FACULTY OF SCIENCE AND TECHNOLOGY

MASTER THESIS

Study programme / specialisation:
Risk Management and Governance
(Risikostyring og Samfunnssikkerhet)

The spring semester, 2022

Open / ~~Confidential~~

Author: Caroline B. Øyaas

……
(signature author)

Course coordinator: Eirik Bjorheim Abrahamsen

Supervisor(s): Frederic Emmanuel Bouder

Thesis title: Transboundary supply chain risk management: A consolidation of transboundary and supply chain risk management

Credits (ECTS): 30

Keywords:
Supply chain risk,
Transboundary risk management,
Supply chain risk management

Pages: ……86……

+ appendix: ……

Stavanger, ……15.06.2022……
date/year

Transboundary supply chain risk management

A consolidation of transboundary and supply chain risk management

Author

Caroline B. Øyaas

Abstract

Supply chains are becoming increasingly vulnerable to disruptions and face greater exposure from the dynamics of global interconnectivity. The growing complexities of modern societies have prompted renewed focus towards supply chain risk management (SCRM) research over the last decade. However, research related to transboundary risk issues has yet to be given substantial attention in recent years. Contributing to the developments in the field of SCRM, this thesis proposes an approach for managing global supply chain risk which modifies current SCRM processes to account for the dynamic nature of transboundary risks. This work extends current literary contributions and aims to compensate for the lack of transboundary risk focus in SCRM. Introducing the taxonomy of transboundary supply chain risk management (TSCRM), the present paper conceptualises a holistic integrative framework that incorporates resilience principles to adaptively manage the transboundary risk environment of global supply chains. In line with this framework, additional templates, tables, and a TSCRM planning process are proposed to facilitate the navigation through the TSCRM process, in particular the risk identification, and risk response selection and implementation phases.

Preface

This master thesis is a conclusion of my Master of Science in Risk Management and Governance at the University of Stavanger Business School. The topic is motivated by recent global events spurring the need for broader global considerations and understanding of the dynamics and complex interactions which influence the everyday operations of inter-organisational actors. In light of current developments following the Covid-19 pandemic and the Russia-Ukraine conflict the topic of transboundary risk in supply chain risk management is considered by the author as a highly relevant and interesting area of research which, until now has received limited focus.

This process has been both challenging and rewarding. It has led to a journey of discovery into the exciting world of transboundary complexities. For his excellent guidance, inspiration, and invaluable contributions to this process, I would like to extend my gratitude to my supervisor Frederic Emmanuel Bouder. Finally, I also offer thanks to my friends and family who have provided me with both motivation and support along the way.

Faculty of Science and Technology

The University of Stavanger Norway

Stavanger, June 2022

_____

Caroline B. Øyaas

Table of Contents

List of Figures

List of Tables

List of abbreviations

GSC	Global supply chain
GSCN	Global supply chain network
SCN	Supply chain network
SCR	Supply chain risk
SCRM	Supply chain risk management
TRM	Transboundary risk management
TSC	Transboundary supply chain
TSCN	Transboundary supply chain network
TSCR	Transboundary supply chain risk
TSCRM	Transboundary supply chain risk management

1 Introduction

Over the last decade, a rapid change has occurred in the global risk climate (Aven, 2020; El Baz & Ruel, 2021; Renn, 2008). Organisations and governing bodies have to operate in a global trade context in which supply chains face significant challenges that may impact the scope of the global supply chains' (GSC) risk exposure (Manuj & Mentzer, 2008a; Pournader, Kach, & Talluri, 2020). Following the greater use of overseas suppliers and global marketing schemes, organisations today have become more dependent upon trade with international partners requiring to a greater extent the use of global supply chain networks (GSCN) (see e.g., Bandaly, Satir, Kahyaoglu, & Shanker, 2012; Manuj & Mentzer, 2008a). This globalisation trend of modern societies affects the dynamics of GSCs which have to account for variations and changes in the cultures, economies, infrastructure, and the political and competitive environments they operate in (Manuj & Mentzer, 2008a). In this global environment where people, resource and finance movements are connected, intricately, between regions, risk events are not restricted by national borders (Kasperson & Kasperson, 2001). Greater interdependence and interconnectivity exists between national economies through the globalisation of trade, value chains and supply chains (Nadin & Roberts, 2018). Followingly, the transnational mobility of people, information, products, capital and services, along with advancements in modern technology, e-trade and production techniques attributed to this modern global trade landscape contributes to an increase in GSC's vulnerability to disruptive events (Kırılmaz & Erol, 2017).

A temporarily reduced or halted transborder flow of goods and services, such as the semiconductor shortage of 2021 (see e.g., Voas, Kshetri, & DeFranco, 2001), may cause significant disruptions in social and economic functions resulting in spillover impacts beyond the originating country's own borders (UNISDR, 2017). In the last decade, global societies have witnessed numerous events with transnational consequences including terrorist attacks, natural disasters, international accidents, conflicts, and war. These events may have devastating effects particularly when the effects caused cascade through tightly coupled international systems (see Thoma, Scharte, Hiller, & Leismann, 2016). Tight coupling here refers to the close links between a systems individual components, which increases the likelihood that disruptive impacts cascade through the system (Thoma et al., 2016). The impact on global economies and organisational operations resulting from Covid-19 pandemic and the Russia-Ukraine conflict, exemplify the transboundary consequences resulting from the tight coupling in globalised trade practices, and further emphasises the need for resilient supply chains. The Russia-Ukraine conflict has, for instance, highlighted Europe's overreliance on crude oil, natural gas and other mineral exports

from Russia, along with the dependence on key agricultural commodities from Ukraine and Russia (Kilpatrick, 2022). The potential global impact on crop yields should Russia, being a major exporter of fertiliser (Dun & Bradstreet, 2022), restrict access to fertiliser or the conflict result in a fertiliser shortage, stresses the relevance of a transboundary perspective in supply chain risk management (SCRM).

