Risk Assessment of Technology Trends in Supply Chain Management

Carina Keller
University of Bayreuth, Bayreuth, Germany

Mathias Köhler*
University of Bayreuth, Bayreuth, Germany

Since supply chain risk management (SCRM) is still at an early stage of development, managers try to improve operational efficiency but rarely consider the corresponding risks. The already existing risk management tools and methodologies neglect fundamental questions in risk assessment. Owing to this fact, companies often question a mechanism to consider the contribution degree of resources in their business goal, about the likelihood of calculating a threat, or how to model the dependency severity between resources. As a result, there is a need for a structural approach that is suitable for a technology-oriented supply chain management and simultaneously ready-to-use for practitioners. Based on the method of Design Science Research (DSR) a conceptual framework for companies is developed to assist them by introducing a risk assessment suitable for new technologies in a supply-chain context.

* Corresponding Author. Email address: mathias.koehler@uni-bayreuth.de

I. INTRODUCTION: TECHNOLOGY TRENDS AND SCRM

IT is a key enabler to collaboration across the supply chain. It facilitates communication and process automation in real-time and with accurate data so that companies can handle higher volumes faster and with lower error rates in their supply chain. Technologies, like IoT, additive manufacturing, industrial robots, big data, artificial intelligence, and simulation modeling are driving new chances in supply chains (Alieyan et al., 2020; Evtodieva et al., 2020; Hassan et al., 2018; Hugos, 2018).

Besides all these advantages, companies need to take a further look at associated risks when implementing new technologies. Risk assessment tends to be among the younger scientific fields but provides an important contribution to support decision-makers (Aven, 2016). Risk assessment can be described as synonymous with the assessment of uncertainties (Raiffa, 1982). Uncertainties in common usage describe a state unconscious whether a statement is true or false (Holton, 2004). Moreover, risk assessments are both time-consuming and costly, therefore it is not practicable to carry them out from scratch each time when a system is updated and/or modified. This motivates decision-makers to employ a specific methodology addressing the maintenance of risk assessment (Stølen et al., 2003). Risk assessment processes in companies cause many challenges, i.e., the growing number of non-critical resources rise, not accurately calculated effects of threats, close output of different risks that make detection of significant risks hard, and an imprecise evaluation of risk. These challenges lead to a lack of proper risk management (Shameli-Sendi et al., 2016).

Risk management describes coordinated activities for directing and controlling an organization regarding risks. Risk management extends the risk assessment by involving the impact of uncertainty on objectives which represents the definition of the ISO guideline 31000:2018. The risk management process should be an integral part of management and decision-making and it should be integrated into the structure, procedures, and processes of the organization (Deutsches Institut für Normung e. V. & International Organization for Standardization, 2018; Ritchie & Brindley, 2009).

Supply chain risk management (SCRM) is a multi-disciplinary area including enterprise risk management, supply chain management, business continuity, and crisis management (Fahimnia et al., 2015; Khojasteh-Ghamari & Irohara, 2018). SCRM is a pro-active approach to manage risks and performance in the supply chain in advance to minimize potential undesirable consequences or avoid them. SCRM aims to secure the continuation of supply chains as planned with smooth and uninterrupted flows of materials from the initial supplier through to the final customer. Proper SCRM dependents on good quality management, like knowledge, abilities, experiences, and skills. The undeniable importance of individual judgments required in most risky decision situations cannot be replaced by concepts, tools, and technologies but they can support them (Dani, 2009; Ritchie & Brindley, 2009; Waters, 2007). Practitioners deal with the growing pressure of dynamic, vulnerable, and volatile supply chains because the nature of the supply chain and their complexity makes them vulnerable to internal and external risks. These risks tend to drift upwards due to the little to no attention paid to them by managers in advance. Another cause for the increased risk levels and growing vulnerability are the efforts of the supply chain manager to enhance efficiency by raising customer service levels and lowering costs (Waters, 2007). Due to the increased co-operation of companies and linkage between the supply chain members, risks from one company may increase or decrease risks for other members of the supply chain (Hallikas et al., 2004).

Thus, the new technology trends change the economic world and environmental conditions, for instance by letting businesses manage devices, analyze data, and automate workflow (Evtodieva et al., 2020). For the success of supply chains, managers need to understand how information is gathered and analyzed because IT serves as the eyes and ears of management in a supply chain by capturing and analyzing necessary information to make good decisions (Chopra & Meindl, 2007). There are four key components of IT that build the basis for function in business and understand how emergent technologies can be used in supply chains. These components are cloud computing, data transmission (Electronic Data Interchange and Extensible Mark-up Language), databases with business analytics (e.g., big data), and application systems (e.g., ERP, CRM, or SCM systems).

Besides IT's role as an enabler, the introduction of these technologies contains associated risks, not to be neglected. The more ingrained IT becomes, the greater is the risk of malfunctioning after IT suffered a major failure. Due to the necessary regular updates and modifications of IT systems, new risks through changes need to be assessed on a regular basis to provide a secure system. Consequences of improper use have the potential of harming people and properties (Chopra & Meindl, 2007; Griffor, 2017;

Stølen et al., 2003). Furthermore, communication networks and supply chain integration exacerbate information and security risks with increasing collaboration using mainly the Internet and web-based portals. Due to unauthorized access and modification in IT systems, businesses are confronted with serious effects from vulnerable systems. But not only the causative company faces major risks of information system failures but also the other members of the supply chain are at risk. A good way to address these security information problems in the corporate world is to use a risk-based approach (Bandyopadhyay et al., 2010; Shameli-Sendi et al., 2016; Trkman & McCormack, 2009).

These trends corroborate a lack of conceptional risk management research in supply chain with new technologies and leads to our research goal of providing a conceptual framework for technology-oriented supply chains. For this purpose, the following chapters describe the research method and our approach to analyze the already existing methods and frameworks. Based on these findings, we designed an initial framework and conducted a first testing with experts to develop an improved practice-oriented version of the framework. Subsequently, this paper ends with a discussion of the approach, a chapter on research contribution, and a short conclusion.

II. RESEARCH METHODOLOGY

Risk assessment of new technologies in SCM is a complex problem and requires an integrated approach that is related to IT and organizational aspects. Therefore, there is a need for comprehensive methodological support for the generation of a framework. This paper follows a structural framework generation approach, so that different methodologies could be utilized to reach the aim in the development of a conceptual framework concerning risk assessment of technology trends in a supply chain context. Mostly frameworks are developed based on existing methods and guidelines whereas these could be refined and validated or grounded by experience and expertise. All of them start with an initial literature study for identifying data to inform the framework followed by the development of the framework and finally validation, tests, and refinishing are executed (McMeekin et al., 2020). The authors choose a qualitative research method based on literature reviews which has been successfully undertaken in similar contexts to address relevant problems in practice (König & Spinler, 2016).

To overcome the boundaries of human and organizational capabilities, DSR will be applied as a research methodology to generate a framework to solve the objective of this paper (Deng & Ji, 2018; Hevner et al., 2004). There are two paradigms which describe DSR, the first goal is to find truth through developing and justifying theories that predict or explain organizational and human behavior with analysis, design, implementation, management, and the use of IS. This has evolved from the natural sciences, which traditionally studies physical, biological, social, and behavioral phenomena. The second paradigm is DSR with the goal of gaining utility through developing innovative artifacts (Hevner et al., 2004; March & Smith, 1995). Design science is the appropriate research method for our research goal because it creates and evaluates IT artifacts intended to solve identified organizational problems (Hevner et al., 2004). The roots of DSR go back to engineering and "The Sciences of the Artificial" (Simon, 1996). Fundamentally, it is a problem-solving paradigm to create innovations which are defining ideas, practices, technical capabilities, and products through the analysis, design, implementation, and management (Cross, 1993; Denning, 1997; Tsichritzis, 1997). The purpose of DSR is to enhance practice and to provide applicable solutions. It, therefore, increases the effectiveness of companies (Denyer et al., 2008; Holmström et al., 2009). Following the DSR guidelines from Hevner, March, Park, and Ram (2004), with the goal to design a viable artifact in form of a construct, model, method, or instantiation. The artifact produces a technology-based solution to a relevant business problem. Further, the design evaluation requires the demonstration of utility, quality, and efficacy via well-executed evaluation methods. Also, it contributes clearly and verifiably to the areas of the design artifact, foundations, and/or design methodologies. The application of rigorous methods for both construction and evaluation are crucial as well as appropriate the communication of the research to technology- and management-oriented audiences (Hevner et al., 2004). Fig. 1 provides an overview of the research project process, starting with the examination of the literature base to reach preliminary theoretical considerations that build the base for the requirement setting of the framework. In the design cycle, the framework is created, following the seven steps of framework development pattern from Vaishnavi and Kuechler (2007). Beginning with data extraction in this context and embodies concurrently the design cycle to reach a first version of the artifact based on different existing risk methodologies. This was followed by the processing of information and evaluation to check the literature-based findings with the existing frameworks and approaches. This corresponds in DSR to the rigor cycle.

