purvishkumar	Mitigating Supply Chain Risk via Sustainability Using Big Data Analytics: Evidence from the Manufacturing Supply Chain	X		X		
50	Yan B.; Wang X.; Shi P	Risk assessment and control of agricultural supply chains under IoT		X	X		X
51	Schlüter, F. F.; Hetterscheid, E.; Henke, M	A Simulation-Based Evaluation Approachfor Digitalization Scenarios in Smart SupplyChain Risk Management	X	X	X		X
			40	32	35	13	26

An "X" means that the paper referreed in the row discusses the SCRMA phase in the column

Table 2 Papers included in our content analysis by technology

#	Authors	Title	IoT	BDA	CC	AI/ML	block-chain	CPS	DTS	IR	AM
1	Baghalzadeh Shishehgarkhaneh M.; Moehler R.C.; Fang Y.; Aboutorab H.; Hijazi A.A	Construction supply chain risk management		X		X					
2	Rafi-Ul-Shan P.; Bashiri M.; Kamal M.M.; Mangla S.K.; Tjahjono B	An Analysis of Fuzzy Group Decision-Making to Adopt Emerging Technologies for Fashion Supply Chain Risk Management	X			X	X	X		X	
3	Jegan Joseph Jerome J.; Sonwaney V.; Bryde D.; Graham G	Achieving competitive advantage through technology-driven proactive supply chain risk management: an empirical study	X	X							
4	Wu, Mengna; Fu, Changxin; Holguin-veras, Jose; Enz, Matias G.; Mondy, Christopher	The impact of digital technology deployment on mitigating supply chain disruptions: Evidence from Chinese automotive manufacturers during the COVID-19 crisis	X	X	X	X	X				
5	Mittal U.; Panchal D	AI-Based Evaluation System for Supply Chain Vulnerabilities and Resilience Amidst External Shocks: An Empirical Approach				X					
6	Yang M.; Lim M.K.; Qu Y.; Ni D.; Xiao Z	Supply chain risk management with machine learning technology: A literature review and future research directions				X					
7	Kumar S.; Sharma S.C	Integrated Model for Predicting Supply Chain Risk through Machine Learning Algorithms				X					
8	Kalbouneh N.Y.; Bataineh K.A.; Al-Hamad A.A.-S.A.; Dwakat M.K.A.; Abualoush S.; Almasarweh M.S.; Al-Smadi R.W	The effects of the blockchain technology and big data analytics on supply chain performance: The mediating effect supply chain risk management		X			X				
9	Yang Y.; Peng C.; Cao E.; Zou W	Building Resilience in Supply Chains: A Knowledge Graph-Based Risk Management Framework		X	X	X					
10	Chenger D.; Pettigrew R.N	Leveraging data-driven decisions: a framework for building intracompany capability for supply chain optimization and resilience		X							
11	Spieske A.; Gebhardt M.; Kopyto M.; Birkel H.; Hartmann E	The future of industry 4.0 and supply chain resilience after the COVID-19 pandemic: Empirical evidence from a Delphi study	X	X		X	X			X	X
12	Raman P.; Seetha R.; Sankar S.; Suresh K.; Arunkumar R.; Mohanaprakash T.A	Cuckoo search support vector machine for supply chain risk management				X					
13	Shah H.M.; Gardas B.B.; Narwane V.S.; Mehta H.S	The contemporary state of big data analytics and artificial intelligence towards intelligent supply chain risk management: a comprehensive review		X	X	X					
14	Rauniyar K.; Wu X.; Gupta S.; Modgil S.; Lopes de Sousa Jabbour A.B	Risk management of supply chains in the digital transformation era: contribution and challenges of blockchain technology					X				
15	Rezki N.; Mansouri M	Improving supply chain risk assessment with artificial neural network predictions				X					

Table 2 (continued)

#	Authors	Title	IoT	BDA	CC	AI/ML	block-chain	CPS	DTS	IR	AM
16	Wyrembek M	The application of adaboost.m1 based on ant colony optimization to classify the risk of delay in the pharmaceutical supply chain				X					
17	Wong W.P.; Saw P.S.; Jomthanachai S.; Wang L.S.; Ong H.F.; Lim C.P	Digitalization enhancement in the pharmaceutical supply network using a supply chain risk management approach				X			X		
18	Al-Ayed S.I.; Al-Tit A.A	The effect of supply chain risk management on supply chain resilience: The intervening part of Internet-of-Things	X								
19	Aljabhan B	Economic strategic plans with supply chain risk management (SCRM) for organizational growth and development		X		X					
20	Li L.; Gong Y.; Wang Z.; Liu S	Big data and big disaster: a mechanism of supply chain risk management in global logistics industry		X							
21	Giudici, Paolo; Centurelli, Mattia; Turchetta, Stefano	Artificial Intelligence risk measurement				X					
22	Kassa, Adane; Kitaw, Daniel; Stache, Ulrich; Beshah, Berhanu; Degefu, Getachew	Artificial intelligence techniques for enhancing supply chain resilience: A systematic literature review, holistic framework, and future research				X					
23	Aljohani, Abeer	Predictive Analytics and Machine Learning for Real-Time Supply Chain Risk Mitigation and Agility		X		X					
24	Deiva Ganesh A.; Kalpana P	Supply chain risk identification: a real-time data-mining approach				X					
25	Meyer M.M.; Glas A.H.; Eßig M	A Delphi study on the supply risk-mitigating effect of additive manufacturing during SARS-COV-2									X
26	Kosasih E.E.; Margaroli F.; Gelli S.; Aziz A.; Wildgoose N.; Brintrup A	Towards knowledge graph reasoning for supply chain risk management using graph neural networks				X					
27	de Assis Santos L.; Marques L	Big data analytics for supply chain risk management: research opportunities at process crossroads		X							
28	Park M.; Singh N.P	Predicting supply chain risks through big data analytics: role of risk alert tool in mitigating business disruption		X							
29	Deiva Ganesh A.; Kalpana P	Future of artificial intelligence and its influence on supply chain risk management – A systematic review				X					
30	Žigienė G.; Rybakovas E.; Vaitkienė R.; Gaidelys V	Setting the Grounds for the Transition from Business Analytics to Artificial Intelligence in Solving Supply Chain Risk									
31	Schroeder M.; Lodemann S	A Systematic Investigation of the Integration of Machine Learning into Supply Chain Risk Management				X					
32	Meng L	Using iot in supply chain risk management, to enable collaboration between business, community, and government	X	X	X						
33	Li S.; Sun Q.; Liu S	Risk assessment for supply chain based on Cloud model			X	X					
34	Shah S.M.; Lütjen M.; Freitag M	Text mining for supply chain risk management in the apparel industry				X					
35	Ivanov, Dmitry; Dolgui, Alexandre	A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0	X			X			X		

Table 2 (continued)

#	Authors	Title	IoT	BDA	CC	AI/ML	block-chain	CPS	DTS	IR	AM
36	Spieske, Alexander; Birkel, Hendrik	Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic	X	X	X	X	X	X			X
37	Gao Q.; Guo S.; Liu X.; Manogaran G.; Chilamkurti N.; Kadry S	Simulation analysis of supply chain risk management system based on IoT information platform	X			X			X		
38	Handfield R.; Sun H.; Rothenberg L	Assessing supply chain risk for apparel production in low cost countries using newsfeed analysis				X					
39	Chu C.-Y.; Park K.; Kremer G.E	A global supply chain risk management framework: An application of text-mining to identify region-specific supply chain risks				X					
40	Birkel H.S.; Hartmann E	IoT – the future of managing supply chain risks	X	X							
41	Er Kara M.; Oktay Fırat S.Ü.; Ghadge A	A data mining-based framework for supply chain risk management									
42	Messina, Dario; Barros, Ana Cristina; Soares, António Lucas; Matopoulos, Aristides	An information management approach for supply chain disruption recovery		X	X						
43	Fischer-pre, Diana; Eismann, Kathrin; Fischbach, Kai	Information technology and risk management in supply chains	X	X		X					
44	Baryannis G.; Validi S.; Dani S.; Antoniou G	Supply chain risk management and artificial intelligence: state of the art and future research directions				X					
45	Singh N.P.; Singh S	Building supply chain risk resilience: Role of big data analytics in supply chain disruption mitigation		X							
46	Ivanov D.; Dolgui A.; Sokolov B	The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics	X	X			X				X
47	Baryannis G.; Dani S.; Antoniou G	Predicting supply chain risks using machine learning: The trade-off between performance and interpretability				X					
48	Qazi, Abroon; Dickson, Alex; Quigley, John; Gaudenzi, Barbara	Supply chain risk network management: A Bayesian belief network and expected utility based approach for managing supply chain risks				X					
49	Mani, Venkatesh; Delgado, Catarina; Hazen, Benjamin T.; Patel, Purvishkumar	Mitigating Supply Chain Risk via Sustainability Using Big Data Analytics: Evidence from the Manufacturing Supply Chain	X	X							
50	Yan B.; Wang X.; Shi P	Risk assessment and control of agricultural supply chains under IoT	X		X						
51	Schlüter, F. F.; Hetterscheid, E.; Henke, M	A Simulation-Based Evaluation Approachfor Digitalization Scenarios in Smart SupplyChain Risk Management	X	X					X		
			15	15	8	32	7	2	4	2	3

An "X" means that the paper referred to in the row discusses the SCRMA technology in the column

Pettigrew (2023) showed how vertical information systems have been used to collect information from multidisciplinary teams in the oil and gas industry. Aljabhan (2023) and Wong et al. (2023) leveraged data inputs from IoT sensors, ERP, and BC transactions and employed AI/ML, BDA, and DTS to enable advanced data analysis and support real-time risk identification and categorization.