These events highlight the distinctive managerial challenges and far-reaching potential effects of transnational character posed by transboundary operating activities. In light of the increased vulnerabilities of and reliance on supply chains, supply chain risk (SCR), and as such SCRM, has become a growing field of interest both within academia and for practitioners (see e.g., Bandaly et al., 2012; Jüttner, Peck, & Christopher, 2003; Sodhi, Son, & Tang, 2012; C. S. Tang, 2006; O. Tang & Musa, 2011). A key area in SCR research, and the aim of SCRM, has been the development of strategies that contribute to the supply chains' risk identification, assessment, treatment, and monitoring (Fan & Stevenson, 2017). In addition, particular attention has been given towards the financial performance implications and competitive advantages for organisations utilising SCRM strategies (see e.g., Manuj & Mentzer, 2008; Ritchie & Brindley, 2007), the development of proactive SCRM, mitigation of supply chain risks (see Colicchia & Strozzi, 2012; El Baz & Ruel, 2021; Kırılmaz & Erol, 2017), and the management of supply chain uncertainties (see e.g., Jüttner et al., 2003). Despite the increase in globalised trade and greater interdependence of GSC, few studies have examined supply chains in a global context (Manuj & Mentzer, 2008a), or from the perspective of transboundary risk management (TRM). Developments in the field of TRM within the 21st century remain scarce. Transboundary risk can be understood as "any potential negative externality that might" (p.68) be a result of the national and international movement of goods and services throughout their entire life cycle (K'nIfe, 2007). The TRM encompasses the anticipation, communication and mitigation of these transboundary externalities (K'nIfe, 2007).

Given the limited GSC and TRM focus, it may not be particularly surprising to note that TRM in relation SCRM has remained relatively unstudied; this, in spite of regions sharing supply chains, critical infrastructure, and commerce (UNISDR, 2017). The modern era's increasingly interconnected and complex supply chain characteristics, and consequences resulting from climate change and cross-border movements of capital, people, and goods, therefore, sets the stage for renewed focus on transboundary risks in global SCRM practices. Supporting the need for further developments in SCRM, Bandaly et al. (2012) argued that current supply chain practices and characteristics alter the supply chain members exposure to risks, necessitating the development of new approaches for managing these risks. Manuj and Mentzer (2008a) further

suggested that GSCs require network systems adept at handling the requirements of operating in a dynamic and complex environment. Responding to the challenges related to the changing GSC context, this thesis takes the work of Manuj and Mentzer (2008a) a step further by incorporating TRM into a GSC perspective using resilience theory to account for the complexity of a transboundary risk context within GSCNs. Resilience theory is used here to consolidate the two modes of risk management, and account for the dynamic and complex global operating environment. It contributes to the development of a versatile framework by including important areas that require consideration when accounting for the transboundary dimension, and the supply chain network's (SCN) need for flexibility and adaptability.

The objective of this thesis was to formalise a conceptual framework that enables and encourages a focus on transboundary complexities associated with inter-organisational operations using insights and developments from TRM and SCRM disciplines. The proposed management approach modifies existing SCRM frameworks placing greater emphasis on identifying, assessing, and addressing transboundary supply chain risk (TSCR). This modified approach is referred to as transboundary supply chain risk management (TSCRM). The conceptual methodology serves the objective of this thesis in three ways. Firstly, as a TSCRM framework has yet to be established, it is considered necessary to employ a conceptual research methodology in its development to allow for a holistic introduction of the idea of TSCRM and offers a context in which future research can be based. Secondly, this conceptual approach is intended to shape how individuals see, respond, design, and manage TSCRs within a global context, assisting in a new way of identifying TSCR issues and dimensions prior to further developments being made on a qualitative and quantitative level. The TSCRM framework provides a preliminary foundation for the way supply chain managers can engage with modern GSC environments through identifying, assessing, evaluating, and monitoring transboundary risk domains. Lastly, it attempts to compensate for the current lack of transboundary focus in SCRM research. This thesis thereby highlights the importance of transboundary awareness in GSCs and extends existing research in the SCRM and TRM fields.

The remainder of the paper is structured as follows. Section 2 presents a review of current relevant literature introducing theory and developments within the fields of resilience, TRM, and SCRM, along with how the thesis answers two main gaps in literature. The conceptualised framework is then presented in section 3, complete with models, templates and tables aimed at simplifying the frameworks practical application, and subsections describing each phase of the TSCRM process. Subsequently, the TSCRM framework along with its theoretical and practical implications are discussed in section 4. Finally, section 5 summarises and concludes the thesis.