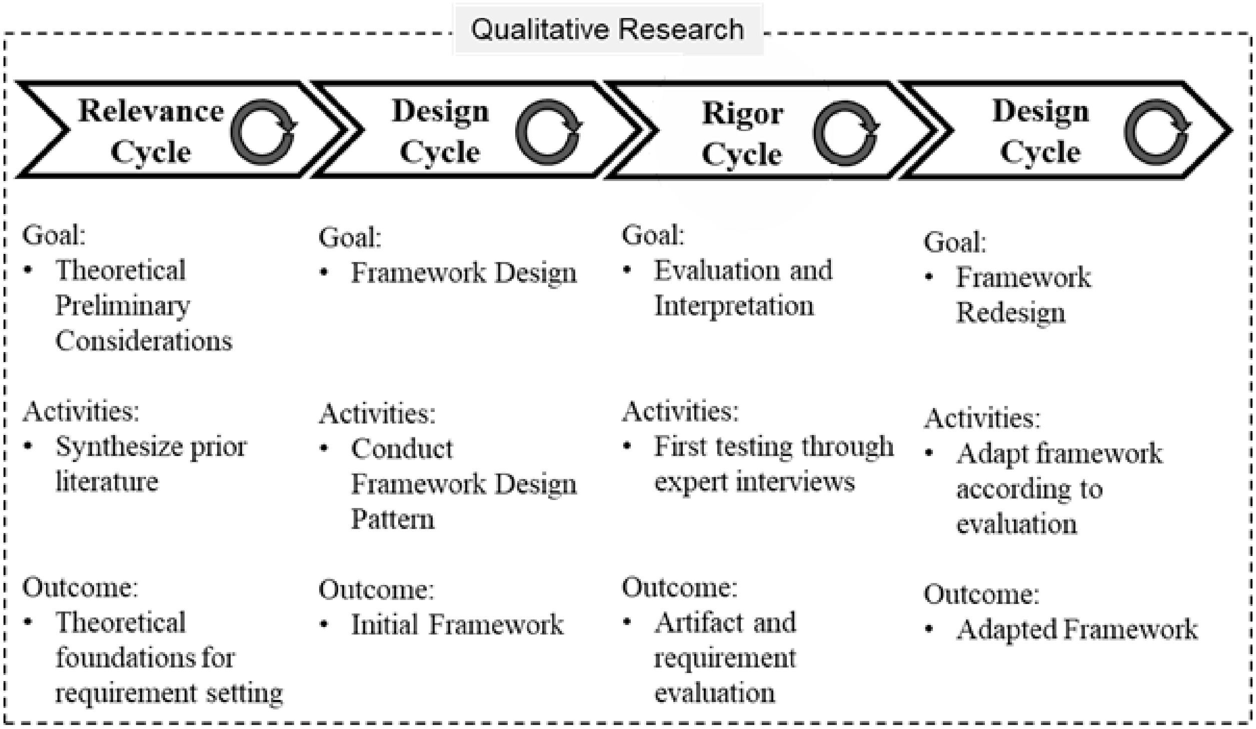
Qualitative Research
Relevance Cycle
Design Cycle
Rigor Cycle
Design Cycle
Goal:
• Theoretical Preliminary Considerations
Goal:
• Framework Design
Goal:
• Evaluation and Interpretation
Goal:
• Framework Redesign
Activities:
• Synthesize prior literature
Activities:
• Conduct Framework Design Pattern
Activities:
• First testing through expert interviews
Activities:
• Adapt framework according to evaluation
Outcome:
• Theoretical foundations for requirement setting
Outcome:
• Initial Framework
Outcome:
• Artifact and requirement evaluation
Outcome:
• Adapted Framework

FIGURE 1. QUALITATIVE RESEARCH APPROACH ACCORDING TO DESIGN SCIENCE RESEARCH

In this research project, expert interviews were executed to gain experience and expertise and to compare the results with scientific theories and methods. The results were then interpreted, and the artifact was adapted in a repeated design cycle, according to the insights from the rigor cycle. The second design cycle considers the knowledge gained through testing with the experts, which results in the development of a practice-oriented framework. Through this iterative procedure, the first design cycle was validated and supplemented with further findings, thus forming a bundle of theoretical and practical knowledge. The result is a framework for companies to assist them by introducing a risk assessment suitable for new technologies in a supply-chain context. The main goal of the work is thus to reconcile theoretical knowledge from different disciplines and link it to practical experience, while giving a clear structure with activities, techniques and targeted results per process step that are ready- to-use for practitioners.

III. FRAMEWORK DEVELOPMENT

3.1 Requirement settings and goal definition

The requirements for the framework start with compliance with laws and regulations for application and security due to good governance and low-risk technology use (Waters, 2007). The SCM requirements are efficiency, service quality, timeliness, and flexibility to ensure the supply chain objectives and should, therefore, be incorporated in an SCRM framework (Gaudenzi, 2009). Due to the use of technology, it is important to fulfill the requirements of IT security. These requirements are confidentiality, integrity, availability, non-repudiation, authenticity, and privacy (Aissa et al., 2010; Eckert, 2014).

Furthermore, some design requirements must be considered in addition to the content requirements. First, the use of a formal procedure is essential to identify and analyze threats from risks (Waters, 2007). Second, defined goals and the determination of roles and responsibilities can be considered as key drivers for a successful project and process management. Third, the monitoring of risks and performance is necessary due to the multi-actor dimensions of supply chains and their vast amount of information needed to manage associated risks to eventually mitigate negative business effects (Gaudenzi, 2009). Fourth, comprehensibility is another design factor to consider because of the different relevant stakeholders who gather information, discuss, and analyze in the risk management process. In the end, the report must be readable for everyone not involved in the analysis, regardless of their role or background in the organization (Lund et al., 2011; Otto, 2003).

3.2 Analysis of existing approaches (relevance cycle)

Following the steps from Vaishnavi and Kuechler (2007), we started by collecting a literature base to develop a classification scheme. Therefore, we selected six risk assessment methodologies with different key aspects from the field of SCRM because this is the main field to operate in according to the goal of this paper. The methodologies were chosen grounded by a systematic research approach concerning risk assessment in the field of supply chain and technology management. A broader basis of methodologies is aggregated to six risk assessment technologies which meet the core issue and enable a research contribution in the field of SCRM.

These methods are mentioned and referenced for further analysis with the respective abbreviations R-1, S-1 to S-6 and T-1 to T-4. A table with research goals and sources of all the abbreviations is provided in Table 1.