Analytical approaches (Classification methods, Regression modelling, Clustering, Association Rule Learning, Supervised Learning, Text Mining, Sequence Mining, …) can support the identification of various risk types that were previously difficult or impossible to detect (Kalbouneh et al., 2023; Park & Singh, 2023; Shah et al., 2023). Furthermore, Baryannis et al. (2019b), Rafi et al. (2024), and Yang et al. (2023) discussed the modified Analytical Hierarchy Process to identify the most prevalent threats in supply and demand risk. Hence, integrating existing risk identification methods with these technologies can improve the risk detection accuracy (Li et al., 2023; Singh & Singh, 2019).

Literature also showed I4.0 technologies ability to extract real-time risk information and assess information polarity from social media in the fashion/apparel industry by using natural language processing (NLP) techniques such as Regular Expressions, Fuzzywuzzy, and TextBlob (Handfield et al., 2020; Shah et al., 2021): for instance, Deiva Ganesh and Kalpana (2022b) harnessed real-time information from Twitter, identifying several key risks, including port congestion and semiconductor shortages.

Also, AI-based techniques including hybrid algorithms, artificial neural networks, agent-based systems and unsupervised learning techniques such as Petri Nets, knowledge graph, and Bayesian Belief Networks can help identify patterns and support sophisticated risk analyses, enabling organizations to obtain advanced information on supplier availability (Baryannis et al., 2019b; Gao et al., 2020; Yang et al., 2024) and to enhance comprehensive risk identification (Li et al., 2021; Mittal & Panchal, 2023; Qazi et al., 2018; Žigienė et al., 2022). Similarly, ML models demonstrated good accuracy in forecasting potential delays within the SC, as shown by Wyrembek (2023).

Moreover, CPS and data analytics tools like any Logistix support risk detection by integrating data from IT systems and simulating disruptions (Rafi et al., 2024). Discrete-event simulation models were also employed to effectively represent and analyze complex workflows. Moreover, literature emphasized BC as a tool for identifying informational and cyber risks, such as cyber threats, security breaches, and data breaches, while also ensuring information security, trust, and addressing intentional risks in SCM (Rauniyar et al., 2023). However, there remains a need for dynamic risk identification models to overcome traditional static approaches, especially in addressing market changes and demand uncertainties (Er Kara et al., 2020; Spieske et al., 2023; Yang et al., 2023).

Risk assessment

By assessing risks quantitatively, rapidly, and cost-efficiently, companies can focus on critical risks and prioritize mitigation actions, thereby facilitating informed decision-making (Hallikas et al., 2002; Harland et al., 2003). Assessment often shares the same timing and approach as the detection phase, leading to examining it within the context of SC risk detection, rather than by itself (Sodhi et al., 2012).

Risk assessment is frequently seen as subjective, relying on expert judgment and scenario analysis; however, expert judgment could potentially lead to bias and inconsistency (Handfield et al., 2020; Li et al., 2021; Rezki & Mansouri, 2023; Tran et al., 2018). This is why "classic" research differentiates qualitative, quantitative, and semi-quantitative techniques following the extent to which they combine objective data with subjective perceptions (Jüttner et al., 2003). Assessing risk severity by combining both impact and likelihood is a generally agreed-upon standpoint (Dong & Cooper, 2016; Samvedi et al., 2013), with various qualitative, quantitative, and hybrid indicators used to model occurrence likelihood (Aqlan & Lam, 2015a). Classic SCRM literature highlights various assessment methods and techniques ranging from vulnerability-based frameworks (Pettit et al., 2013) to parameter categorizations (Aqlan & Lam, 2015b) and indicator-based methodologies (Tran et al., 2018). However, classic methods often suffer from subjectivity and imprecision (Rafi et al., 2024). Refinements like Orders-of-Magnitude AHP improve traditional models by clustering criteria (Dong & Cooper, 2016), while advanced fuzzy set techniques (TrINFs, ELECTRE TRI-C) (Chenger & Pettigrew, 2023) and Bayesian methods enhance supplier risk evaluation (Dong & Cooper, 2016; Duong et al., 2023). Pettit et al. (2013) introduced a tool incorporating seven vulnerability factors, whereas Aqlan and Lam (2015b) categorized risks based on occurrence, predictability, duration, type, and frequency. Tran et al. (2018) classified risk indicators into single, paired, and aggregate measures, assessing their impact on SC performance. Despite the challenge of subjectivity, integrating quantitative analyses has significantly advanced risk assessment methodologies: while organization and corporate culture highlight qualitative aspects of risk, parameters like occurrence, duration, and predictability introduce a structured and quantitative perspective that can enhance accuracy (Mittal & Panchal, 2023; Yang et al., 2024).

I4.0 technologies enable a more objective risk evaluation by reducing subjectivity (Spieske et al., 2023). To assess risk likelihood, researchers utilized secondary data: for instance,

Rezki and Mansouri (2023) used 5 years of audit reports to train a risk assessment ML model. Similarly, Cisco evaluated supplier risk using World Bank data (Shah et al., 2023). Deiva Ganesh and Kalpana (2022a) merge historical analysis with predictive and proactive approaches to assess risks.

Further, Fuzzy Analytic Hierarchy Process (FAHP) and Fuzzy Analytic Network Process (FANP) are used in construction projects for their ability to handle uncertainty and complex decision-making criteria (Baryannis et al., 2019b; Chenger & Pettigrew, 2023). Similarly, in telecom SCs, hybrid fuzzy approaches have been employed to analyze interrelationships among risk factors (Aljabhan, 2023). Moreover, the risk diffusion convergence model is used to measure risk fluctuations in the agricultural SC using IoT and AI (Yan et al., 2017).

Additionally, ML algorithms like Support Vector Machines, Random Forest, and Decision Trees are recognized for their robust classification and prediction capabilities (Baryannis et al., 2019b; Kosasih et al., 2024; Raman et al., 2023; Wyrembek, 2023). These methods, along with Natural Language Toolkit (NLTK), stochastic programming, and Bayesian networks, offer a broad framework for identifying and evaluating SC risks (Chu et al., 2020; Ivanov & Dolgui, 2021; Kassa et al., 2023; Micheli et al., 2009; Žigienė et al., 2022). For example, Baghalzadeh et al. (2024) leveraged SC data and digital tools like Social Network Analysis and Structural Equation Modelling to quantify risk impact and uncover hidden patterns, while the ML-based "Supply Watch" model used by DHL and genetic algorithms discussed by Baryannis et al. (2019b) are increasingly popular for identifying risk types and predicting risk impacts. Chu et al. (2020) proposed a framework based on text mining and Bayesian Network Modelling to assess risks and guide supplier selection (Qazi et al., 2018). Some models incorporate suppliers' feedback to enhance the qualitative assessment and improve risks' understanding (Aljabhan, 2023; Li et al., 2021). Finally, Baryannis et al. (2019a), Ivanov et al. (2019), and Park and Singh (2023) all demonstrated automated risk alert tools based on BDA.

Risk mitigation

Miller (1992) famously proposed five classes of risk mitigation policies, namely: risk avoidance, control, cooperation, limitation, and flexibility. Most of the existing literature has followed Miller's policies (De Assis Santos & Marques, 2022; El Baz & Ruel, 2021; Gao et al., 2020; Mani et al., 2017; Spieske & Birkel, 2021; Yan et al., 2017). Additionally, Tang and Nurmaya Musa (2011) provided a comprehensive discussion of various risk elements with qualitative and quantitative mitigation approaches.

It is sometimes possible to avoid risks or to eliminate them entirely by acting on their root causes: for instance, when a risky supplier is eliminated, the corresponding risk exposure is completely avoided (Ojala & Hallikas, 2006). For unavoidable threats, reduction focuses on minimizing their impact: this is what happens, for instance, when a risky supplier is paired with a safer one. Transferring risk to external parties like insurers or outsourcers is an option considered when the probability is low, but the effect is high (Hoffmann et al., 2013; Thun & Hoenig, 2011). Furthermore, Chen et al. (2013) and Jüttner et al. (2003) emphasize risk cooperation, that is, a joint effort between supplier and customer to improve visibility, share information, and plans: this is what happens when a risky supplier grants the customer a certain level of dedicated capacity and/or stock (Hallikas et al., 2004; Mani et al., 2017; Singh & Singh, 2019). When none of those options is viable, especially for low-impact, low-probability, accepting risks avoids the need for mitigation (Berger et al., 2023; Deiva Ganesh & Kalpana, 2022a; Kassa et al., 2023). Since risks are often interconnected, addressing one risk type may either exacerbate or mitigate another. Therefore, organizations must thoroughly evaluate options before making a choice.

The rise of I4.0 has been found to enhance SC flexibility across procurement, production, and logistics (Chu et al., 2020; Fischer et al., 2020; Toorajipour et al., 2021; Wu et al., 2024). For example, Sentrisk, developed by Marsh McLennan, uses AI to analyze documentation, identifying structural vulnerabilities and map supply chain networks (Marsh, 2025), while Genetic algorithms used to determine flexible SC configurations (Baryannis et al., 2019b) enable proactive risk mitigation. Additionally, fuzzy logic models incorporating fuzzy multicriteria decision-making are applied to enhance organizational flexibility in SCs (Aljohani, 2023). The work of Meyer et al. (2022) demonstrates how organizations can hedge against SC risks by combining conventional manufacturing and AM as supply alternatives, thereby crafting a more resilient and flexible SC that can effectively manage disruptions. The deployment of robots and cobots can improve operational efficiency and reduce human errors in manufacturing and warehouse settings (Rafi et al., 2024), thereby mitigating risks associated with delays caused by misplaced or unavailable inventory (Spieske & Birkel, 2021). Various techniques are presented in literature to foster collaboration among SC partners and facilitate supplier selection: for example, Volkswagen's ML-based bidder list generator precisely identifies potential suppliers, thereby reducing delays and procurement risks (Emrouznejad et al., 2023; Schroeder & Lodemann, 2021). A GRA-based linguistic model, Information Sharing Technologies (IST) (Gao et al., 2020), and CPS-enabled real-time monitoring and control of operations enhance collaboration through automated and intelligent systems (Li et al., 2023; Shah et al., 2023). An integrated information sharing infrastructure with BDA supports decision-making, helps stabilize operations,

and reduces time disruptions by tracing their roots (Jegan et al., 2024). IoT allows for continuous supplier evaluation, mitigating risks and supporting joint decision-making among SC members through Collaborative Decision Support Systems (Birkel & Hartmann, 2020; Qazi et al., 2018). BC further enhances transparency by enabling validation, automation, and tokenization, thereby preventing fraud or manipulation (Kalbouneh et al., 2023; Rauniyar et al., 2023). Moreover, Park and Singh (2023) highlight that integrating IT infrastructure with BDA can significantly improve knowledge management capabilities, enabling firms to collect and analyze data from multiple sources in real time, thereby facilitating data-driven decision-making (Kassa et al., 2023).