2 Literature review

2.1 Lessons from resilience and resilience engineering theory

The term *resilience* has been applied to a wide range of multidisciplinary contexts over a long period of time (Hollnagel, 2014b; Hollnagel, Woods, & Leveson, 2006; Negri, Cagno, Colicchia, & Sarkis, 2021). The term was first used by Tredgold (1818) in his study on strength of timber to explain the enduring properties of some timber types over others. Decades later resilience was used within the field of ecology to describe an ecosystems ability to absorb disruptions without adversely affecting the populations or state variables relationships (i.e., the variables required to describe the behaviour of a dynamic system (Holling, 1973). Here resilience was equated with system persistence. In his work, Holling (1973) contrasted resilience with the concept of stability, defined as a systems return to a steady-state after disruptions, identifying both as central properties of ecological systems. This distinction later led to Holling's (1996) combination of resilience and engineering, along with the division of ecological resilience and engineering resilience. Following these developments, the business community of the early 21st century began applying the concept to a business context, introducing the term *strategic resilience* (Hollnagel, 2014b). Resilience was here used to describe a business model's and a strategy's ability to be dynamically reinvented along with changing circumstances, i.e., to continuously anticipate and adapt to changes and trends which may permanently impair an organisations core business (Hamel & Välikangas, 2003). The use of resilience terminology within a range of scientific disciplines has resulted in the emergence of a wide variety of resilience definitions, making the term semantically overloaded (Becker, Abrahamsson, & Tehler, 2014; Madni & Jackson, 2011). Although these definitions may be useful for their intended purpose, systems in human environments are adaptive and involves the ability of humans to anticipate and learn from disruptions not only react to them (Becker et al., 2014).

Through the development of resilience theory, the resilience concept has been divided into different sub-elements/characteristics. Westrum (2006) argued that resilience involves a minimum of two of the following elements: avoidance, recovery, and survival. According to Westrum (2006), avoidance was related to prevention through the ability to anticipate potential mishaps. Recovery is related to a system's ability to survive major disruptions, whilst survival was used to describe a system's ability to resist being incapacitated or destroyed following a disruption (Westrum, 2006). More recently, resilience has been attributed four common characteristics, including diversity, efficiency, adaptability i.e., the ability to adjust or transform responses in line with changing conditions, and cohesion i.e., processes that maintain continuity (Steen & Pollock, 2022). Prior to the introduction of these characteristics, Hollnagel (2009),

introduced four cornerstones of resilience required for a system to remain in or recover to a stable-state over time. These include anticipation, monitoring, responding, and learning. Accordingly, being resilient therefore entails adapting the system in advance and learning from previous events, utilising this knowledge in the response (Hollnagel, 2009). Without knowledge about potential future events, which makes use of experiences from past events, anticipation according to Sundström and Hollnagel (2011) becomes impossible. Hence, resilience is about more than just bouncing back from disruptive events. A resilient system is distinct from other systems due to its ability to dynamically respond to continuous change, adapt to, and learn from unanticipated situations (Thoma et al., 2016).

Around the same time as resilience was being applied by the business community, *resilience engineering* (RE) was taken into use by safety specialists as an alternative approach for handling accidents, safety issues, and risks in industrial systems (Hollnagel, 2014b; Sundström & Hollnagel, 2011). The RE approach was proposed as a way to preserve a functions efficiency (Holling, 1996) and for safety to be controlled and managed in complex socio-technical systems (Hollnagel et al., 2006). The RE theory was developed from principles of organisational reliability, from studies on how one in hazardous environments could learn, adapt and create safety, and from the research examining how organisations and individuals attempted to anticipate failure pathways (see e.g., Hollnagel et al., 2006; Reason, 1997; Shirali, Azadian, & Saki, 2016). The emergence of RE occurred partly due to the observation that failures and successes were a result of the different manifestations of a set of similar underlying processes or events (Sundström & Hollnagel, 2011). In addition, the starting point of RE theory was the notion that blaming an accident on an individual did not, for complex systems, contribute to improve, sustain, or prepare the system for present or future disruptions (Thoma et al., 2016). Within safety management, the RE paradigm focuses on the individual's capacity to achieve success by providing aid so that they can better cope with complexity (Hollnagel et al., 2006). Complexity relates to situations when physically separated elements and actors in a linked system shifts from being loose and highly autonomous, to tightly coupled and interdependent within a short period of time (Bergström, Henriqson, & Dahlström, 2014).

Defined as a systems intrinsic ability to make adjustments prior, during or after disruptions and changes in order to sustain the necessary operations both under anticipated and unanticipated conditions, RE was quickly acknowledged as a viable safety management approach (Bergström et al., 2014; Hollnagel, 2014b). Here, a clear distinction was made, establishing resilience, not as a system's feature or quality, but rather as a characteristic of a system's behaviour and performance (Hollnagel, 2014b). Accordingly, RE looks at the system functions or capabilities

needed in order to achieve control over operations, focusing on the possibilities rather than probabilities (Sundström & Hollnagel, 2011; Thoma et al., 2016). The RE definition is, followingly, operationalised as the study of four main abilities: 1) the ability of knowing what to do i.e., addressing what is actually occurring, 2) the ability to monitor and address what is critical i.e., knowing what to search for, 3) being able to know what has happened and learn from it, and 4) having the ability to address potential developments, opportunities and threats by knowing what to expect (Hollnagel, 2014b). As such, two positive features of RE are the ability to prevent failures along with the ability to return to a steady-state (Tavana, Nazari-Shirkouhi, & Farzaneh Kholghabad, 2021).