TABLE 1. EXPLANATION AND SOURCES OF METHODOLOGIES

Abbreviation	Research goal	Source
R-1	General guideline that helps to provide general knowledge about risk management	DIN ISO 310000
S-1	Risk management process for a complex supplier network in a cooperative environment	Hallikas et al. (2004)
S-2	Conceptual framework for managing disruptions in supply chains by strategic activities and joint directions	Kleindorfer & Saad (2005)
S-3	Providing a supply chain risk management tool from initial idea to final implementation and control	Waters (2007)
S-4	Integration of concepts, frameworks, and insights in several disciplines to one global supply chain risk management model	Manuj & Mentzer (2008)
S-5	Setting of guidelines to support an effective management of supply chain risks and performance	Ritchie & Brindley (2009)
S-6	Structured and ready-to-use approach for managers to assess and manage risks using the SCRM process	Tummala & Schoenherr (2011)
T-1	Using OCTAVE method for security risk evaluation focused on the risks to those assets	Alberts et al. (2001)
T-2	Set CORAS as an improved methodology and computerized support for risk assessment of security-critical systems	Lund et al. (2011); Stølen et al. (2003)
T-3	Tool for offline risk assessment of cloud service providers with the help of attack surface measurements	Madria & Sen (2015)
T-4	Determine a taxonomy of information security risk assessment to better understand the risk management by comparing concepts	Shameli-Sendi et al. (2016)

In particular, these methods are as follows: Beginning with DIN ISO 31000 (R-1), as a general risk assessment guideline, represents a common denominator for the more specific application areas of SCRM and tech-based methods. Concerning the focus of each methodology, R-1 is a general guideline that helps to provide general knowledge about risk management. Risk management processes in supplier networks (S-1) (Hallikas et al., 2004), managing disruptions in supply chains (S-2) (Kleindorfer& Saad, 2005), supply chain risk management (S-3) (Waters, 2007), global supply chain risk management (S-4) (Manuj & Mentzer, 2008), effective management of supply chain – risks and performance (S-5) (Ritchie & Brindley, 2009), assessing and managing risks using the SCRM process (S-6) (Tummala & Schoenherr, 2011). Besides, the four tech-based risk models are OCTAVE (T-1) (Alberts et al., 2001), CORAS (T-2) (Lund et al., 2011; Stølen et al., 2003), offline risk assessment of cloud service providers (T-3) (Madria & Sen, 2015), and the taxonomy of information security risk assessment (T-4) (Shameli-Sendi et al., 2016). Lastly, DIN ISO 31000 (R-1), as a general risk assessment guideline, represents a common denominator for the more specific application areas of SCRM and tech-based methods. Concerning the focus of each methodology, R-1 is a general guideline that helps to provide general knowledge about risk management. S-1 and T-3 are goal-oriented which means that they focus on the results. They first define the goals they want to achieve by implementing the respective framework and design their process accordingly. S-2 and T-1 are vulnerability-oriented means they are starting with analyzing their risks and vulnerabilities and align their process to them. S-3 and S-4 merge different concepts and frameworks but do not define a specific focus for their resulting framework. S-5 is characterized as performance-oriented because of the focus on the interaction between risk and performance. The goal of S-5 is to achieve an effective and efficient assessment of risks. Whereas S-6 focuses on the structure of its process, therefore they use defined phases and common methods within the phases to design their risk framework, e.g., Delphi method and Monte Carlo simulation (Tummala & Schoenherr, 2011).

T-2 needs further explanation because of the two different purposes. First, according to Stølen et al. (2003), it was defined as Model-based. They found evidence for better efficiency of the risk assessment process and more reliable results due to the understanding of evaluation targets by the precise specification of its structure and behavior (Stølen et al., 2003). Second, Lund et al. (2011) define the CORAS approach as asset-oriented. An asset-driven risk analysis method is suitable for many domains, e.g., security, safety, health, and so forth, due to the same basic principles. The authors changed focus and area of application over the years to an asset-driven risk analysis, which refers to the definition of protective assets as the first steps of the CORAS process (Lund et al., 2011). In T-4 the decision of the purpose is part of the process. The user of this framework decides if the focus will be asset-, service-, or business-driven based on the selection of the organization's resource level to identify the corresponding risks.

The timeframe determines if the methodology is used before, during, or after the implementation of new technology. Unfortunately, only T-3 defines that it is executed before the implementation of new technology, in particular, cloud technology. The other frameworks can be used anytime in the process of developing a risk assessment method. During the analysis process, the methods show different limitations partly mentioned by the authors in their publications, partly discovered by us after the analysis of all said methods, as shown in Table 2. Concluding, the analysis demonstrates that none of the obtainable methodologies include all predefined requirements. Therefore, it is necessary to develop a framework to assess the relevant topics.

3.3 Framework building (design cycle)

To identify best practices for the core steps of the desired framework, we analyzed the abovementioned frameworks by comparing the individual steps, phases, and contents with the requirements of the DIN ISO 31000 standard (R-1) (Deutsches Institut für Normung e. V. & International Organization for Standardization, 2018). Table 3 shows the results of this analysis sorted in the categories supply chain-based and tech-based in chronological order, "+" denotes that for this step, there is a comparable one provided in the methodology, whereas "-" means that there is no such step available. None of the methods fulfills all the steps of the standard (R-1). The step "communication and consultation" is only executed in S-3. An analysis upfront of the "context and criteria" is considered in S-3 too and in three of the four tech-based approaches (T-1, T-2, T-3). One explanation for this observation could be that tech-based approaches focus on different perspectives for reaching their objectives, which must be defined before the actual analysis. These perspectives are asset-based, model-based, mission-oriented, service-based, and/or business-driven. In contrast to the tech-based approaches, the supply chain methods place more emphasis on managing risk through treatments, monitoring, and reviews. S-3, S-5, S-6 consider the treatment and monitoring of risks.

TABLE 2. ANALYSIS OF EXISTING RISK METHODOLOGIES AND FRAMEWORKS

	SCRM oriented	Technology oriented	Practice oriented	Compliance oriented	Focus	Time-frame	Limitations
R-1	+	-	-	-	General guideline	N/A	Structure too high-level
S-1	+	-	-	+	Goal-oriented	N/A	Structure too high-level
S-2	+	-	+	-	Vulnerability-oriented	N/A	Lack of technology-risk consideration
S-3	+	-	-	-	N/A	N/A	Part of the process too complex for practice
S-4	+	-	-	+	N/A	N/A	Lack of performance measurements
S-5	+	-	-	-	Performance-oriented	N/A	Complex structure
S-6	+	-	+	-	Structure oriented	N/A	Lack of technology risk consideration
T-1	-	+	+	-	Vulnerability-oriented	N/A	Lack of SCRM focus, survey-based
T-2	+	+	+	-	2003: model-oriented 2011: asset oriented	N/A	Lack of SCRM focus, based on Common Criteria (CC)
T-3	-	+	+	-	Goal-oriented	Before implementation	Lack of consideration of SaaS, PaaS, IaaS, and customer wrote software
T-4	-	+	+	-	Asset, service, business-oriented	N/A	Imprecise evaluation, lack of context consideration

Index: Yes (+), No (-), Not available (N/A)

TABLE 3. EVALUATION OF STEPS ACCORDING TO DIN ISO 31000

R-1	Communication and Consultation	Establishing context and criteria	Risk identification	Risk analysis	Risk evaluation	Risk treatment	Recording and reporting	Monitoring and review
S-1	-	-	+	+	+	-	-	+
S-2	-	-	+	+	+	-	-	-
S-3	+	+	+	+	+	+	-	+
S-4	-	-	+	+	+	-	-	-
S-5	-	-	+	+	+	+	-	+
S-6	-	-	+	+	+	+	-	+
T-1	-	+	+	+	+	+	-	-
T-2	-	+	+	+	+	+	-	-
T-3	-	+	+	-	-	-	-	-
T-4	-	-	-	+	+	+	-	-

Index: Yes (+), No (-)