This aligns with the broad academic consensus that digital and knowledge management capabilities are crucial for supporting mitigation policies (Shah et al., 2023). Several scholars discussed hybrid quantitative models that offer effective risk mitigation by analyzing complex interrelationships among risk entities and by leveraging mathematical techniques (Schlüter et al., 2017). AI-based classification algorithms further support this effort by categorizing SC elements into distinct risk profiles, allowing for targeted mitigation strategies (Meng, 2021). Additionally, data from Failure Mode and Effect Analysis (FMEA) or simulation models provide valuable insights into risk behaviours and triggering factors, facilitating a deeper understanding of SC dynamics (Wong et al., 2023).

Research also addressed the integration of IoT and social media to enhance collaboration among SC stakeholders in crisis times (Meng, 2021). Further, I4.0 technologies can help mitigate global sourcing risks: for example, Handfield et al. (2020) discussed using web-crawler algorithms and ML to develop market intelligence and enhance global corporations' decision-making. Finally, while a more traditional body of research primarily focuses on mitigating risks through reduced lead times, improved data quality, and enhanced collaboration, AI and BDA are also considered effective tools for risk mitigation, through such techniques as ensemble learning, random forests, and support vector machines that can model SC risk dynamics and enable proactive as well as reactive mitigation strategies through accurate predictions (Kumar & Sharma, 2023; Raman et al., 2023; Schroeder & Lodemann, 2021).

Risk monitoring

Effective risk monitoring is important for organizations to proactively manage their exposure to threats. In the case of suppliers that could determine a disrupting effect despite having a rather small interruption probability, the monitoring phase analyzes analytic data to confirm the low probability (Blome & Schoenherr, 2011). Likewise, high-probability risks require real-time surveillance to detect early warning signals (Deiva Ganesh & Kalpana, 2022a; Hoffmann et al., 2013). Only a limited number of studies have explicitly addressed risk monitoring with technology, and among these, IoT, BDA, and AI/ML are the primary technologies discussed.

Risk monitoring involves dynamic surveillance tailored to specific risk types, severity, and contextual factors. External risks, such as geopolitical instability, might need continuous news monitoring, while internal risks, like supplier financial health, require periodic assessments using metrics such as payment history, debt levels, and performance indicators (Spieske & Birkel, 2021). By continuously monitoring and in-depth analyzing SC information over time, firms can gain a clear understanding and early warning of the evolving risk landscape, enabling preventive strategies and enhancing overall resilience. In this regard, conventional SCRM approaches often struggle to manage the extensive and diverse data and especially the extremely dynamic approach required for effective risk monitoring. To address these challenges, researchers have proposed specialized data management systems, early-warning processes using knowledge graphs, and smart information-sharing tools (Yang et al., 2023).

Technologies like the IoT, predictive analytics, and ML are transforming continuous risk monitoring by enabling real-time data collection, early warning capabilities, and proactive risk prevention (Gao et al., 2020; Meng, 2021). By the same token, technologies like support vector machine classifiers, semi-supervised learning, and deep learning focus on analyzing the data to identify abnormal conditions (Žigienė et al., 2022). These techniques enable sophisticated analysis of complex datasets, providing critical insights into understanding vendor trustworthiness (Žigienė et al., 2022) or monitoring financial risks (Raman et al., 2023; Yang et al., 2023).

Hybrid models combining deep learning and BC have been developed to monitor social media data and identify potential disruptions (Rauniyar et al., 2023). Additionally, IoT-based systems integrating AI and fuzzy logic provide early warnings for occupational safety in specialized SCs, such as cold chains. ML has emerged as a cornerstone technology for risk monitoring, with applications ranging from pattern recognition using neural networks to time series forecasting with long-short-term memory (LSTM) networks (Kosasih et al., 2024). Techniques such as random forests, gradient boosting machines, and Bayesian networks (BN) improve prediction accuracy (Aljabhan, 2023), while anomaly detection algorithms like isolation forests identify unusual patterns indicative of risks (Yang et al., 2023). Reinforcement learning is also being applied in dynamic risk management scenarios, offering adaptive solutions for evolving SC environments (Shah et al., 2023).

Risk handling

Despite efforts made ex-ante to identify, assess, mitigate, and monitor SC risks, unwelcome events still happen. Upon occurrence, firms should react in the fastest and most effective way in order to reduce the effects. Proactive risk handling is connected to SC's robustness and agility (Wieland & Wallenburg, 2012). As both internal and external conditions constantly evolve, businesses must regularly update their risk-handling policies to adapt quickly to changes (agility), maintain adaptability (flexibility), recover effectively (resilience), and withstand disruptions (robustness) in the dynamic environment (Deiva Ganesh & Kalpana, 2022a, b). A comprehensive SC risk-handling plan includes disruptions' detection, response, and recovery (Chowdhury & Quaddus, 2016). Detection identifies the disruption; response implements countermeasures, like activating backup suppliers; and recovery restores normal operations by going back to the previous equilibrium or finding a new steady state. All these stages should be prepared ex-ante by issuing contingency plans.

Reducing the time gap between the occurrence of an event and its *detection* is crucial and is based on information and visibility. For instance, Qazi et al. (2018) evaluate the vulnerability of individual SC nodes and analyze disruption propagation using Bayesian networks and deep neural networks. Many I4.0 technologies, such as IoT and CC, have demonstrated the ability to enhance SC visibility by enabling tracking, tracing, and data accessibility (Rezki & Mansouri, 2023; Wu et al., 2024). To improve detection, organizations can leverage structured and extensive databases, decision-making models that integrate data from various sources, including ERP systems, RFID, and cyber sources (Kalbouneh et al., 2023; Rauniyar et al., 2023). Ivanov and Dolgui (2021) proposed a data-driven decision support system that leverages on second-order cybernetics to capture both the physical and cyber dimensions of SCs. These systems can enhance learning and pattern recognition related to disruptions. Additionally, robotic process automation can cross-reference data and present the results through dashboards (De Assis Santos & Marques, 2022). AI-driven models enable continuous monitoring of supplier performance across parameters such as delivery punctuality, product quality, and financial stability. This continuous monitoring allows for proactively identify perturbations before they escalate into major disruptions (Baghalzadeh et al., 2024).

Mapping connections between disruption factors and outcomes through techniques like Fault Tree Analysis and Discrete-Event Simulation helps in visualizing and analyzing root causes (Singh & Singh, 2019). After identifying a disruption, descriptive and diagnostic analysis is needed to understand its nature, scope, and underlying causes, enabling the development of response and recovery policies. AI can help visualize and analyze existing networks, improving visibility on dependencies and potential bottlenecks (Mittal & Panchal, 2023). For instance, Petri Nets and Triangularization clustering have been used to analyze SC network vulnerabilities and ripple effects of disruptions (Ivanov et al., 2019; Liu et al., 2021). Furthermore, Bayesian networks can automatically identify interconnections among risk factors for various stakeholders, enabling the assessment of disruption probabilities (Baryannis et al., 2019b).

In the *response* phase, organizations implement actions to minimize disruptions severity. This phase concentrates on immediate countermeasures and agile responses to minimize consequences for the SC. Researchers agree that agility, flexibility, and robustness are key SC resilience aspects to enable recovery from disruptions (Ivanov & Dolgui, 2021; Wieland & Wallenburg, 2012; Wu et al., 2024). Proactive planning and contingency plans are crucial for effectively responding to SC disruptions. This approach allows companies to anticipate issues and develop appropriate countermeasures, rather than reacting in crisis mode. Technology can enhance these efforts by enabling more effective inter-organizational information sharing and collaboration (Li et al., 2021). Integrating BDA and BC technologies allows organizations to derive actionable intelligence for responding to disruptions (Kalbouneh et al., 2023). Similarly, Qazi et al. (2018) highlight the use of Bayesian networks to facilitate the selection of alternative suppliers during a disruption, which can reduce dependency on a single source and enhance agility. Additionally, IoT facilitates rapid communication and data sharing, enabling agile decision-making and swift action to minimize the impact of disruptions (Aljohani, 2023; Kassa et al., 2023; Yang et al., 2024).

The *Recovery* phase restores SC to pre-disruption standards, emphasizing efforts to stabilize operations and return to normal functioning. This phase addresses the disruption's impact, aiming to minimize downtime and ensure continuity (Baryannis et al., 2019b; Raman et al., 2023). According to these authors, establishing redundancy is an effective approach to improve resilience and enable faster recovery from disruptions. Backup suppliers, transportation options, external subcontractors, and safety stocks are all examples of redundancy. They might be costly, but, overall, they help to redesign and improve the SC. The key factor influencing recovery is the existence of effective contingency plans, as well as collaborative efforts with partners to align the information used in implementing recovery policies (Messina et al., 2020). Hence, effective recovery is achieved through real-time data from physical SC operations, such as information from risk databases, IoT sensors, track-and-trace systems, and RFID (Al Ayed & Al Tit, 2023; Ivanov & Dolgui, 2021; Meng, 2021). The integration of disruption data with external risk data enables accurate simulation of how

different recovery policies would perform under current SC conditions. Analyzing the results of these simulations allows to compare different recovery policies' effectiveness. This process empowers data analytics to function as a proactive learning system that generates disruption scenarios to support the design and planning of resilient SC operations (Colicchia et al., 2011; Gao et al., 2020; Schlüter et al., 2017; Wu & Olson, 2008).