The ability to anticipate plays a central role in RE theory, making it a proactive system and not just a reactive one (Hollnagel, 2014b). As such, RE encourages the continuous adjustments in responses of organisations and individuals to changing real-world conditions (Madni & Jackson, 2011). The theory of RE argues that the performance of a system should be all inclusive and not limited to situations where something has gone wrong. It should encompass both the negative and positive outcomes (Hollnagel, 2014b). Moreover, the theory states that outcomes of both positive and negative nature result from the combination of numerous potential conditions or states (Sundström & Hollnagel, 2011). Negative outcomes refers to failures; a system's inability to adapt to surprising real world events given the presence of finite time and resources (Madni & Jackson, 2011). There are four premises on which RE is based. These build on Hollnagel's (2009) resilience cornerstones. Firstly, the non-specific nature of performance conditions require constant performance adjustments to match the current resources and demands. Secondly, a number of adverse events can be attributed to identifiable causes. Others, however, cannot and should therefore be understood as resulting from unexpected combinations of inconsistencies in performance (Sundström & Hollnagel, 2011). Thirdly, safety management cannot be reliant on failure and error calculations, nor purely based on hindsight knowledge. It must be both reactive and proactive. Lastly, safety and core business processes cannot be viewed separately as productivity is required for safety and vice versa (Sundström & Hollnagel, 2011).

Recognising the importance of resilience in operating environments with increased competition, tighter regulations, and greater consumer pressure, resilience theory was extended towards supply chain research. These studies encompassed ways for the supply chain to prepare, resist and recover from the disruptions that occur along the SCN (Negri et al., 2021). Additionally, contrasting traditional risk management, the proactive scope of RE searches for ways in which organisations can enhance their risk monitoring ability whilst also making trade-offs which are appropriate in relation to safety concerns, production capacity and economic resources (Madni

& Jackson, 2011). Within the supply chain context, RE thereby involves the evaluation of each member's capacity to quickly handle, respond to, and recover from disruptive events as disruptions in the upstream or downstream flow of a supply chain can cause irreversible failures for every member of the extended SCN (Tavana et al., 2021). Thus, having comprehensive procedures resilient enough to continue operations and return the network to a normal state are needed for effectively managing SCRs (Tavana et al., 2021). The capacity for resilience has therefore been argued to have an important role in SCRM (Negri et al., 2021).The application of resilience theory can play a crucial role in TSCRM by contributing to the developing transboundary supply chain network (TSCN) practices, such as dynamic assessments and updating of risk evaluations to enhance effective response prioritisations, that account for complex systems, human performance drivers, and risk contributions resulting from the organisation.

2.2 Transboundary risk management developments

Differences in risk views between regions and in debates, such as with the application of technology e.g., bio technological innovations, signals how the variations in regulatory processes and local risk assessments can be impacted by political tensions and cultural values (Kasperson & Kasperson, 2001). This may thereby place transboundary risks at fore front of disputes and conflict. According to Kasperson and Kasperson (2001), transboundary risks are the risks arising from human activities in one region that threaten the future or current conditions, including human health and environmental quality in other regions. Linnerooth-Bayer (2001) further suggested that transboundary risks encompass both the risks arising from man-made activities and natural hazards including the human and economic losses from extreme weather and the movement of capital across jurisdictions into vulnerable regions or areas. Löfstedet and Sjöstedt (2001) argued that transboundary issues were becoming more pervasive and global. This is due to increased global trade resulting in issues being exported across borders, such as hazardous waste shipments from Europe to Africa, and a predilection of multinational organisations to outsource operations for the purpose of reducing costs (Löfstedet & Sjöstedt, 2001). Linnerooth-Bayer (2001) further exemplified this with the import and export of genetically modified organisms (GMO) food products. These GMO trade activities entailed the transportation of risks across domestic borders through the use of airlines, cargo vessels, roads, etc., thereby placing a greater demand on the development of trade agreements. Hence, countries and organisations are faced with the management challenges from interacting transboundary risks which cannot be addressed by a single entity alone (Nadin & Roberts, 2018).

As a result of changing global conditions and the increased interconnectivity and interdependence that bind national economies in the globalised society, researchers have argued for a greater awareness towards the transboundary risks faced by modern firms and countries (see e.g., Blondin & Boin, 2020; Lidskog, Uggla, & Soneryd, 2011; Petersen, 2019; Prabhakar, Issar, Bakar, & Yokoo, 2021; Rose, 2018). However, the TRM topic has remained relatively unstudied in recent years with few studies focusing on or making reference to the concept of transboundary risk. A majority of the studies covering the transboundary topic have focused on transboundary issues in relation to food security, environmental issues, or human health (see e.g., Becton et al., 2022; Booth et al., 2020; Opitz-Stapleton et al., 2021; Prabhakar et al., 2021). A recent study by Prabhakar et al. (2021) integrated TRM into existing frameworks on health and disaster risk reduction. Examining transboundary risk in relation to the Covid-19 pandemic, Prabhakar et al. (2021) developed a framework for risk mitigation and management aimed at facilitating the national and international systems and frameworks management of transboundary risks. Viewing, the pandemic as a transboundary disaster, Prabhakar et al. (2021) further highlighted the wide-reaching consequences of unexpected global events and the limited awareness towards the development of national response plans aimed at addressing transboundary risks. In addition, the authors provided an overview of emerging transboundary risks, placing particular focus on agricultural production and food supply chains (Prabhakar et al., 2021).