TABLE 4. CLASSIFICATION OF CONTENTS ACCORDING TO THE CORE STEPS

Core Steps	Supply chain activities	Tech activities
Context and Criteria	• Get commitment and resources from senior management • Identify key people, risk policies, aims, lessons learned from previous projects • Prepare a schedule for risk management activities	• Establish strategic, organizational, risk context/evaluation, involve top management • Identification and valuation of assets, prepare people involved • Identification of security policies, define criteria and documentation of results • Scenario selection to find readiness of assessment (*CFD, DFD*)
Risk identification	• Specify risk sources and vulnerabilities: • Define supply chain process with related operations • Collect Opinion: interviews, Delphi method, group meetings • Analyze Operations: process charts, threat diagrams, SCEM, FTA, supply chain mapping, FMEA • Analyze past events: *5-Whys, cause-effect-diagrams, Pareto analysis, checklists*	• Specify risk sources and vulnerabilities: brainstorming with a diverse target team • Analyze threat scenarios • Evaluate technology weaknesses: software, checklists, scripts • Analyze Operations: *Threat Diagrams, HazOp analysis, FMECA, FTA, STRIDE, SIEM*
Risk analysis	• Determine probability and impact and time factor (time window, frequency): *Probability and impact assessment scale, Delphi method, expert focus group, parameter estimation, five-point estimation, Monte Carlo simulation*	• Estimate level of risk with likelihood and consequences • Define critical assets: *OCTAVE event tree* • Analyze system state: *Markov analysis, Bayesian network* • Likelihood estimation: *FMCEA, ETA, CCA, Attack trees* • Identifying attacks before exploitation: *CAPEC*
Risk evaluation	• Rank and prioritize risks according to ALARP principle: *HTP analysis*	• Form risk diagram by comparing risks against criteria and setting priorities with the involvement of decision-makers • Prioritization according to the relative probability of occurrence and legal, financial, regulatory, or reputational effects • Rank threats: *DREAD*
Risk treatment	• Categories to deal with risk: clarify or resolve risk with further information; assess options to manage risk sources, drivers, and occurrence; mitigate consequences or undertake insurance • Risk management strategies: *transfer/sharing, taking, elimination, reduction, further analysis, avoidance, postponement, speculation, hedging, control, security, mitigate*	• Develop protection strategy and/or security policies • Define revised security requirements and build a security architecture • Continuously control measures • Risk management strategies: *avoid, retain, mitigate*
Monitoring and review	• Audit process: regularly report, audit, and legal reviews of implementation plans and results: *Data Management System* • Define preventive measures and guidelines for further improvement	• Review, refine and approve strategies and plans with senior management: documentation of each step of the process

After identifying the core steps the contents of each step will be further analyzed selected by supply chain activities which represent S-1, S-2, S-3, S-4, S-5, S-6, and tech activities representing T-1-, T-2, T-3, T-4. The distinctions between the steps are often fluid as in some methods risk identification, analysis, and evaluation are also referred to as assessment and evaluation (Manuj & Mentzer, 2008) or as measurement, assessment, and evaluation which is divided into ranking and acceptance as well as risk mitigation and contingency plans (Tummala & Schoenherr, 2011). Table 4 shows the result of the analysis. The left column represents the formerly identified core steps. The first row categorizes the different methodologies to their background of the supply chain or Tech. The italic text describes techniques whereas the not-italic text drafts the activities for each step.

In the first core step *context and criteria,* both the supply chain activities, as well as the tech activities, highlight an analysis of the organization's environment and its actual situation. Companies need to define responsibilities and goals. They also identify the organization's readiness and lessons learned.

The recommended techniques are as follows. Starting with a SWOT analysis to structure the surroundings and do a benchmark with firms from their branch (Alberts & Dorofee, 2001; Stølen et al., 2003; Waters, 2007). Next, goals will be defined and finally, the organization can assess their readiness in scenario selection with context flow diagrams (CFD) and data flow diagrams (DFD) (Madria & Sen, 2015). The result will be specified objectives and requirements for their risk policy as well as key drivers and people involved in the execution of the risk assessment process. After that, the *risk identification* follows. The Supply chain side needs an overview of the whole supply chain process and related operations. Both approaches then identify risk sources and vulnerabilities by collecting opinions of a diverse target team through brainstorming, interviews, the Delphi method, or group meetings. An analysis of operations follows then, including threat scenarios through process charts, threat diagrams, supply chain event management (SCEM), security incident and event management (SIEM), fault tree analysis (FTA), supply chain mapping, failure mode and effect analysis (FMEA)/failure mode and effect criticality analysis (FMECA), STRIDE (Spoofing identity, tampering with data, repudiation, information disclosure, denial of service and elevation of privilege), and HazOp analysis (Hazard and Operability) (Bhatt et al., 2014; Bouti & Ait-Kadi, 1994; Crawley & Tyler, 2015; Eckert, 2014; Kleindorfer & Saad, 2005; Tummala & Schoenherr, 2011; Waters, 2007). Furthermore, the analysis of past events and the evaluation of technology weaknesses can be used to define threat scenarios. For this purpose, the techniques of 5-Whys, cause-effect-diagrams, pareto analysis, checklists, scripts, and software can be utilized. The result is an overview of vulnerabilities and key components of the supply chain and the technical background of the organization. The vulnerabilities and threats can be collected and summarized in a risk register or database (Waters, 2007). The core step *risk analysis* estimates the level of risk by determining probability, consequences and time factor of certain events and vulnerabilities. OCTAVE event trees support the determination of critical assets (Lund et al., 2011). In addition, with CAPEC which provides attack detection, these techniques are useful for technologies (Barnum, 2008). The system state can be analyzed with Markov analysis or Bayesian network. Likelihood estimations will be supported by probability models such as FMCEA, ETA, CCA, Attack trees, Monte Carlo simulation, five-point estimation, parameter estimation (Ericson, 2005; Kleindorfer & Saad, 2005). More qualitative methods are the probability and impact assessment scale, Delphi method, and expert focus groups. The result will rank the risks according to their impact, likelihood, and timing. This enables a prioritization of risks. (Waters, 2007).

The core step *risk evaluation* contains the activities of ranking and prioritizing risks by comparing their criteria of the relative probability of occurrence and consequences with the involvement of decision-makers. These activities need to follow legal, financial, regulatory, or reputational requirements. The supply chain approaches recommend the As Low As Reasonably Practicable (ALARP) principle and the use of Hazard Totem Pole (HTP) analysis (Grose, 1987; Hurst et al., 2019). Whereas in IT security settings the DREAD (damage, reproducibility, exploitability, affected, discoverability) method is applied for the ranking of threats (Eckert, 2014). The result of this step is a classification of risks that can be cumulated in a risk diagram. The core step *risk treatment* provides design options for each risk. Therefore, it is necessary to identify risk treatment options, evaluate them and prepare treatment plans. General categories are to clarify or resolve specific risks with further information or assess options to manage risk sources, drivers, and occurrences. The knowledge supports organizations by deciding whether they mitigate consequences or undertake insurance. It also may help to develop a protection strategy and/or security policy as a guideline for such decisions. It is useful to take continuous control measures for evaluating if the taken decisions are suitable to prevent negative effects. There exist many different risk management strategies that build the basis for treatment plans, like transferring/sharing, reduction, further analysis, avoidance, postponement, speculation, hedging, control, retain, security, and mitigate. This core step results in treatment diagrams including unwanted incidents and assets (Hallikas et al., 2004; Manuj & Mentzer, 2008; Miller, 1992; Shameli-Sendi et al., 2016).

M*onitoring and review* verify and refine the former taken measures and processes. If it is suitable approved by decision-makers. Regular reports, audits, and legal reviews of implementation plans, and results are necessary (Kleindorfer & Saad, 2005). Since there is a fast change in environment and hence in risk perception. This helps to take up-to-date preventive measures and establish guidelines for further improvements and individual adaptations (Tummala & Schoenherr, 2011). Techniques to support the step are on the one side the documentation of each step in the process to secure reproducibility and transparency. On the other side, it helps to use a Data Management System because of the high amount of data. The result of this step is on-going feedback to management and supply chain participants on performance and compliance as well as the accordance to agreed standards within the supply chain (International Organization for Standardization & International Electrotechnical Commission, 2005; National Institute of Standards and Technology [NIST], 2012).

3.4 Framework evaluation (rigor cycle)

As for the validity check of the first version of the framework, four experts from the fields of supply chain management, data management, and risk management were interviewed via semi-structured interviews. All the experts have a work experience of more than three years and are selected by different criteria so that all the core fields of research are considered. First, the supply chain manager represents the purchasing and production view in accordance with the ongoing business success. Second, the audit manager establishes the risk perspective while making use of the expertise in compliance and regulations. Third, the Data Scientist reflects with its technological background the evaluation of developed framework. Last, the asset consultant represents the expert for checking the feasibility and readiness for use in practice. All the questions are listed in the Appendix 1 and the concrete statements and opinions of the experts are incorporated the following part. Their feedback was checked with current literature and lead to the framework in Figure 2. The new insights from this rigor cycle are printed in bold letters and complement the initial framework.