Discussion

This section synthesizes insights from the previous section to outline the transformations that are ongoing in SCRM due to the implementation of I4.0 technologies. We examine the implications of our empirical findings in SCRMA research with the lens of our three research questions. Given that this is the first thorough literature review on SCRMA, many of the following results are entirely new; however, we cited the papers in the extant literature that give confirmation of our findings.

Figure 6 synthesizes our empirical findings by presenting the percentage of the 51 SCRMA papers that we examined in depth that discuss each of the technologies in columns as a support for each of the SCRM phases in rows. This overview highlights both the technologies most frequently applied in SCRM and the stages of the process that have been the focus of prior research.

Research question 1—SCRMA process stages

Building on this overview, we address the first research question, "Which stage or activity within SCRM is most and least affected by Industry 4.0 technologies?." Our analysis reveals a strong imbalance across the five phases of risk management.

As shown in Fig. 6, the majority of contributions cluster around risk detection, assessment, and mitigation, while (especially) monitoring and handling have received comparatively little attention. This skew was expected because the earlier phases primarily involve data gathering, analysis, and processing, which are easier to automate with I4.0 technologies such as IoT, AI, ML, and BDA. By contrast, mitigation and handling involve a more decision-making and actions-oriented approach that is comparatively harder to digitize. From the analysis, it is evident that the progression from descriptive to prescriptive approaches remains limited, as prescriptive practices in risk mitigation and handling demand complex methods and advanced analytical tools, simulation models, and optimization frameworks. This pattern is consistent with prior work by Birkel and Hartmann (2020), Blome and Schoenherr (2011), and Spieske and Birkel (2021), who noted that monitoring, in particular, has been underexplored in the broader SCRM literature (none of these authors was speaking about SCRMA, however, but rather about SCRM). Automating this phase is particularly challenging due to the need to leverage a wide range of highly dynamic and often unstructured data sources, such as news, social media, or other real-time information sources. Thus, this phase requires hybrid technological approaches and infrastructure to monitor the complexity of interconnected SCs, which are still underdeveloped. Another reason why risk monitoring has received limited attention to date could be because its automation requires fulfilling the automation of previous phases. However, some progress has been made using AI, ML, and BDA to enable real-time risk assessment and proactive management, for instance, with advanced BDA used to exclude unqualified suppliers from bid solicitation while also leveraging social media to enhance first-tier visibility and mitigate reputational risks in the supply chain (Schroeder & Lodemann, 2021).

Risk handling also received a fair number of papers (half of our sample), but these seldom clarify how a specific technology group can support recovery phase activities, and most studies still focus on immediate response rather than long-term handling/recovery (Spieske & Birkel, 2021). However, AI is the most widely used technology for the response phase, but DTS can aid decision-making during

I4.0 Technologies SCRM phases	IoT	BDA	CC	AI/ML	BC	CPS	DTS	IR	AM	SCRM phase
Detection	22%	33%	8%	49%	12%	4%	2%	4%	6%	**78%**
Assessment	16%	22%	6%	45%	6%	2%	0%	4%	4%	**63%**
Mitigation	25%	39%	10%	39%	14%	4%	2%	4%	8%	**69%**
Monitoring	10%	14%	8%	18%	4%	2%	4%	0%	2%	**25%**
Handling	18%	27%	12%	27%	12%	2%	2%	2%	6%	**51%**
I4.0 technology	**29%**	**43%**	**14%**	**61%**	**14%**	**4%**	**4%**	**4%**	**8%**	

Fig. 6 Percentage of SCRMA articles dealing with each SCRM phase and I4.0 technology

both the response and recovery phases. So, research should focus on developing frameworks that leverage information to guide the choice of suitable recovery policies. However, the literature has not adequately addressed the importance of detecting disruptions to date (Messina et al., 2020), leaving considerable scope to design reliable automated systems to promptly identify disruptions and avoid delays in detection.

Research question 2—Support technologies

The second research question focused on identifying "Which I4.0 technologies are most useful in supporting different stages of SCRM?" The results show that AI and ML are the most widely applied technologies, appearing in a wide number of applications across all phases. The predominance of AI/ML is not surprising: first, because this family of technologies is currently experiencing global hype, and second, because their appeal lies in their ability to harvest dynamic, variable, and unstructured information from a wide variety of mostly unknown and frequently little trustable data sources, and, even more challenging than that, to give them a sense. For example, AI/ML techniques are particularly effective in risk detection, where they provide an alternative to expert-driven assessments, even when working with imbalanced datasets (Baryannis et al., 2019b). Applications include text mining to identify risks from external data (Chu et al., 2020; Shah et al., 2021), natural language processing to improve the efficiency of risk identification algorithms (Er Kara et al., 2020), and reinforcement learning and transformer-based models such as BERT, GPT, and T5 for dynamic decision-making (Baghalzadeh et al., 2024). For example, prewave is an AI-driven platform that integrates web crawling, natural language processing, and classification models to evaluate multi-tier supplier risks. By extracting insights from supply chain data, news sources, and social media, it generates early alerts on compliance threats, including environmental degradation, human rights violations, and corruption. Its deployment by leading manufacturers such as the Volkswagen and BMW Groups enhances supply chain transparency and enables proactive mitigation of operational and regulatory disruptions (Prewave, 2025). However, current AI/ML applications are largely limited to relatively simple scenarios, and their broader SCRMA potential remains underexplored. For example, future research could experiment with the usage of AI/ML techniques such as graph neural networks, support vector machines, or deep neural networks to automate the largely overlooked risk monitoring phase (Yang et al., 2023; Yang et al., 2024).

Following AI/ML, BDA and IoT represent the second and third most widely studied technologies. BDA is present across all phases but particularly in mitigation and handling, often with a descriptive rather than prescriptive focus. IoT follows, enabling the collection of valuable real-time data, which can then be ingested and processed by BDA and AI/ML. For example, in pharmaceutical supply chains, this reduced delivery delays by 20% (Wong et al., 2023), and in logistics firms such as DHL and FedEx, the combination of IoT and ML generates and analyzes large data pools, to optimize transportation and improve disruption visibility (Schroeder & Lodemann, 2021). Other technologies, such as CC, CPS, DTS, and BC, are less represented despite strong potential. CC could provide the infrastructure to handle, store, and ensure accessibility of real-time data required, especially in the mitigation, monitoring, and handling phases; accordingly, in our sample, these three phases are the most frequently treated by this technology. Despite its potential, authors argue that "data accessibility still poses some limitations" (Baghalzadeh et al., 2024; Chu et al., 2020), thus indicating space for further research on improving the ability to search, gather, and make sense of freely accessible or purchasable data. Yet, CC also raises issues regarding data quality and reliability, emphasizing that text cleaning, verification, and processing of input data are essential prerequisites to feed SCRMA analytics.

However, BC, CPS, and DTS highlight a thematic shift from isolated data processing toward system-wide intelligence, simulation, and trust-building. CPS embeds intelligence into physical objects and environments, enabling autonomous decisions, adaptation to changing conditions, and performance optimization. This is highly relevant to risk mitigation, handling, and monitoring, where decision-making is most intensive. However, their integration into supply chains set data security risks, highlighting the need for research on how CPS can contribute to SCRMA without putting valuable data at risk. DTS further enhances decision-making, as it is "often used to perform what-if analyses on complex systems fed with real-time data" (Ivanov & Dolgui, 2021). This enables quick responses in complex situations. DTS is especially promising in risk assessment, mitigation, monitoring, and handling phases, where its simulation capacity can reveal the effects of threats or perturbations.

BC adds value by certifying transactions and reducing information asymmetry, fraud, and improving trust. By connecting supply chain actors, BC enables the SC perspective to obtain more resilient and less failure-prone relations. It proves especially useful in risk prevention within the mitigation phase, in monitoring, and in handling, fostering resilience and trust across supply chain partners (Schlüter et al., 2017). Hence, CPS and DTS show promise for decision-intensive stages (Ivanov & Dolgui, 2021), and blockchain can reduce fraud and strengthen trust (Schlüter et al., 2017), yet empirical applications in SCRM are scarce.

More physical technologies such as AM and IR are almost absent from SCRMA studies despite their potential to enhance resilience. This limits our understanding of the

implementation of I4.0 in SCRM (Spieske et al., 2023), even though these technologies have been identified as promising opportunities to support future SCRMA advancements (Baryannis et al., 2019a). It is evident from the analysis that existing gaps in technological capability and organizational readiness create significant asymmetries in the adoption of Industry 4.0 technologies, often resulting in a skewed emphasis on particular or groups of technologies. The complex technologies such as CPS, DTS or BC face relatively higher implementation challenges compounded by limited interoperability, persistent data silos, and limited access to real-time connectivity. Hence, more research is needed on the practical applications and empirical research of these less discussed technologies (Kalbouneh et al., 2023; Mani et al., 2017; Schroeder & Lodemann, 2021).

Research question 3—Maturity level

Our third research question asks: **"**Which is the level of maturity achieved by the implementation of I4.0 technologies in SCRM?" The findings show that SCRMA is still at a relatively early stage of development, with most studies fragmented, experimental, and technology-push rather than systematically integrated.

Risk detection is the most developed area, with more than three-quarters of reviewed papers addressing it. This suggests tangible progress toward business applications, although current frameworks often neglect the dynamic nature of risks. For instance, geopolitical and microeconomic risks gained attention only after the COVID-19 pandemic (Chu et al., 2020; Park & Singh, 2023). Reputational, policy, and regulatory risks particularly related to sustainability also remain underexplored (Mani et al., 2017). Furthermore, nuanced approaches to risk classification remain underdeveloped in areas such as cyber threats (Deiva Ganesh & Kalpana, 2022a; Tang & Nurmaya Musa, 2011).