Taking an environmental view, Lidskog et al., (2011) explored how complex issues related to transboundary environmental problems were rendered governable through a discussion on the Germany-Russia gas pipeline and oil pollution in the Baltic Sea. The authors elucidated how transboundary issues were renegotiated across geographical borders. Lidskog et al., (2011) argued that in order for transboundary issues to be manageable, they had to be territorially anchored. Environmental issues, regardless of it being acknowledged as a global concern and transboundary risk, required the assignment of a specific administration or organisation (Lidskog et al., 2011). In addition, the authors showed that the consequences resulting from transboundary issues had uneven or unanticipated spatial distributions (Lidskog et al., 2011). Along a similar vein, Rose (2018) examined the transboundary risk governance of environmental threats in relation to distributional considerations. The author found a positive economic impact on outcome predictions of transboundary decision processes and information dissemination in cases where public participation was accounted for.

Examining transboundary risks from a feed contamination perspective, Dee et al. (2016) applied model simulation to an analysis of the transboundary risk in swine feed ingredients with pathogen contamination. Dee et al. (2016) demonstrated the pathogens ability to survive long-

term shipment between China and the U.S., supporting the prospect that transportation of contaminated feed ingredients may serve as a transboundary risk factor. Within a similar frame of study, Becton et al., (2022) focused on the import and dissemination risks of high impact, transboundary pathogens into U.S. feed production. The authors argued for the importance of continued evaluation on the role of regulation effectiveness, and proposed that stakeholder cooperation and collaboration were imperative for addressing transboundary pathogen risks along with the development of mitigation strategies (Becton et al., 2022).

2.3 Risk and Supply Chain

Prior to reviewing current literary contributions on SCRM, I find it relevant to briefly cover the topics of risk, supply chain, and SCR to encompass the scope of this thesis. The literature presents several conceptualisations of risk depending on the field in which the term is being applied (see e.g., Amundrud & Aven, 2015; Aven, 2015b, 2020; Manuj & Mentzer, 2008a). Aven (2015b) described risks as the uncertainty related to the risks consequences and the associated severity it can have on a given activity when using something an individual values as a point of reference. However, risk in finance literature is primarily considered in terms of probabilities related to areas including bankruptcy, expected outcomes, return on investment, and defaults (Manuj & Mentzer, 2008a). In supply chain literature, risks account for the micro and macro level conditions and events which are unexpected, and adversely influence the SCN along with other supply chain phenomena, resulting in failures or irregularities on a tactical, operational, or strategic level (Ho, Zheng, Yildiz, & Talluri, 2015). These SCR's are transmitted amongst the SCN members, hereafter referred to as network members, and could be significantly impacted by network effects (G. Li, Fan, Lee, & Cheng, 2015). Risks are here incurred on multiple levels including transportation, administration, processing, human resources, finance, and suppliers (Ho et al., 2015).

The use of *supply chain* terminology poses challenges. Numerous definitions exist which focus on specific attributes or perspectives (see e.g., Ritchie & Brindley, 2007a; Sodhi et al., 2012; C. S. Tang, 2006; O. Tang & Musa, 2011). Ritchie and Brindley (2007a) describe supply chains as networks made up of organisations which are involved, through the relationships of their distribution channels and supply sources, in the various operations that result in the produced value of goods and services. However, other definitions suggest the incorporation of additional dimensions to account for both tangible and intangible aspects, such as the development of relationships and information flows (Sinha, Whitman, & Malzahn, 2004). This is done to account for supply chain complexity and dynamics. A number of participants,

including network members and other stakeholders, are involved in and influence supply chains. This in turn makes them vulnerable to impacts from the uncertain factors associated with each network members activities and other external forces, especially when operating globally (de Oliveira, Marins, Rocha, & Salomon, 2017; Manuj & Mentzer, 2008b). Hence, the growing complexity that accompanies globalisation and modernisation increase GSC challenges. The effect a singular event has on the SCN resulting in interrupted operations of other network members has been demonstrated regularly. Such events include the semiconductor shortage of 2020 (see Voas et al., 2001), with extreme weather events, as with Hurricane Katrina and Harvey, and the terrorist attack of 9/11 (Manuj & Mentzer, 2008a).

The SCNs are particularly complex when the network organisations operate internationally. Numerous areas and participants are involved in supply chains (Negri et al., 2021). Followingly, supply chain related decisions are differentiated from other risk related decisional settings within the organisation (Ritchie & Brindley, 2007a). The SCRs are more intricate than the risks associated with decision situations of a more isolated and independent character occurring at firm level (Bandaly et al., 2012). In supply chains a specific event may, to varying degrees, cascade through the network, and this non-linear effect makes SCRs challenging to quantify (Ho et al., 2015; Jüttner, 2005; Manuj & Mentzer, 2008b). Two overarching categories are often utilised in the classification of SCRs: 1) operational risks encompassing the disruptions in supply chain operations which have regular occurrences, such as demand fluctuations, and 2) disruptive risks relating to risks occurring from natural or man-made disasters leading to major supply chain disruptions, such as terrorist attacks, economic crises, and extreme weather (see e.g., El Baz & Ruel, 2021; Gouda & Saranga, 2018; Kırılmaz & Erol, 2017). Jüttner et al. (2003) proposed the inclusion of three additional categories: 1) internal organisational risks, 2) external risk from organisations operating environment, and 3) internal SCRs which are external to the organisation.