First, the defined requirements were checked. As result, compliance with laws and regulations will be added to the first step due to its relevance for reporting. According to the supply chain requirements, the question arises of how efficient and expensive the implementation of such a risk framework is. To keep costs for a risk framework manageable, the underlying technology must offer enormous savings potentials or service improvements. Therefore, the framework must be well adapted to the needs of the respective company to efficiently implement relevant prevention measures. This objective is already considered in the first and second step via goals and requirement setting, as well as risk identification but it needs attention during risk treatment, too. Risk matrices can be helpful to facilitate risk treatments. The IT-security requirements need to be considered during the implementation of new technology. If necessary external experts support the compliance with the requirements according to the maturity level of the company and the complexity of the technology. The interviewed experts reported that many companies overestimate the complexity of simple technologies and therefore often do not dare to use them. Nevertheless, decision-makers need to understand the underlying risks, because systems can always contain possible errors that can be minimized but not eliminated.

Furthermore, the design requirements seem to be fulfilled by the developed risk framework. They are either mentioning by name or implicitly through the analysis of the internal/external environment and by following the internationally accepted DIN ISO 31000:2018 (Deutsches Institut für Normung e. V.& International Organization for Standardization, 2018).

3.5 Framework adaption (design cycle)

Core Step 1: Data collection should be replenished in this step, as noted in all three interviews. Expert interviews can be conducted to collect qualitative data. It is advisable to interview different employees or external experts to better assess the situation of the company and the potential of the technology that is planned to be introduced. Since quantitative data is needed, especially for later evaluation of the results, companies should use their already existing internal data, and if necessary, supplement them with external data from databases. This might support them to acquire a better overview of influencing factors. Yet, companies are often not able to use their internally collected data, because the data quality and the data application is still a challenge. Common issues of data quality are lack of data availability, incorrect data, poor data definition, data privacy/security, data inconsistency across sources, data redundancy, unused data, and organizational confusion about data (Redman, 2008). The improvement of data quality contributes to the consideration and incorporation of IT security requirements. Since especially the introduction of new technologies should not conflict with regulatory requirements. This must be considered at the beginning of the process. For clarification of compliance with laws and regulations companies can consult external experts, like IT auditors who assess IT controls and processes. They are experts in IT-related laws and regulations. If available, an internal risk or compliance department can also be useful (Moeller, 2010).

According to the findings, collection and preparing data as well as to clarifying compliance with laws and regulations will be added. Besides, the techniques expert interviews and external databases will be added. This results in enclosing objectives and requirements to form risk policy following laws and regulations and usable data.

Core Step 2: The analysis of past events improves preparation for similar cases in the future, e.g., with an SCEM system. Literature also supports that there are three essential steps to consider for preventing a supply chain crisis: first, identify previous incidents with similar circumstances, second determine key characteristics of each incident, third and finally execute a statistical analysis through histograms and correlation calculations of the before found key characteristics (Hittle & Moustafa Leonard, 2011).

For risk assessments, the interview-based analysis will be used, as well as document reviews with system-relevant descriptions. Data-based methods are also used to record processes, for example with the help of process mining. Process mining is a discipline that uses on the one hand machine learning as well as data mining and on the other hand process modeling and analysis. The purpose of process mining is to discover, monitor, and improve real processes by extracting knowledge from event logs available through companies' systems (van der Aalst, 2016). As a solution for the interface problem of different little departments and people involved a business continuity approach is recommended. It exploits risk charts and for refinement risk nodes. This approach is intended to make risk aggregations and interdependencies visible and thus traceable and controllable; risk causalities become transparent and improve the understanding of risk among managers and specialists at all levels of the company. Also, top-down as well as bottom-up analysis of the risk landscape is made possible (Scholz & Mörl, 2003). According to these findings, the analysis of the actual situation of the company top-down and bottom-up to the activities of this step, as well as experience reports, risk charts, risk nodes, literature research, and document reviews to the techniques of this step will be added.

Core Step 3: For this core step, there were few comments, so we assume that the current implementation in the initial framework reflects the activities and techniques well.

Core Step 4: The risk matrix is based on the identified and analyzed risk from the previous core steps. It serves as an overview, and therefore, must be constantly maintained and updated. A risk matrix consists of the two elements risk classes and risk probability classes. The creation of these two classes is of importance for risk management, as they form the basis for what risk treatments will be introduced, to avoid the occurrence of risks, or to control negative effects at early stages. General risk classes describe the severity of a risk, i.e., the effects that the occurrence of risk can have without further dealing with the risk. Specific risk classes on the other hand additionally describe the risk. The probability classes provide information about the expenditure that is necessary for the analysis and evaluation of the risks contained. The application of a risk matrix is also recommended for technology use and can incorporate different stakeholders that are relevant for supply chain networks (Khojasteh-Ghamari & Irohara, 2018; Versteegen, 2003). Therefore, it will be added to the framework.

Core Step 5: Risk strategies are very context-dependent and must be weighed up due to the potential damage for companies. In most cases, not one exclusive strategy is followed but a mix of different gradations between prevention and reaction. The challenge is to balance proactive and reactive approaches (Pavlak, 2004; Tummala & Schoenherr, 2011). Due to the negligence of prevention in this step, develop preventive measures and guidelines will be added to clarify relevance in this step.

Core Step 6: Despite the postponement of the preventive measures to the step before, they are also relevant here because of the need to revise and update them regularly. Another important point is the communication with/to employees because they can better react to complex situations and can combine data and information with experiences and knowledge (Piorkowski et al., 2013). Due to the refinement of strategies and plans and the focus on effectiveness in SCM, the measurement of performance will be added to check if the objectives from the first core step will be achieved. This may help to analyze the process and if required activities can be adapted to the needs of the company to improve their performance. Besides, a share point is added to the techniques of this step to enable the exchange of information.

The concrete contribution to the scientific research is the classification of the risk management processes in activities, techniques, and result for each process step. In a well-present way, the main issues can be understood so that suitable technologies will help to gain the results. The combination of risk management and technology in a supply chain context is therefore a completely new structural approach and ready-to-use for practitioners. Figure 2 shows the revised framework with the adaptions in bold type.

	Context and Criteria	Risk Identification	Risk Analysis	Risk Evaluation	Risk Treatment	Monitoring and Review
Activities	• Analyze organizations' environment • Define responsibilities and goals • Identify readiness and lessons learned • **Collect and prepare data** • **Clarify compliance with laws and regulations**	• Identify risk sources and vulnerabilities by collecting opinions (1), analyze operations (2) and past events (3) • **Analyze actual situation top-down and bottom-up**	• Determine the probability of each risk • Assess consequences/impact of each risk • Analyze their time window (point in time and frequency)	• Rank and prioritize risks according to the ALARP principle • Form a risk diagram	• Develop protection strategy and/or security policy • Control measures and deal with risk • **Develop preventive measures and guidelines**	• Review, refine and approves strategies and plans with decision makers • Define preventive measures and guidelines • **Measure performance**
Techniques	• SWOT analysis • Benchmarking, • CFD, DFD • **Expert interviews** • **External databases**	• (1) Interviews, Delphi method, group meetings, brainstorming, **experience reports** • (2) Process charts, **process mining,** threat diagrams, HazOp analysis, FMEA/FMECA, FTA/ETA/Attack Trees/Fault Trees, Root-cause analysis, **risk charts and nodes** SCEM/SIEM, STRIDE • (3) 5-Whys, Cause-effect-diagrams, pareto analysis, checklists, scripts, software • **Literature research, document reviews**	• OCTAVE event trees, ETA, Attack trees, CCA, FMECA, • Bayesian network, Markov analysis, parameter estimation, Monte Carlo simulation • Probability and impact assessment scale, Delphi method, expert focus group • CAPEC	• **Risk matrix** • HTP analysis • DREAD	• Risk management strategies*:* transferring/sharing, reduction, further analysis, avoidance, postponement, speculation, hedging, control, retain, security, mitigate	• Documentation of each step • Reports, legal reviews, audits • Data Management System • **Share point**
Results	➢ Objectives and requirements to form risk policy **following laws and regulations** ➢ People involved ➢ Key drivers ➢ **Usable data**	➢ Overview of vulnerabilities and key components ➢ Risk register/DB	➢ Ranking of risks according to their impact, likelihood and timing, prioritization	➢ Risk diagrams and classification of risks	➢ Treatment diagrams with unwanted incidents and assets	➢ On-going feedback to decision-makers and supply chain participants on performance and compliance with agreed standards

FIGURE 2. ADAPTED FRAMEWORK OF RISK ASSESSMENT OF TECHNOLOGY TRENDS IN SCM

IV. DISCUSSION

4.1 Status quo and conceptualization of the risk framework

Until now, companies often evaluate with a quantitative analysis if the implementation of a new technological solution is economically viable but neglect the associated risks. The risk assessment and analysis are a challenge for companies, especially the concrete implementation of activities, according to the experts. This may also be due to the subjective probabilities used for risk analysis. The problem is that a subjective probability can always be assigned but the knowledge background can be uncertain. Whereas an assigned probability is considered with stronger knowledge than it can be justified.