The risk assessment phase shows moderate maturity. Conceptual models for risk assessment tools in evaluating the likeliness and the magnitude of their SC risks are well established, yet the literature lacks comprehensive frameworks that thoroughly address risk antecedents, key vulnerabilities, and the interconnectedness of various risks, underscoring the need for a more holistic approach to risk assessment. By the same token, while literature largely measures risks in financial terms, future studies should also address intangible losses such as credibility, reputation, authority, and trust. Moreover, the scarcity of empirical case studies restricts practical implementation, leaving a gap between theory and application (Al Ayed & Al Tit, 2023; Birkel & Hartmann, 2020; Fischer et al., 2020).

Risk mitigation research is less mature, despite being covered by more than two-thirds of the scrutinized studies. Technological improvements in detection and assessment have not translated into faster or more effective mitigation strategies. Similarly, risk handling and monitoring remain in their infancy, with limited evidence of business-ready applications and frameworks.

Yet, by looking at the big picture that emerges from our literature review, instead of focusing on single phases or technologies within the SCRMA process, some other and more fundamental flaws of extant research emerge in full light. For instance, a relevant limitation found in the scrutinized papers is that most contributions rely on single technologies. Only limited literature explores hybrid approaches integrating multiple methods (Jegan et al., 2024). Mirroring this failure of extant literature to exploit integration and interoperability among different technologies, we also experienced a lack of integrated approaches encompassing all or several phases of the SCRM process. Out of 51 papers, just one (Deiva Ganesh & Kalpana, 2022a) attempted a comprehensive approach addressing all key SCRM phases, which highlights that the current state of research has not embraced an integrated approach yet. Thus, it emerges that the current literature is fragmented across phases and technology applications, with little integration, which opens up a wide space to develop research in more encompassing and integrated approaches. Hybrid models integrating multiple data sources and technologies could provide a more comprehensive approach to risk management (De Assis Santos & Marques, 2022; Kassa et al., 2023), though this remains another area open to further investigation.

Although some research has addressed the application of digital technologies to individual risks, considerably less attention has been given to analyzing the interactions and interdependencies among different risks, despite their correlated nature. For example, if a financially weak supplier operates in a geopolitically risky country, it is not clear whether its weak financial statements already incorporate the difficulty of operating in such a risky environment, or whether this condition should further increase the likelihood of supply interruption. Only a few recent contributions (Gao et al., 2020; Mittal & Panchal, 2023; Spieske et al., 2023) have begun to explore cross-risk interactions. So, developing cross-risk models remains a promising avenue for future research.

Moreover, most SCRM research has been conducted primarily from the perspective of a focal firm, with limited attention to inter-organizational relationships. Yet, firms are not only concerned with their tier-1 suppliers but increasingly require visibility across their entire supply chain. Despite this, research on the impact of SCRMA at the broader supply chain level is limited, and further empirical evidence and more integrated and encompassing theoretical models are needed to understand how digital technologies can help manage disruptions and risks across whole SCs. Overcoming this limitation might require the

use of both qualitative and quantitative data, which can support broader exploration and application of advanced analytics (Raman et al., 2023). DTS technologies could help to reinforce our handling of complex relationships among different risks or firms along the SC, so aiming SCRMA research towards a more holistic direction.

Further, very few of the scrutinized studies include real-world case applications, limiting the practical transferability of findings (Aljabhan, 2023; Gao et al., 2020; Kosasih et al., 2024; Schlüter et al., 2017). These findings suggest that SCRMA has not yet matured to a point where technologies can reliably support practically usable solutions. Advancing maturity will require empirical case-based studies, hybrid models, and inter-organizational approaches that consider multi-tier supply chains.

Finally, the literature highlights that while SCRMA aims to prevent costly disruptions, implementing I4.0 technologies can come with even higher costs than those connected to potentially mitigated risks and therefore raise doubts related to their returns on investment. Approaches such as Extended Performance Analysis have been proposed to evaluate returns on RFID adoption (Schlüter et al., 2017), but further research is required to establish robust cost–benefit frameworks, to assess the trade-offs between costs and benefits, before businesses can be fully confident to invest in these systems.

Putting all these limitations together and further considering that many of the most-used technologies are quite obviously in their infancy, it is shown that the maturity of the field is still low, not just in terms of technological adoption but also in conceptual and empirical development.

Conclusion and main contributions

This paper explores how I4.0 technologies can improve SCRM, using a two-level structured literature review on SCRMA: we firstly used a set of 171 papers to perform a descriptive analysis and then restricted our selection to 51 to perform a more detailed content analysis. To our best knowledge, it is the first thorough SCRMA literature review issued to date. We explored the 51 selected papers with the lens of the five typical SCRM phases: detection, assessment, mitigation, monitoring, and handling of risks. For each, we identified and discussed the data gathered, the algorithms and models through which it is processed, and the specific 4.0 technologies used to do so.

We discuss the main takeaways of this study in two sections dedicated to theoretical and managerial implications, and then, we present the main limitations of this study.

Theoretical implications

This study contributes to the enhancement of SCRMA theoretical knowledge in three main ways. The first one is by setting a clear, complete, and up-to-date status-of-the art of research on this discipline. Our 171 papers-strong descriptive analysis showed that SCRMA research is experiencing a hype in terms of the number of publications issued in scientific papers and illustrated that this is happening mainly in operations management journals. Our detailed content analysis advances the theoretical understanding of how the five phases of SCRM are digitalized through nine focal Industry 4.0 technology families. We found that AI/ML, BDA, and IoT are the most used technology families, especially adopted within the detection, assessment, and mitigation phases. On the grounds of this detailed map, the review presents a novel theoretical distinction between phases readily digitalized and conceptually nascent phases that are harder to digitalize. Detection and assessment, which primarily involve information gathering and analysis, are naturally suited to data collection and processing technologies (Das et al., 2025) such as AI, IoT, and BDA. Mitigation and handling, in contrast, involve complex decision-making and action, making them harder to digitize. This distinction contributes to theory by clarifying that digitalization is not uniform across phases but contingent upon the cognitive and operational demands of each stage. It helps explain why progress is clustered in early phases, while later stages require more advanced and integrated technological approaches.

The second valuable result of our study is to highlight the main gaps that emerge from our literature review. By systematically mapping technologies across phases, we clarified the differential of suitability in adoption. We identified largely overlooked technologies such as DTS, CPS, and BC, which hold significant promise for advancing decision-making in SCRMA. Moreover, our study highlights that existing literature is disproportionately focused on early phases of risk management (risk detection and assessment) (Blome & Schoenherr, 2011; Spieske & Birkel, 2021), with far less attention to monitoring and handling. Yet, the most relevant gaps of the extant research body emerge more from a holistic view, rather than from these specific drilldowns. For instance, we found that often I4.0 technologies are used in isolation, without systematically linking them to some/all SCRM phases (Baryannis et al., 2019b; Ivanov & Dolgui, 2021). By the same token, we also found a relative lack of hybrid approaches adopting several I4.0 techniques together, while studies focused on just one or a few technologies abound. Moreover, this study highlights the limited attention dedicated to inter-organizational relationships, particularly in multi-tier supply chains and cross-supplier dynamics in SCRMA (Mittal & Panchal, 2023; Schroeder & Lodemann,

2021). Another clear gap of the extant research is the minimal number of practical case studies that we found in the 51 examined papers (Aljabhan, 2023; Gao et al., 2020; Kosasih et al., 2024). Overall, these gaps point to the fact that researchers are just beginning to develop digital applications of SCRM, and thus we are still assisting to an initial, technology-push SCRMA phase.

Finally, our study advances the discussion by focusing on the gaps identified in existing studies which highlights the main paths to deliver new and fruitful SCRMA research. The most obvious findings here are about the SCRMA process phases and technologies that were found to be most overlooked by extant research. In fact, mainly decision-intensive phases such as monitoring and handling remain underexplored despite their critical importance, revealing a theoretical blind spot and creating avenues for advancing literature. Moreover, intensifying research on DTS, CPS, and BC technologies could establish a wider and clearer theoretical basis for understanding which technologies can be integrated in SCRMA, and which will remain just conceptual opportunities. But by far the most promising research paths that leave plenty of room for researchers to deliver new and fresh insights are to develop new theoretical models and case studies approaching SCRMA with a wider multi-tier, multi-risk, and multi-technique approach and to build resilient, anti-fragile, and adaptive systems against disruptions.

Managerial implications

Our findings highlight several key business implications as well. First, technology selection should align with the specific requirements of each SCRM phase. For example, in the context of risk detection and assessment, AI/ML, IoT, and BDA have received the most research attention and provide businesses with actionable insights. Hence, Firms can leverage these technologies to enhance the identification of risks. Managers should be aware, however, that existing frameworks often overlook the dynamic nature of and the interconnections among risks, necessitating careful adaptation of technological tools to address both tangible and intangible impacts.

Second, decision-intensive stages such as mitigation, monitoring, and handling require more advanced technologies, like digital twins, CPS, and blockchain. Although risk mitigation and handling have received some research attention, the field remains nascent, and empirical evidence on practical applications is limited. Managers should therefore avoid uniform adoption strategies and instead tailor technology choices to the distinct needs and maturity of each SCRM phase. Incremental adoption, through pilot projects and small-scale experiments, is recommended to test technologies, refine processes, and minimize risks before scaling up. Successful applications in logistics monitoring, where IoT and AI have improved responsiveness, illustrate the value of gradual adoption.