2.4 Conceptualising supply chain risk management

Risk management has emerged as a central decision support tool. It has been applied in a variety of areas including finance and manufacturing (de Oliveira et al., 2017) and considered differently by researchers. Norrman and Jansson (2004) consider risk management as decision-making related to risks, including the estimation, evaluation, and implementation of risk responses. According to the authors, the focus of the risk management process is on comprehending the risks and minimising their consequences (Norrman & Jansson, 2004). Risk management was viewed in light of two different processes by de Oliveira et al. (2017). Firstly, the authors viewed risk management as a structured process used when responding to and treating the effects of risks.

Secondly, it was considered a proactive decision-making process for mitigating the adverse consequences from future events through the use of risk identification, analysis, treatment, and monitoring (de Oliveira et al., 2017). As such, common risk management elements include the likelihood, significance, and consequences of losses from potential risks (Manuj & Mentzer, 2008b). While risk management research on firm level is extensive and encompassed by a variety of academic disciplines, Bandaly et al. (2012) highlight the importance of studying risk management within the context of supply chains where the focus is placed on the chain rather than at firm level.

Management of supply chains could be considered a multi-functional and multi-disciplinary set of activities dealing with behavioural and physical aspects along with other (in)tangible dimensions (Ritchie & Brindley, 2007a). Moreover, managing SCRs is required to avoid disruptions and system failures (de Oliveira et al., 2017). Through SCRM, organisations seek to understand and avoid the ripple effects that disruptions, from minor events or disasters, have on the SCN (Norrman & Jansson, 2004). The aim of SCRM is the identification of potential risks in order to implement appropriate risk responses and reduce the chains vulnerability (Jüttner et al., 2003). Within the field of SCRM there is a growing body of research (see e.g., Jüttner, 2005; Jüttner et al., 2003; Manuj & Mentzer, 2008a; Sodhi et al., 2012; O. Tang & Musa, 2011). However, SCRM has been approached from different perspectives with variations in methodology, scope and risk focus, therefore, a universally accepted SCRM definition has yet to be established (see e.g., Fan & Stevenson, 2017; Pournader et al., 2020; Sodhi et al., 2012). Some researchers take probabilistic approaches to SCRM, defining it as a practice in which probabilities associated with matching supply and demand are dealt with (see e.g., Jüttner et al., 2003; Sodhi et al., 2012). Other approaches limit the scope of SCRM to large impact events which occur rarely or to the predominant belief that SCRM is about the uncertainties in supply and demand (see e.g., Lavastre, Gunasekaran, & Spalanzani, 2014; Sodhi et al., 2012).

According to Ho et al. (2015), SCRM is the use of both qualitative and quantitative methodologies for risk management in an inter-organisational collaboration. These methods endeavour to identify, assess, mitigate, and monitor events or situations on a micro and macro level that are unexpected and have the potential to adversely impact the SCN (Ho et al., 2015). Studying SCRM from the perspective of practitioners, Jüttner (2005) described SCRM in terms of SCR identification and management through the coordinated activities amongst the network members for the purpose of reducing the vulnerability of the supply chain as a whole. Taking a similar perspective Elmsalmi, Hachicha, and Aljuaid (2021) presented SCRM as being concerned with collective activities and prevention, rather than exclusively being a reactive endeavour

aimed at improving the capacity organisations have to absorb disruptions. The authors described SCRM as the process of systematic risk identification and implementation of required measures in order to limit risk exposure. This included activities, such as risk assessments and analysis, the collection of information and data, application of risk mitigating measures, and controlling and evaluating the process and corresponding results regularly (Elmsalmi et al., 2021).

Various frameworks and models for managing risks in supply chains have been proposed in literature. Examining upstream SCRM, Kern, Moser, Hartmann, and Moder (2012) proposed a conceptual model linking risk identification, assessment, mitigation, and the continuous improvement process to risk performance. Using partial least squares analysis with data from manufacturing firms in Germany, the authors' findings suggested a positive relationship between the SCRM constructs of their model. Their risk assessment was supported by the prior risk identification which further contributed to improved risk mitigation (Kern et al., 2012). Focusing on risk mitigation, Kırılmaz and Erol (2017) took a proactive approach to SCRM proposing a risk mitigation procedure to account for upstream risks i.e., risks on the supplier side of the supply chain. The authors proposed two linear programming models. The first was used to obtain an initial procurement plan, and the second to revise the initial plan by qualitatively assessing the supplier risks and risk profiles (Kırılmaz & Erol, 2017). Norrman and Jansson (2004) similarly studied proactive SCRM when examining the risk management approach initiated by Ericsson following a fire at a sub-supplier which greatly affected the organisation. However, contrasting Kırılmaz and Erol (2017), Norrman and Jansson (2004) expanded the scope beyond that of risk mitigation, accounting for additional stages in the SCRM process.