Assigned probabilities can be based on a weak knowledge background which results in a difficult or even impossible assignment of a subjective probability with a high degree of certainty. The question can be raised if the subjective probability is appropriate (Aven, 2016).

A similar problem arises in the risk evaluation because they are mainly based on subjective judgments and therefore inherently contain errors. To address this issue, more quantitative methods should be used (Tummala & Schoenherr, 2011). This also relates to the necessity of improving data quality and rising transparency of companies' processes. This lack of transparency due to manual process handling with paper means that companies themselves lose an overview of their risks, which in the worst case can lead to process disruption and loss of reputation. Due to the lack of transparency of their processes, it is often not possible to share data or even risk data with supply chain members. Another obstacle could be that companies overestimate the complexity of simple technologies that are now available and therefore do not dare to introduce them. These reasons can be indications, why the maturity level of digitization in companies is lower than described in theory. The results from literature and expert interviews resemble, but companies in practice do not seem to use state of the art methods and technologies. Possible causes of this development can be uncertainties regarding technologies and their rapid development. Furthermore, the introduction of technology is also associated with high expenditures, as systems sometimes must be converted, and employees must be trained. The motivation, time, and qualifications for this development are often lacking during day-to-day operations. Moreover, the question arises when a new technology is mature enough for industrial use. An indication of the maturity level of technologies is provided by the Gartner Hype Cycle (Gartner Inc., 2020) or the NASA Technology Readiness Level (Thuy Mai, 2017). Besides, decision-makers must recognize the need for technologies. Currently, they have different digital skills which makes it more difficult for them to evaluate the technologies with their potentials and risks. These factors often act as obstacles to implementation (Ternès & Schieke, 2018).

Practical Implications: In summary of the findings from the literature section show apart from the objectives of each company, that all units should have common supply chain objectives concerning end customers and users. The different perspectives of the distinct actors involved should be carefully acknowledged by managers to avoid that various companies or decision-makers assess and evaluate risks in different ways. This could negatively influence the achievement of the overall goals (Gaudenzi, 2009). Nevertheless, supply chains cannot be completely insulated from risks because it is inherent in every link within companies' supply chains (Faisal, 2009).

Hence, the development of risk management should move from only a reporting function to a strategic partner, who is involved in the decision-making process to choose new systems or external service providers. In most cases, companies are executing overall risk assessments to make a strategic assessment or through a trigger. The strategic assessment is usually carried out on behalf of the management or supervisory board, as they consider the company's viability and risk appetite in its strategic orientation. A trigger would be, for example, the sale of a division of a company. Risk management in companies has a more administrative role and ensures that risk reporting is committed to regulatory requirements.

Moreover, there is often an interface problem. Risks are overlooked due to various decentralized units who report risks that are not networked. Besides, risks are sometimes only known on a personal level and therefore, are not reported to managers. This shows the necessity of using data-based and interview-based techniques. It is recommendable to minimize the bias between reported and actual risks. Only when companies have reached their level of maturity in terms of data collection, analysis, and evaluation, they can consider sharing risk information with supply chain partners.

These points show that companies still have some different perceptions in practice of implementing risk management and introducing new technologies in supply chain management. Despite the low degree of maturity of companies concerning digitization and the concurrent pressure of digitization, it is necessary to provide them with as much support as possible. Moreover, a structured and comprehensible approach should be guaranteed to secure efficiency and traceability. Therefore, this work offers an added value for practitioners, as the framework can be used as a guideline for the implementation of a risk assessment of new technologies in supply chain management.

4.2 Research contribution

In this paper we have developed a comprehensive and integrative framework for the risk assessment of technology trends in a supply chain context. The design was created based on existing approaches from the fields of IT security, risk management, and SCM. Therefore, the initial framework is a theoretical superordinate model that works as synthesis of risk assessment. It offers contribution not only for practitioners but also for the scientific community by creating an artifact mixing different disciplines. We refined the framework iteratively with design and evaluation cycles using existing literature and expert interviews.

To express the quality of our research approach, we will summarize the efforts to achieve compliance with the guidelines of DSR proposed by Hevner, March, Park and Ram (2004). First, this research project aims to design an artifact in the form of a framework for the risk assessment of new technologies in supply chain management. The description of the artifact should allow its application and implementation in organizational practice. Second, the objective of DSR is to solve a relevant problem. By proposing the framework, the design artifact can be considered purposeful in practice because it solves an important organizational problem. Third, design evaluation needs to demonstrate the utility, quality, and efficacy of a design artifact via well-executed evaluation methods. To secure this guideline, semi-structured interviews have been executed and using information from the already existing approaches and frameworks. Fourth, research contribution is addressed in filling the identified research gap, and hence, make a valuable contribution to theory. Fifth, research rigor was applied through rigorous research methods, both in designing the artifact and in the evaluation phase. Sixth, design as a search process is addressed through the iterative development of the framework according to the design science research cycles. Seventh, the communication of research is addressed through the submission of the paper.

4.3 Research limitation

A limitation of this research project may be the verification of the reliability. Qualitative research is measured by quality criteria, like reliability and validity. Reliability is a measure of the dependability of scientific studies. The reliability of data analysis in qualitative studies can be ensured by stability and reproducibility (Goldenstein et al., 2018). Nevertheless, the stability and replicability could not be tested due to the single analysis and small research team. However, this could be the subject of future research, e.g., case study, another research team, or workshops. Validity presupposes reliability and describes the resilience of empirical results. It can be ensured with a comprehensibly documented survey as an analysis instrument. The basic idea here is to compare self-perception and external perception (Goldenstein et al., 2018). Semantic validity has been tried to the best of our knowledge and belief by describing every step during the development of the framework to secure the traceability of the results. To reach construct validity, the introduction depicts the basic concepts, and the requirements are identified through literature and therefore through theoretical preliminary considerations. The expert interviews were executed to achieve communicative validity to compare self-perception with external perception and to evaluate the results that were reached so far.

4.4 Further research

The subject of future research in this field can be a case study where the developed framework is used in a company-setting to test the actual implementation. Thus, with more qualitative and quantitative research, it is possible to further validate the framework presented in this paper. The application of the developed framework in various branches could gather further information about the feasibility and need for adjustments due to industry idiosyncrasies. Corresponding research will also enhance the understanding of the activities, and techniques that are important and are missed and/or overlooked by technology implementation projects in supply chains. Moreover, more concepts and methods from other disciplines such as risk management, supply chain management, supply chain risk management, IT security management, project management, and change management may also be explored to validate and/or refute parts of the framework. Another point is, that risk can vary between countries, the size of companies, and the organization and/or governance structures. However, the underlying framework impresses with the goal of general applicability, there may occur facts requiring a refinishing of different core steps of the framework. Especially governmental issues, legal regulations and compliance differ from one country to another so that adjustment according to these particularities are recommendable. Therefore, different perspectives can help to refine the framework.

V. CONCLUSION

In this research project, we proposed a comprehensive framework for the risk assessment of new technologies in supply chain management. We used existing methodologies, especially six supply chain risk assessment methodologies as well as four IT security risk assessment methods. The design was refined by the evaluation of expert interviews and by reviewing the predefined requirements. This was followed by the adaptation process. The results demonstrate that the predefined evaluation criteria have mostly been met and that the framework is considered valuable by the experts.