Third, investment decisions must carefully consider cost–benefit trade-offs. While I4.0 technologies can reduce disruptions and enhance resilience, they require substantial upfront resources, and their returns are not guaranteed, particularly for less mature SCRM phases such as risk handling and monitoring. Firms should evaluate both tangible outcomes (e.g., reduced delays) and intangible benefits (e.g., reputation, trust, and credibility) when assessing potential returns. Frameworks such as Extended Performance Analysis (Schlüter et al., 2017) can support these evaluations but may require further adaptation to account for the full range of economic, operational, and reputational impacts.

Finally, supply chain resilience requires collaboration across organizational boundaries. Most research focuses on focal firms, yet disruptions often cascade across multiple tiers. Managers should therefore prioritize visibility beyond tier-one suppliers, using technologies such as IoT and blockchain to strengthen transparency and coordination. Collaborative initiatives can also help address persistent challenges related to data quality, interoperability, and trust, which remain critical obstacles in translating research insights into effective business practice.

Overall, the above-described context confirms a relatively low level of SCRMA maturity, with scientific papers starting to ramp up in the last 4–5 years, many different and frequently unrelated approaches attempted, scarcity of consequentiality, and lack of integration. This is further confirmed by the industrial context, where companies struggle to apply SCRMA technologies due to data-related challenges, including inconsistent quality, limited availability, and integration difficulties with existing systems, resulting in a lack of visibility (Mittal & Panchal, 2023; Schroeder & Lodemann, 2021).

Limitations

Despite the rich set of findings it provides, this study is not without limitations. We think that these limitations should be taken into consideration by readers to appropriately evaluate above-discussed takeaways. First, our findings are based solely on peer-reviewed international journal articles, excluding grey literature and conference papers.

Additionally, the study considers only nine technology families; thus, incorporating other relevant technologies could be a valuable extension for future research. As an extension of I4.0, Industry 5.0 should be explored in future research as a complementary to SCRMA, leveraging human–machine synergy to incorporate human insight into digital models for more effective responses to disruptions

like geopolitical events or climate-related crises. It better supports risk handling and risk mitigation, where more complex decisions are made.

Furthermore, the current study primarily focuses on supply chain and management perspectives, while a deeper analysis of the technologies themselves could offer further insights and enrich the understanding of their capabilities and limitations.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s12525-025-00844-1.

Data Availability The detailed data used in this paper is available upon request to the authors.

Declarations

Competing interest None.

References

Al Ayed, S. I., & Al Tit, A. A. (2023). The effect of supply chain risk management on supply chain resilience: The intervening part of Internet-of-Things. *Uncertain Supply Chain Management, 11*(1), 179–186. https://doi.org/10.5267/j.uscm.2022.10.009

Aljabhan, B. (2023). Economic strategic plans with supply chain risk management (SCRM) for organizational growth and development. *Alexandria Engineering Journal, 79*, 411–426. https://doi.org/10.1016/j.aej.2023.08.020

Aljohani, A. (2023). Predictive analytics and machine learning for real-time supply chain risk mitigation and agility. *Sustainability, 15*(20), Article 15088. https://doi.org/10.3390/su152015088

Aqlan, F., & Lam, S. S. (2015a). Fuzzy-based integrated framework for supply chain risk assessment. *International Journal of Production Economics, 161*, 54–63. https://doi.org/10.1016/j.ijpe.2014.11.013

Aqlan, F., & Lam, S. S. (2015b). Supply chain risk modelling and mitigation. *International Journal of Production Research, 53*(18), 5640–5656. https://doi.org/10.1080/00207543.2015.1047975

Arkestro. (2021). BASF, UCB Biopharma, and Dover Chemical leverage Bid Ops predictive sourcing AI to predict and win faster savings: Three case studies. Arkestro. https://arkestro.com/blog/basf-ucb-biopharma-and-dover-chemical-leverage-bid-ops-predictive-sourcing-ai-to-predict-and-win-faster-savings-three-case-studies/

Baghalzadeh, S. M., Moehler, R. C., Fang, Y., Aboutorab, H., & Hijazi, A. A. (2024). Construction supply chain risk management. *Automation in Construction, 162*, 105396. https://doi.org/10.1016/j.autcon.2024.105396

Baryannis, G., Dani, S., & Antoniou, G. (2019a). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. *Future Generation Computer Systems, 101*, 993–1004. https://doi.org/10.1016/j.future.2019.07.059

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019b). Supply chain risk management and artificial intelligence: State of the art and future research directions. *International Journal of Production Research, 57*(7), 2179–2202. https://doi.org/10.1080/00207543.2018.1530476

Berger, N., Schulze-Schwering, S., Long, E., & Spinler, S. (2023). Risk management of supply chain disruptions: An epidemic modeling approach. *European Journal of Operational Research, 304*(3), 1036–1051. https://doi.org/10.1016/j.ejor.2022.05.018

Birkel, H. S., & Hartmann, E. (2020). Internet of things – The future of managing supply chain risks. *Supply Chain Management, An International Journal, 25*(5), 535–548. https://doi.org/10.1108/SCM-09-2019-0356

Blome, C., & Schoenherr, T. (2011). Supply chain risk management in financial crises—A multiple case-study approach. *International Journal of Production Economics, 134*(1), 43–57. https://doi.org/10.1016/j.ijpe.2011.01.002

Blos, M. F., Hoeflich, S. L., & Miyagi, P. E. (2015). A general supply chain continuity management framework. *Procedia Computer Science, 55*, 1160–1164. https://doi.org/10.1016/j.procs.2015.07.087

Chen, J., Sohal, A. S., & Prajogo, D. I. (2013). Supply chain operational risk mitigation: A collaborative approach. *International Journal of Production Research, 51*(7), 2186–2199. https://doi.org/10.1080/00207543.2012.727490

Chenger, D., & Pettigrew, R. N. (2023). Leveraging data-driven decisions: A framework for building intracompany capability for supply chain optimization and resilience. *Supply Chain Management, an International Journal, 28*(6), 1026–1039. https://doi.org/10.1108/SCM-12-2022-0464

Chowdhury, M. M. H., & Quaddus, M. (2016). Supply chain readiness, response and recovery for resilience. *Supply Chain Management, an International Journal, 21*(6), 709–731. https://doi.org/10.1108/SCM-12-2015-0463

Chu, C. Y., Park, K., & Kremer, G. E. (2020). A global supply chain risk management framework: An application of text-mining to identify region-specific supply chain risks. *Advanced Engineering Informatics, 45*, Article 101053. https://doi.org/10.1016/j.aei.2020.101053

Cigolini, R., Cozzi, M., & Perona, M. (2004). A new framework for supply chain management. *International Journal of Operations & Production Management, 24*(1), 7–41. https://doi.org/10.1108/01443570410510979

Colicchia, C., Dallari, F., & Melacini, M. (2011). A simulation-based framework to evaluate strategies for managing global inbound supply risk. *International Journal of Logistics Research and Applications, 14*(6), 371–384. https://doi.org/10.1080/13675567.2011.644270

Cooper, M. C., & Ellram, L. M. (1993). Characteristics of supply chain management and the implications for purchasing and logistics strategy. *The International Journal of Logistics Management, 4*(2), 13–24. https://doi.org/10.1108/09574099310804957

Das, S. K., Saccani, N., & Bressanelli, G. (2025). How do digital technologies trigger sustainability and circularity in operations management processes? The role of environmental drivers. *Business Process Management Journal*. https://doi.org/10.1108/BPMJ-05-2025-0653

De Assis Santos, L., & Marques, L. (2022). Big data analytics for supply chain risk management: Research opportunities at process crossroads. *Business Process Management Journal, 28*(4), 1117–1145. https://doi.org/10.1108/BPMJ-01-2022-0012

Deiva Ganesh, A., & Kalpana, P. (2022a). Future of artificial intelligence and its influence on supply chain risk management – A systematic review. *Computers & Industrial Engineering, 169*, 108206. https://doi.org/10.1016/j.cie.2022.108206

Deiva Ganesh, A., & Kalpana, P. (2022b). Supply chain risk identification: A real-time data-mining approach. *Industrial Management & Data Systems, 122*(5), 1333–1354. https://doi.org/10.1108/IMDS-11-2021-0719

Dong, Q., & Cooper, O. (2016). An orders-of-magnitude AHP supply chain risk assessment framework. *International Journal of Production Economics, 182*, 144–156. https://doi.org/10.1016/j.ijpe.2016.08.021

Duong, A. T. B., Hoang, T.-H., Nguyen, T. T. B., Akbari, M., Hoang, T. G., & Truong, H. Q. (2023). Supply chain risk assessment in disruptive times: Opportunities and challenges. *Journal of Enterprise Information Management, 36*(5), 1372–1401. https://doi.org/10.1108/JEIM-02-2023-0104

Durach, C. F., Kembro, J. H., & Wieland, A. (2021). How to advance theory through literature reviews in logistics and supply chain management. *International Journal of Physical Distribution & Logistics Management, 51*(10), 1090–1107. https://doi.org/10.1108/IJPDLM-11-2020-0381

El Baz, J., & Ruel, S. (2021). Can supply chain risk management practices mitigate the disruption impacts on supply chains' resilience and robustness? Evidence from an empirical survey in a COVID-19 outbreak era. *International Journal of Production Economics, 233*, Article 107972. https://doi.org/10.1016/j.ijpe.2020.107972

Emrouznejad, A., Abbasi, S., & Sıcakyüz, Ç. (2023). Supply chain risk management: A content analysis-based review of existing and emerging topics. *Supply Chain Analytics, 3*, Article 100031. https://doi.org/10.1016/j.sca.2023.100031

Er Kara, M., OktayFırat, S. Ü., & Ghadge, A. (2020). A data mining-based framework for supply chain risk management. *Computers & Industrial Engineering, 139*, 105570. https://doi.org/10.1016/j.cie.2018.12.017

Fischer, P. D., Eismann, K., Pietrowski, R., Fischbach, K., & Schoder, D. (2020). Information technology and risk management in supply chains. *International Journal of Physical Distribution & Logistics Management, 50*(2), 233–254. https://doi.org/10.1108/IJPDLM-04-2019-0119