Using the ISO31000 risk management guideline as a starting point for a SCRM framework, de Oliveira et al. (2017) examined the applicability of using the ISO31000 standard as a systematic procedure for SCRM and how it might be implemented in a SCRM context. Based on a systematic literary review and the Analytic Hierarchy Process of an automotive supply chain de Oliveira et al. (2017) inferred that a ISO31000 standardisation could be advantageous in SCRM provided the organisational needs and characteristics were accounted for. Fan and Stevenson (2018) developed a holistic definition of SCRM encompassing the entire SCRM process including the SCRM objectives and pathways. In their review of extant SCRM literature and assessment of theories applied to SCRM research, Fan and Stevenson (2018) classified the literature according to four SCRM stages: risk identification, assessment, treatment, and monitoring. Alternatively, Ritchie and Brindley (2007b) suggested a model consisting of a different set of components: 1) risk context and drivers, 2) factors impacting the risk management process, 3) risk management responses including the acts of mitigation, monitoring, acceptance,

and avoidance, 4) the decision makers involved, their perceptions, experiences and attitudes, and 5) the final performance outcome. The purpose of this work was to examine the interactive relationship between risk and performance, and underline the main constructs of risk management within the context of supply chains (Ritchie & Brindley, 2007b).

Using a sample of 164 French industrial firms, Lavastre et al., (2014) studied the effects of firm characteristics, relationships with suppliers, and SCRM techniques. The authors proposed a framework that introduced firm and respondent characteristics, risk perceptions, and the relationship characteristics of industrial partners, into the SCRM process. Broadening the scope of SCRM research, Manuj and Mentzer (2008b) developed a global SCRM framework and strategy selection process consisting of five steps: 1) the identification of risk based on four risk source classifications, 2) the assessment and evaluation of risk, 3) selection of appropriate strategies for managing risks, 4) implementation of the proposed strategies, and 5) risk mitigation. This framework was built on the understanding that a potential outcome at one area of the supply chain might be a risk event at another (Manuj & Mentzer, 2008b).

2.5 Identified gaps in literature

The review of literature shows two major gaps in SCRM literature which this thesis aims to answer. Firstly, few papers have taken a holistic approach to SCRM as argued by Fan and Stevenson (2017). A number of studies have proposed systematic approaches for managing SCRs (see e.g., Pournader et al., 2020; Sodhi et al., 2012; C. S. Tang, 2006; O. Tang & Musa, 2011). The majority of this research focuses on individual steps of SCRM rather than viewing all steps of the SCRM as an integrated process. The research with a focus on the integrative process tends to have a fragmented approach concentrating on two stages in the SCRM process, with the greatest attention being attributed risk identification, assessment, and mitigation, rather than the entire process from risk identification to risk control and monitoring (see e.g., Bandaly et al., 2012; Ho et al., 2015; Kern et al., 2012; Ritchie & Brindley, 2007b; Sodhi et al., 2012). Ritchie and Brindley (2007a) argued that a narrow or singular perspective makes it challenging to envisage the potential chain-wide implications resulting from the decision-making process. Furthermore, Ritchie and Brindley (2007a) stressed the need to concentrate less on individual framework components and more on how they are related. This is supported by Ho et al. (2015), who highlighted the significant relationship that exists between the SCRM processes.

Limited research has been attributed to conceptualising frameworks for global SCRM (Manuj & Mentzer, 2008a), and to the author's knowledge, a comprehensive framework for including transboundary risks in SCRM has yet to be developed. The risks in GSCs have complex

interlinking patterns making them more unpredictable, and challenging to manage (Manuj & Mentzer, 2008b). When managing SCRs in a transboundary operating environment it is important to consider the entire supply chain including network members in other regions, as risks cascade through cross border systems and networks (Boin, t'Hart, Stern, & Sundelius, 2017). Responding to the call for a more fully integrative framework and global focus, the current thesis takes a holistic integrative approach in the framework development. This is done to better account for the relationship between the stages of the SCRM process, and the continuous monitoring, adaptation and inter-organisational focus required for managing transboundary risks.

Secondly, a broader risk type focus is warranted. According to Ho et al. (2015), focus on a singular risk type dominates the research agenda, a majority of which focus on supply, demand, or manufacturing risks. Contrasting the majority of prior research, the current TSCRM introduces five broad risk domains within both the macro and micro operating environment. This is done to account for the complexity, scope, and interactive nature of transboundary risk. SCRs have multiple different drivers and sources resulting from international trade, transport and production being located worldwide (Bandaly et al., 2012). These SCRs may include man-made and natural disasters, currency fluctuations, political instability, and rapidly changing market requirements (Bandaly et al., 2012). By addressing these gaps in existing research, the conceptual work of this thesis extends the existing knowledge and adds a further dimension into SCRM research which accommodates for the intricate transboundary nature of global operations.