In summary, this research project responds to the multiple requests from practitioners for a detailed roadmap for risk management to support the concrete implementation of risk assessment. The developed framework provides practitioners with an overview of steps to follow with explicitly named activities and techniques to introduce a risk assessment suitable for new technologies within the supply chain. The first step is context and criteria in which the organizations' environment, including data, laws, regulations, and responsible people will be analyzed by methods like SWOT analysis and expert interviews. Then, the risk identification step follows with further analysis of risk sources and vulnerabilities throughout the company. The following methods are used for this step: collecting opinions, operation analysis, and past events. After that risk analysis determines the probabilities of risks and their impact including the time window in which the risks may occur by using mainly statistical techniques, like ETA and attack trees. This leads to risk evaluation where the risks are ranked and prioritized according to the ALARP principle to form, for instance, a risk diagram or a risk matrix. Then the risk treatment is conducted. It evaluates different risk strategies to develop a protection strategy or security policy for the company. Additionally, it prevents as well as controls measures to deal with risks. The last step is monitoring and review in which the whole process is reviewed and refined as well as the measuring of performance takes place. Techniques like documentation throughout the process help, e.g., to execute audits and reports.

Results of the discussion section revealed a need for further research to check reliability and to assess the subjectivity of probability and/or judgements of risk evaluations. In addition, companies need to work on their digitization maturity level to know their information and processes to achieve high quality data and transparency. Risk management my provide huge potential it is seen as strategic partner and not only as reporting function due to its improvement of decision-making process.

In summary, there are many different perceptions in the practice of implementing risk management and introducing new technologies in supply chain management. A structured framework may help to synthesize the different perceptions and may lead to better outcomes.

REFERENCES

Aissa, A. B., Abercrombie, R. K., Sheldon, F. T., & Mili, A. (2010). Quantifying security threats and their potential impacts: a case study. *Innovations in Systems and Software Engineering*, *6*(4), 269– 281. https://doi.org/10.1007/s11334-010-0123-2

Alberts, C. J., & Dorofee, A. J. (2001). *OCTAVE Method Implementation Guide: Version 2.0* (Networked Systems Survivability Program). Pittsburgh, Pa. Carnegie Mellon University.

Alberts, C. J., Dorofee, A. J., & Allen, J. H. (2001). *OCTAVE(sm) catalog of practices: Version 2.0* (Networked Systems Survivability Program). Pittsburgh, Pa. Carnegie Mellon University.

Alieyan, K., Almomani, A., Abdullah, R., Almutairi, B., & Alautham, M. (2020). Botnet and Internet of Things (IoT): A Definition, Taxonomy, Challenges, and Future Directions. In R. C. Joshi & B. Gupta (Eds.), *Security, privacy, and forensics issues in big data* (pp. 304–316). Information Science Reference, an imprint of IGI Global.

Aven, T. (2016). Risk Assessment and Risk Management: Review of Recent Advances on their Foundation. *European Journal of Operational Research*, *253*(1), 1–13. https://doi.org/10.1016/j.ejor.2015.12.023

Bandyopadhyay, T., Jacob, V., & Raghunathan, S. (2010). Information security in networked supply chains: impact of network vulnerability and supply chain integration on incentives to invest. *American Journal of Industrial and Business Management*, *11*(1), 7–23. https://doi.org/10.1007/s10799-010-0066-1

Barnum, S. (2008). *Common Attack Pattern Enumeration and Classification (CAPEC) Schema Description.* Department of Homeland Security. http://capec.mitre.org/documents/documentation/CAPEC_Schema_Description_v1.3.pdf

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, *12*(5), 35–41. https://doi.org/10.1109/MSP.2014.103

Bouti, A., & Ait-Kadi, D. (1994). A State of the Art Review of FMEA/FMECA. *International Journal of Reliability, Quality and Safty Engineering*, *1*(4), 515–543.

Chopra, S., & Meindl, P. (2007). *Supply chain management: Strategy, planning, and operation* (3rd ed.). Pearson/Prentice Hall.

Crawley, F., & Tyler, B. (2015). *HAZOP: Guide to Best Practice: Guidelines to Best Practice for the Process and Chemical Industries* (Third Edition). Elsevier.

Cross, N. (1993). Science and design methodology: a review. *Research in Engineering Design*, *5*(2), 63–69.

Dani, S. (2009). Predicting and Managing Supply Chain Risks. In G. A. Zsidisin & B. Ritchie (Eds.), *International series in operations research & management science: Vol. 124. Supply Chain Risk: A Handbook of Assessment, Management, and Performance* (pp. 53–66). Springer-Verlag US.

Deng, Q., & Ji, S. (2018). A Review of Design Science Research in Information Systems: Concept, Process, Outcome, and Evaluation. *Pacific Asia Journal of the Association for Information Systems*, *1*(10), Article 2, 1–36. https://doi.org/10.17705/1pais.10101

Denning, P. J. (1997). A new social contract for research. *Communications of the ACM*, *40*(2), 132– 134. https://doi.org/10.1145/253671.253755

Denyer, D., Tranfield, D., & van Aken, J. E. (2008). Developing Design Propositions through Research Synthesis. *Organization Studies*, *29*(3), 393–413. https://doi.org/10.1177/0170840607088020

Deutsches Institut für Normung e. V.; International Organization for Standardization (2018). *DIN ISO 31000:2018-10, Risikomanagement - Leitlinien (ISO_31000:2018)* (DIN ISO 31000_2018-10). Berlin. Beuth Verlag GmbH.

Eckert, C. (2014). *IT-Sicherheit: Konzepte - Verfahren - Protokolle* (9., aktualisierte Aufl.). De Gruyter Oldenbourg. http://www.degruyter.com/search?f_0=isbnissn&q_0=9783486859164&searchTitles=true https://doi.org/10.1515/9783486859164

Ericson, C. A. (2005). *Hazard Analysis Techniques for System Safety*. John Wiley & Sons, Inc. https://doi.org/10.1002/0471739421

Evtodieva, T. E., Chernova, D. V., Ivanova, N. V., & Protsenko, O. D. (2020). Business Analytics of Supply Chains in the Digital Economy. In S. I. Ashmarina, A. Mesquita, & M. Vochozka (Eds.), *Advances in intelligent systems and computing: Volume 908. Digital transformation of the economy: Challenges, trends and new opportunities* (pp. 329–336). Springer.

Evtodieva, T. E., Chernova, D. V., Ivanova, N. V., & Wirth, J. (2020). The Internet of Things: Possibilities of Application in Intelligent Supply Chain Management. In S. I. Ashmarina, A. Mesquita, & M. Vochozka (Eds.), *Advances in intelligent systems and computing: Volume 908. Digital transformation of the economy: Challenges, trends and new opportunities* (pp. 395–403). Springer.

Fahimnia, B., Tang, C. S., Davarzani, H., & Sarkis, J. (2015). Quantitative models for managing supply chain risks: A review. *European Journal of Operational Research*, *247*(1), 1–15. https://doi.org/10.1016/j.ejor.2015.04.034

Faisal, M. N. (2009). Priorization of Risks in Supply Chains. In T. Wu & J. Blackhurst (Eds.), *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers* (pp. 41–66). Springer London.

Gartner Inc. (Ed.). (2020). Gartner Hype Cycle. https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Gaudenzi, B. (2009). Assessing Risks in Projects and Processes. In G. A. Zsidisin & B. Ritchie (Eds.), *International series in operations research & management science: Vol. 124. Supply Chain Risk: A Handbook of Assessment, Management, and Performance* (pp. 67–82). Springer-Verlag US.

Goldenstein, J., Hunoldt, M., & Walgenbach, P. (2018). *Wissenschaftliche(s) Arbeiten in den Wirtschaftswissenschaften: Themenfindung - Recherche - Konzeption - Methodik - Argumentation*. Springer Fachmedien Wiesbaden; Imprint: Springer Gabler.

Griffor, E. R. (Ed.). (2017). *Syngress advanced topics in information security*. *Handbook of system safety and security: Cyber risk and risk management, cyber security, threat analysis, functional safety, software systems, and cyber physical systems*. Syngress. http://proquest.tech.safaribooksonline.de/9780128038383

Grose, V. L. (1987). *Managing Risk: Systematic Loss Prevention for Executives*. Prentice Hall.