Frank, A. G., Dalenogare, L. S., & Ayala, N. F. (2019). Industry 4.0 technologies: Implementation patterns in manufacturing companies. *International Journal of Production Economics, 210*, 15–26. https://doi.org/10.1016/j.ijpe.2019.01.004

Gao, Q., Guo, S., Liu, X., Manogaran, G., Chilamkurti, N., & Kadry, S. (2020). Simulation analysis of supply chain risk management system based on IoT information platform. *Enterprise Information Systems, 14*(9–10), 1354–1378. https://doi.org/10.1080/17517575.2019.1644671

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics, 90*(1), 47–58. https://doi.org/10.1016/j.ijpe.2004.02.007

Hallikas, J., & Lintukangas, K. (2016). Purchasing and supply: An investigation of risk management performance. *International Journal of Production Economics, 171*, 487–494. https://doi.org/10.1016/j.ijpe.2015.09.013

Hallikas, J., Virolainen, V.-M., & Tuominen, M. (2002). Risk analysis and assessment in network environments: A dyadic case study. *International Journal of Production Economics, 78*(1), 45–55. https://doi.org/10.1016/S0925-5273(01)00098-6

Handfield, R., Sun, H., & Rothenberg, L. (2020). Assessing supply chain risk for apparel production in low cost countries using newsfeed analysis. *Supply Chain Management: An International Journal, 25*(6), 803–821. https://doi.org/10.1108/SCM-11-2019-0423

Harland, C., Brenchley, R., & Walker, H. (2003). Risk in supply networks. *Journal of Purchasing and Supply Management, 9*(2), 51–62. https://doi.org/10.1016/S1478-4092(03)00004-9

Heckmann, I., Comes, T., & Nickel, S. (2015). A critical review on supply chain risk – Definition, measure and modeling. *Omega, 52*, 119–132. https://doi.org/10.1016/j.omega.2014.10.004

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research, 53*(16), 5031–5069. https://doi.org/10.1080/00207543.2015.1030467

Hoffmann, P., Schiele, H., & Krabbendam, K. (2013). Uncertainty, supply risk management and their impact on performance. *Journal of Purchasing and Supply Management, 19*(3), 199–211. https://doi.org/10.1016/j.pursup.2013.06.002

Hsu, C. H., Li, M. G., Zhang, T. Y., Chang, A. Y., Shangguan, S. Z., & Liu, W. L. (2022). Deploying big data enablers to strengthen supply chain resilience to mitigate sustainable risks based on integrated HOQ-MCDM framework. *Mathematics, 10*(8), Article 1233. https://doi.org/10.3390/math10081233

Hult, G. T. M., Craighead, C. W., & Ketchen, D. J., Jr. (2010). Risk uncertainty and supply chain decisions: A real options perspective. *Decision Sciences, 41*(3), 435–458. https://doi.org/10.1111/j.1540-5915.2010.00276.x

Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning and ContrOl, 32*(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

Ivanov, D., Dolgui, A., & Sokolov, B. (2019). The impact of digital technology and industry 4.0 on the ripple effect and supply chain risk analytics. *International Journal of Production Research, 57*(3), 829–846. https://doi.org/10.1080/00207543.2018.1488086

Jegan, J. J. J., Sonwaney, V., Bryde, D., & Graham, G. (2024). Achieving competitive advantage through technology-driven proactive supply chain risk management: An empirical study. *Annals of Operations Research, 332*(1–3), 149–190. https://doi.org/10.1007/s10479-023-05604-y

Jüttner, U. (2005). Supply chain risk management. *The International Journal of Logistics Management, 16*(1), 120–141. https://doi.org/10.1108/09574090510617385

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: Outlining an agenda for future research. *International Journal of Logistics Research and Applications, 6*(4), 197–210. https://doi.org/10.1080/1367556031000162716

Kalbouneh, N. Y., Bataineh, K. A., Al-Hamad, A.A.-S.A., Dwakat, M. K. A., Abualoush, S., Almasarweh, M. S., & Al-Smadi, R. W. (2023). The effects of the blockchain technology and big data analytics on supply chain performance: The mediating effect supply chain risk management. *Uncertain Supply Chain Management, 11*(3), 903–914. https://doi.org/10.5267/j.uscm.2023.5.008

Kassa, A., Kitaw, D., Stache, U., Beshah, B., & Degefu, G. (2023). Artificial intelligence techniques for enhancing supply chain resilience: A systematic literature review, holistic framework, and future research. *Computers & Industrial Engineering, 186*, 109714. https://doi.org/10.1016/j.cie.2023.109714

Ketchen, D. J., & Craighead, C. W. (2023). What constitutes an excellent literature review? Summarize, synthesize, conceptualize, and energize. *Journal of Business Logistics, 44*(2), 164–169. https://doi.org/10.1111/jbl.12339

Kosasih, E. E., Margaroli, F., Gelli, S., Aziz, A., Wildgoose, N., & Brintrup, A. (2024). Towards knowledge graph reasoning for supply chain risk management using graph neural networks. *International Journal of Production Research, 62*(15), 5596–5612. https://doi.org/10.1080/00207543.2022.2100841

Krolas, P., & Krolas L. (2010). *Risk in management systems according to ISO Standard* (Special Issue 3, Vol. 10). Archives of Foundry Engineering.

Kumar, S., & Sharma, S. C. (2023). Integrated model for predicting supply chain risk through machine learning algorithms. *International Journal of Mathematical, Engineering and Management Sciences, 8*(3), 353–373. https://doi.org/10.33889/IJMEMS.2023.8.3.021

Li, L., Gong, Y., Wang, Z., & Liu, S. (2023). Big data and big disaster: A mechanism of supply chain risk management in global logistics industry. *International Journal of Operations & Production Management, 43*(2), 274–307. https://doi.org/10.1108/IJOPM-04-2022-0266

Li, S., Sun, Q., & Liu, S. (2021). Risk assessment for supply chain based on cloud model. *Journal of Intelligent & Fuzzy Systems, 41*(2), 3523–3540. https://doi.org/10.3233/JIFS-210883

Liu, M., Liu, Z., Chu, F., Zheng, F., & Chu, C. (2021). A new robust dynamic Bayesian network approach for disruption risk assessment under the supply chain ripple effect. *International Journal of Production Research, 59*(1), 265–285. https://doi.org/10.1080/00207543.2020.1841318

Lu, Y. (2017). Industry 4.0: A survey on technologies, applications and open research issues. *Journal Of Industrial Information Integration, 6*, 1–10. https://doi.org/10.1016/j.jii.2017.04.005

Mani, V., Delgado, C., Hazen, B., & Patel, P. (2017). Mitigating supply chain risk via sustainability using big data analytics: Evidence from the manufacturing supply chain. *Sustainability, 9*(4), Article 608. https://doi.org/10.3390/su9040608

Marsh. (2025). Sentrisk™. Marsh. https://www.marsh.com/en/services/business-interruption-supply-chain/expertise/sentrisk.html

Meng, L. (2021). Using IoT in supply chain risk management, to enable collaboration between business, community, and government. *Smart Cities, 4*(3), 995–1003. https://doi.org/10.3390/smartcities4030052

Messina, D., Barros, A. C., Soares, A. L., & Matopoulos, A. (2020). An information management approach for supply chain disruption recovery. *The International Journal of Logistics Management, 31*(3), 489–519. https://doi.org/10.1108/IJLM-11-2018-0294

Meyer, M. M., Glas, A. H., & Eßig, M. (2022). A delphi study on the supply risk-mitigating effect of additive manufacturing during SARS-COV-2. *Journal of Purchasing and Supply Management, 28*(4), Article 100791. https://doi.org/10.1016/j.pursup.2022.100791

Micheli, G. J. L. (2008). A decision-maker-centred supplier selection approach for critical supplies. *Management Decision, 46*(6), 918–932. https://doi.org/10.1108/00251740810882671

Micheli, G. J. L., Cagno, E., & Di Giulio, A. (2009). Reducing the total cost of supply through risk-efficiency-based supplier selection in the EPC industry. *Journal of Purchasing and Supply Management, 15*(3), 166–177. https://doi.org/10.1016/j.pursup.2009.05.001

Micheli, G. J. L., Cagno, E., & Zorzini, M. (2008). Supply risk management vs supplier selection to manage the supply risk in the EPC supply chain. *Management Research News, 31*(11), 846–866. https://doi.org/10.1108/01409170810913042

Miller, K. D. (1992). A framework for integrated risk management in international business. *Journal of International Business Studies, 23*(2), 311–331. https://doi.org/10.1057/palgrave.jibs.8490270

Mishra, D., Sharma, R. R. K., Kumar, S., & Dubey, R. (2016). Bridging and buffering: Strategies for mitigating supply risk and improving supply chain performance. *International Journal of Production Economics, 180*, 183–197. https://doi.org/10.1016/j.ijpe.2016.08.005

Mittal, U., & Panchal, D. (2023). AI-based evaluation system for supply chain vulnerabilities and resilience amidst external shocks: An empirical approach. *Reports in Mechanical Engineering, 4*(1), 276–289. https://doi.org/10.31181/rme040122112023m

Ojala, M., & Hallikas, J. (2006). Investment decision-making in supplier networks: Management of risk. *International Journal of Production Economics, 104*(1), 201–213. https://doi.org/10.1016/j.ijpe.2005.03.006

Park, M., & Singh, N. P. (2023). Predicting supply chain risks through big data analytics: Role of risk alert tool in mitigating business disruption. *Benchmarking: An International Journal, 30*(5), 1457–1484. https://doi.org/10.1108/BIJ-03-2022-0169

Pettit, T. J., Croxton, K. L., & Fiksel, J. (2013). Ensuring supply chain resilience: Development and implementation of an assessment tool. *Journal of Business Logistics, 34*(1), 46–76. https://doi.org/10.1111/jbl.12009

Pournader, M., Kach, A., & Talluri, S. (2020). A review of the existing and emerging topics in the supply chain risk management literature. *Decision Sciences, 51*(4), 867–919. https://doi.org/10.1111/deci.12470

Prewave. (2025). Identifying sustainability risks: Audi, Porsche, and Volkswagen use Prewave to monitor their supply chain. Prewave. https://www.prewave.com/cases/audi-porsche-volkswagen

Qazi, A., Dickson, A., Quigley, J., & Gaudenzi, B. (2018). Supply chain risk network management: A bayesian belief network and expected utility based approach for managing supply chain risks. *International Journal of Production Economics, 196*, 24–42. https://doi.org/10.1016/j.ijpe.2017.11.008

Rafi, U. S. P. M., Bashiri, M., Kamal, M. M., Mangla, S. K., & Tjahjono, B. (2024). An analysis of fuzzy group decision making to adopt emerging technologies for fashion supply chain risk management. *IEEE Transactions on Engineering Management, 71*, 8469–8487. https://doi.org/10.1109/TEM.2024.3354845

Raman, P., Seetha, R., Sankar, S., Suresh, K., Arunkumar, R., & Mohanaprakash, T. A. (2023). Cuckoo search support vector machine for supply chain risk management. *Journal of Theoretical and Applied Information Technology*, *101*(1). https://jatit.org/volumes/Vol101No1/9Vol101No1.pdf

Rangel, D. A., de Oliveira, T. K., & Leite, M. S. A. (2015). Supply chain risk classification: Discussion and proposal. *International Journal of Production Research, 53*(22), 6868–6887. https://doi.org/10.1080/00207543.2014.910620

Rauniyar, K., Wu, X., Gupta, S., Modgil, S., de Sousa, L., & Jabbour, A. B. (2023). Risk management of supply chains in the digital transformation era: Contribution and challenges of blockchain technology. *Industrial Management & Data Systems, 123*(1), 253–277. https://doi.org/10.1108/IMDS-04-2021-0235

Rezki, N., & Mansouri, M. (2023). Improving supply chain risk assessment with artificial neural network predictions. *Acta Logistica, 10*(04), 645–658. https://doi.org/10.22306/al.v10i4.444

Russmann, M. M. P. (2015). *Industry 4.0: The future of productivity and growth in manufacturing industries*.

Samvedi, A., Jain, V., & Chan, F. T. S. (2013). Quantifying risks in a supply chain through integration of fuzzy AHP and fuzzy TOPSIS. *International Journal of Production Research, 51*(8), 2433–2442. https://doi.org/10.1080/00207543.2012.741330

Schlüter, F. F., Hetterscheid, E., & Henke, M. (2017). A simulation-based evaluation approachfor digitalization scenarios in smart supply chain risk management. *Journal of Industrial Engineering and Management Science, 2017*(1), 179–206. https://doi.org/10.13052/jiems2446-1822.2017.009

Schroeder, M., & Lodemann, S. (2021). A systematic investigation of the integration of machine learning into supply chain risk

management. *Logistics, 5*(3), Article 62. https://doi.org/10.3390/logistics5030062

Shah, H. M., Gardas, B. B., Narwane, V. S., & Mehta, H. S. (2023). The contemporary state of big data analytics and artificial intelligence towards intelligent supply chain risk management: A comprehensive review. *Kybernetes, 52*(5), 1643–1697. https://doi.org/10.1108/K-05-2021-0423

Shah, S. M., Lütjen, M., & Freitag, M. (2021). Text mining for supply chain risk management in the apparel industry. *Applied Sciences, 11*(5), Article 2323. https://doi.org/10.3390/app11052323

Shekarian, M., & Mellat Parast, M. (2021). An integrative approach to supply chain disruption risk and resilience management: A literature review. *International Journal of Logistics Research and Applications, 24*(5), 427–455. https://doi.org/10.1080/13675567.2020.1763935

Siemens. (2025). Power up: Digital risk twin analysis. Simcenter Blog. https://blogs.sw.siemens.com/simcenter/power-up-digital-risk-twin-analysis/#section_7

Singh, N. P., & Singh, S. (2019). Building supply chain risk resilience. *Benchmarking: An International Journal, 26*(7), 2318–2342. https://doi.org/10.1108/BIJ-10-2018-0346

Sodhi, M. S., Son, B., & Tang, C. S. (2012). Researchers' perspectives on supply chain risk management. *Production and Operations Management, 21*(1), 1–13. https://doi.org/10.1111/j.1937-5956.2011.01251.x

Spieske, A., & Birkel, H. (2021). Improving supply chain resilience through Industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. *Computers & Industrial Engineering, 158*, 107452. https://doi.org/10.1016/j.cie.2021.107452

Spieske, A., Gebhardt, M., Kopyto, M., Birkel, H., & Hartmann, E. (2023). The future of industry 4.0 and supply chain resilience after the COVID-19 pandemic: Empirical evidence from a delphi study. *Computers & Industrial Engineering, 181*, 109344. https://doi.org/10.1016/j.cie.2023.109344

Tang, O., & Nurmaya Musa, S. (2011). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Economics, 133*(1), 25–34. https://doi.org/10.1016/j.ijpe.2010.06.013

Thun, J. H., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics, 131*(1), 242–249. https://doi.org/10.1016/j.ijpe.2009.10.010

Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. *Journal of Business Research, 122*, 502–517. https://doi.org/10.1016/j.jbusres.2020.09.009

Tran, T.H., Dobrovnik, M. & Kummer, S. (2018). Supply chain risk assessment: a content analysis-based literature review. *International Journal of Logistics Systems and Management, 31*(4), 562–591. https://doi.org/10.1504/IJLSM.2018.096088

Tranfield, D., Denyer, D., & 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. https://doi.org/10.1111/1467-8551.00375

Tukamuhabwa, B., Stevenson, M., & Busby, J. (2017). Supply chain resilience in a developing country context: A case study on the interconnectedness of threats, strategies and outcomes. *Supply Chain Management, an International Journal, 22*(6), 486–505. https://doi.org/10.1108/SCM-02-2017-0059

Wagner, S. M., & Bode, C. (2006). An empirical investigation into supply chain vulnerability. *Journal of Purchasing and Supply Management, 12*(6), 301–312. https://doi.org/10.1016/j.pursup.2007.01.004

Wang, Y., Gilland, W., & Tomlin, B. (2010). Mitigating supply risk: Dual sourcing or process improvement? *Manufacturing & Service Operations Management, 12*(3), 489–510. https://doi.org/10.1287/msom.1090.0279

Wieland, A., & Wallenburg, C. M. (2012). Dealing with supply chain risks. *International Journal of Physical Distribution & Logistics Management, 42*(10), 887–905. https://doi.org/10.1108/09600031211281411

Wiengarten, F., Humphreys, P., Gimenez, C., & McIvor, R. (2016). Risk, risk management practices, and the success of supply chain integration. *International Journal of Production Economics, 171*, 361–370. https://doi.org/10.1016/j.ijpe.2015.03.020

Wong, C. Y. (2021). Can a descriptive literature review advance knowledge? *International Journal of Physical Distribution & Logistics Management, 51*(3), 205–211. https://doi.org/10.1108/IJPDLM-04-2021-410

Wong, W. P., Saw, P. S., Jomthanachai, S., Wang, L. S., Ong, H. F., & Lim, C. P. (2023). Digitalization enhancement in the pharmaceutical supply network using a supply chain risk management approach. *Scientific Reports, 13*(1), Article 22287. https://doi.org/10.1038/s41598-023-49606-z

Wu, D., & Olson, D. L. (2008). Supply chain risk, simulation, and vendor selection. *International Journal of Production Economics, 114*(2), 646–655. https://doi.org/10.1016/j.ijpe.2008.02.013

Wu, M., Fu, C., Holguin-veras, J., Enz, M. G., & Mondy, C. (2024). The impact of digital technology deployment on mitigating supply chain disruptions: Evidence from Chinese automotive manufacturers during the COVID-19 crisis. *Journal of Purchasing and Supply Management, 30*(3), Article 100936. https://doi.org/10.1016/j.pursup.2024.100936

Wyrembek, M. (2023). The application of adaboost. M1 based on ant colony optimization to classify the risk of delay in the pharmaceutical supply chain. *LogForum*. https://doi.org/10.17270/J.LOG.2023.837

Yan, B., Wang, X., & Shi, P. (2017). Risk assessment and control of agricultural supply chains under Internet of Things. *Agrekon, 56*(1), 1–12. https://doi.org/10.1080/03031853.2017.1284680

Yang, M., Lim, M. K., Qu, Y., Ni, D., & Xiao, Z. (2023). Supply chain risk management with machine learning technology: A literature review and future research directions. *Computers & Industrial Engineering, 175*, 108859. https://doi.org/10.1016/j.cie.2022.108859

Yang, Y., Peng, C., Cao, E.-Z., & Zou, W. (2024). Building resilience in supply chains: A knowledge graph-based risk management framework. *IEEE Transactions on Computational Social Systems, 11*(3), 3873–3881. https://doi.org/10.1109/TCSS.2023.3334768

Žigienė, G., Rybakovas, E., Vaitkienė, R., & Gaidelys, V. (2022). Setting the grounds for the transition from business analytics to artificial intelligence in solving supply chain risk. *Sustainability, 14*(19), Article 11827. https://doi.org/10.3390/su141911827

Zsidisin, G. A. (2003). Managerial perceptions of supply risk. *Journal of Supply Chain Management, 39*(4), 14–26. https://doi.org/10.1111/j.1745-493X.2003.tb00146.x

Zsidisin, G. A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: An exploratory study. *Supply Chain Management, An International Journal, 5*(4), 187–198. https://doi.org/10.1108/13598540010347307