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

Hassan, M., Liu, D., & Paul, G. (2018). Collaboration of Multiple Autonomous Industrial Robots through Optimal Base Placements. *Journal of Intelligent & Robotic Systems*, *90*(1), 113–132. https://doi.org/10.1007/s10846-017-0647-x

Hevner, March, Park, & Ram (2004). Design Science in Information Systems

Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Hittle, B., & Moustafa Leonard, K. (2011). Decision Making in Advance of a Supply Chain Crisis. *Management Decision*, *49*(7), 1182–1193. https://doi.org/10.1108/00251741111151208 Holmström, J., Ketokivi, M., & Hameri, A.-P. (2009). Bridging Practice and Theory: A Design Science Approach. *Decision Sciences*, *40*(1), 65–87. https://doi.org/10.1111/j.1540-5915.2008.00221.x

Holton, G. A. (2004). Defining Risk. *Financial Analysts Journal*, *60*(6), 19–25. https://doi.org/10.2469/faj.v60.n6.2669

Hugos, M. (2018). *Essentials of supply chain management* (Fourth edition). *Essentials series*. Wiley.

Hurst, J., McIntyre, J., Tamauchi, Y., Kinuhata, H., & Kodama, T. (2019). A summary of the 'ALARP' principle and associated thinking. *Journal of Nuclear Science and Technology*, *56*(2), 241–253. https://doi.org/10.1080/00223131.2018.1551814

International Organization for Standardization; International Electrotechnical Commission (2005). *ISO/IEC 27001*. Geneva.

Khojasteh-Ghamari, Z., & Irohara, T. (2018). Supply Chain Risk Management: Comprehensive Review. In Y. Khojasteh (Ed.), *Supply Chain Risk Management* (pp. 3–22). Springer Singapore.

Kleindorfer, P. R., & Saad, G. H. (2005). Managing Disruption Risks in Supply Chains. *Production and Operations Management*, *14*(1), 53–68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x

König, A., & Spinler, S. (2016). The effect of logistics outsourcing on the supply chain vulnerability of shippers. *The International Journal of Logistics Management*, *27*(1), 122–141. https://doi.org/10.1108/IJLM-03-2014-0043

Lund, M. S., Solhaug, B., & Stølen, K. (2011). *Model-Driven Risk Analysis: The CORAS Approach*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-12323-8

Madria, S., & Sen, A. (2015). Offline Risk Assessment of Cloud Service Providers. *IEEE Cloud Computing*, *2*(3), 50–57. https://doi.org/10.1109/MCC.2015.63

Manuj, I., & Mentzer, J. T. (2008). Global Supply Chain Risk Management. *Journal of Business Logistics*, *29*(1), 133–155. https://doi.org/10.1002/j.2158-1592.2008.tb00072.x

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems*(15), 251–266. Design and natural science research on information technology

McMeekin, N., Wu, O., Germeni, E., & Briggs, A. (2020). How methodological frameworks are being developed: Evidence from a scoping review. *BMC Medical Research methodology*, *20*(1), 173. https://doi.org/10.1186/s12874-020-01061-4

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

Moeller, R. (2010). *IT Audit, Control, and Security*. John Wiley & Sons, Inc. https://doi.org/10.1002/9781118269138

National Institute of Standards and Technology (NIST) (2012). *Information Security* (Special Publication 800-30). https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Otto, A. (2003). Supply Chain Event Management: Three Perspectives. *The International Journal of Logistics Management*, *14*(2), 1–13. https://doi.org/10.1108/09574090310806567

Pavlak, A. (2004). Project Troubleshooting: Tiger Teams for Reactive Risk Management. *Project Management Journal*, *35*(4), 5–14. https://doi.org/10.1177/875697280403500403

Piorkowski, B. A., Gao, J. X., Evans, R. D., & Martin, N. (2013). A Dynamic Knowledge Management Framework for the High Value Manufacturing Industry. *International Journal of Production Research*, *51*(7), 2176–2185. https://doi.org/10.1080/00207543.2012.709650

Raiffa, H. (1982). Science and Policy: Their Separation and Integration in Risk Analysis. *The American Statistician*, *36*(3b), 225–231. https://doi.org/10.1080/00031305.1982.10482843

Redman, T. C. (2008). *Data driven: Profiting from your most important business asset*. Harvard Business Press. http://www.loc.gov/catdir/enhancements/fy1312/2008022312-d.html

Ritchie, B., & Brindley, C. (2009). Effective Management of Supply Chains: Risks and Performance. In T. Wu & J. Blackhurst (Eds.), *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers* (pp. 9–28). Springer London.

Scholz, P., & Mörl, R. (2003). Risikomanagement entlang von Wertschöpfungsketten. *Konferenzband Zur Computas*, 1–15.

Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, *57*, 14–30. https://doi.org/10.1016/j.cose.2015.11.001

Simon, H. A. (1996). *The sciences of the artificial* (3. ed.). MIT Press.

Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S.-H.,Stamatiou, Y. C., & Aagedal, J. Ø. (2003). Model-Based Risk Assessment in a Component-Based Software Engineering Process: The CORAS Approach to Identify Security Risks. In F. Barbier (Ed.), *The Kluwer international series in engineering and computer science: Vol. 705. Business component-based software engineering* (pp. 189–207). Kluwer Academic Publishers.

Ternès, A., & Schieke, S. (2018). *Mittelstand 4.0: Wie mittelständische Unternehmen bei der Digitalisierung den Anschluss nicht verpassen. Essentials*. Springer Gabler.

Thuy Mai. (2017). *Technology Readiness Level.* https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_accordion1.html

Trkman, P., & McCormack, K. (2009). Supply chain risk in turbulent environments: A conceptual model for managing supply chain network risk. *International Journal of Production Economics*, *119*(2), 247–258. https://doi.org/10.1016/j.ijpe.2009.03.002

Tsichritzis, D. (1997). The Dynamics of Innovation. In P. J. Denning & R. M. Metcalfe (Eds.), *Beyond Calculation: The Next Fifty Years of Computing* (pp. 259–265). Springer New York. https://doi.org/10.1007/978-1-4612-0685-9_19

Tummala, R., & Schoenherr, T. (2011). Assessing and Managing Risks Using the Supply Chain Risk Management Process (SCRMP). *Supply Chain Management: An International Journal*, *16*(6), 474–483. https://doi.org/10.1108/13598541111171165

Vaishnavi, V. K., & Kuechler, W. (2007). *Design science research methods and patterns: Innovating information and communication technology*. *Information systems*. Auerbach Publications.

van der Aalst, W. (2016). *Process Mining: Data Science in Action* (Second Edition). Springer. Versteegen, G. (2003). Die Risikomatrix. In G. Versteegen (Ed.), *Xpert.press. Risikomanagement in IT-Projekten* (pp. 131–165). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-55737-8_4

Waters, C. D. J. (2007). *Supply chain risk management: Vulnerability and resilience in logistics* (1. publ). Kogan Page. http://www.loc.gov/catdir/enhancements/fy0728/2007022711-d.html

Appendix 1

Interview questionnaire:

General:

- Does risk management, in your opinion, influence the introduction of new technologies in SCM?
- How do you rate the relevance of risk management in supply chain management?

Core steps: context and criteria, risk identification, risk analysis, risk evaluation, risk treatment, monitoring and review

- Which steps do you consider relevant for the introduction of new technologies in SCM?
- What special features characterize risk management in SCM/IT Security Management?

Questions asked per core step:

- What activities do you consider useful in relation to the step context and criteria/risk identification/risk analysis/risk evaluation/risk treatment/monitoring and review?
- What techniques for implementing the activities do you consider desirable or what techniques do you use?
- What do you think should be the outcome at the end of this step?

Conclusion:

- What do you see as the biggest opportunity of a risk management framework when introducing new technologies?
- What factors support a successful introduction of a risk management process?
- What are challenges in the introduction of new technologies in supply chain management?
- What factors hinder successful implementation of a risk management process for technology trends in companies?
- Do you have any recommendations or comments on the approach or contents of the framework?