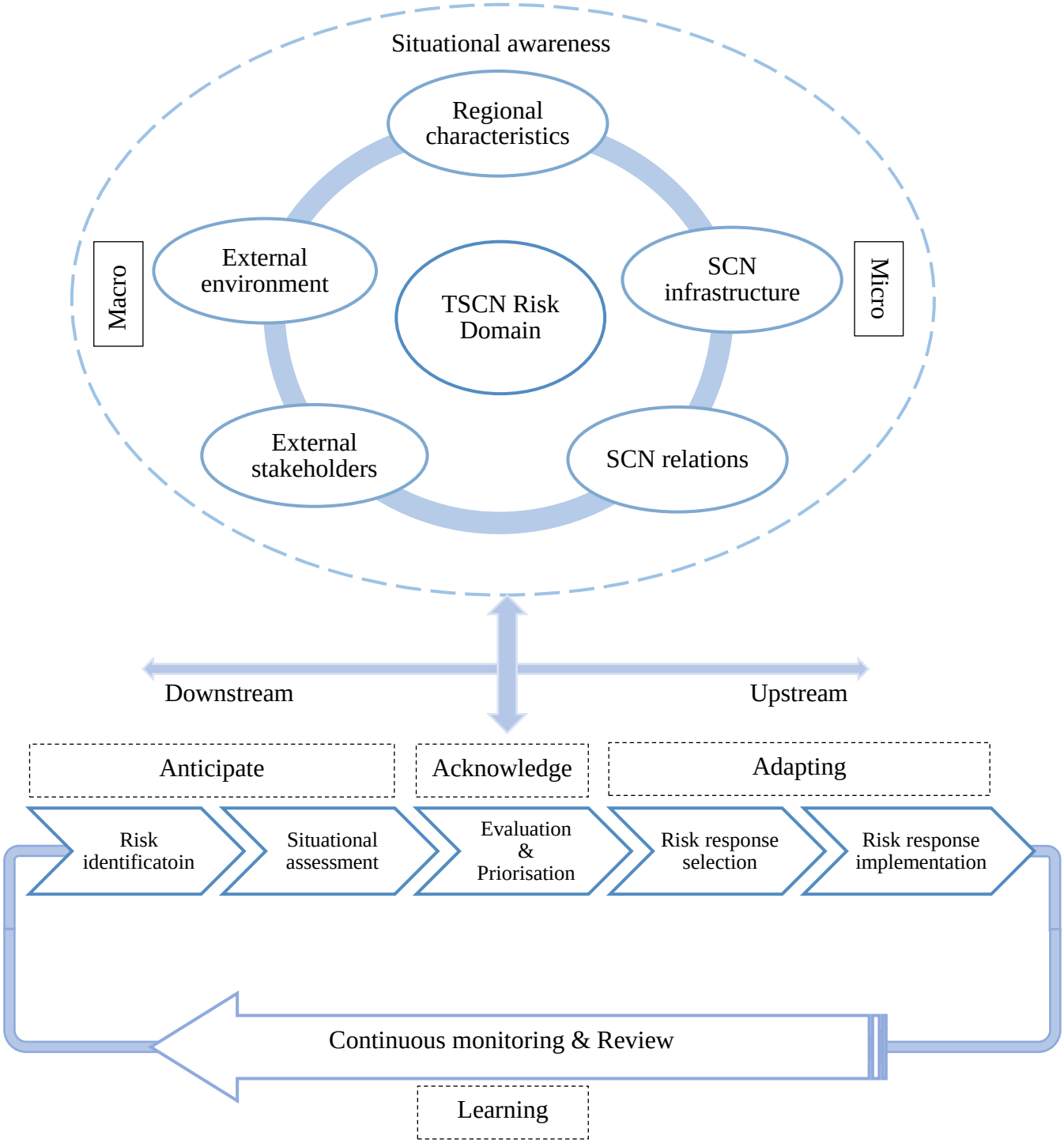
3 A transboundary supply chain risk management framework

Based on the review of current literature, an integrative framework for managing TSCRs is proposed and presented in Figure 1. Each sector/industry needs to account for different aspects which are unique to them; therefore, the generic design of the framework will provide the flexibility needed for adaptations, and function as a guide for TSCRM. The framework consists of seven interrelated phases: situational awareness, risk identification, situational assessment, evaluation and prioritisation, risk response selection and implementation, and continuous monitoring and review. A modification of Hollnagel's (2009) resilience cornerstones is used to further classify the TSCRM phases within a resilience frame. This modification is presented in Figure 2. The design aims to illustrate the dependencies between each phase of the TSCRM process and highlight the continuous nature of TSCRM. Each phase will briefly be presented before a thorough introduction and a discussion follows in the underlying subsections. Accounting for the transboundary feature of globally operating supply chains, these GSCs will, in the subsequent sections, be referred to as transboundary supply chains (TSC).

With the growing pressure from competitive environments and increasing customer demands, organisations have started restructuring their business practices to accommodate for a global operating environment (Manuj & Mentzer, 2008a), thereby requiring multi-national SCNs. The *TSCN risk domain* (see Figure 1) of the situational awareness phase aims to capture the greater complexity of the modern decision-making context, including the widening involvement and considerations towards stakeholders. Over the last decades, the major mishaps and incidents that have occurred stress the need for addressing both internal and external risk, including human and organisational dimensions (Madni & Jackson, 2011). The TSCN risk domain is separated into macro and micro to incorporate a broad risk management coverage and highlight the importance of encompassing the entirety of the SCNs surroundings to account for transboundary risks. The five TSCN risk domains presented in Figure 1 are considered to be an intrinsic aspect of long-term human-environment relationships that encompass everyday life.

Figure 1

Transboundary supply chain risk management framework



Following the situational awareness, the inclusion of *upstream* and *downstream* is here used to acknowledge the importance of accounting for all members of the SCN, both on the supply side and demand side. The recent Russia-Ukraine conflict exemplifies the importance of accounting for the extended SCN. Organisations and economies interconnectivity have facilitated

the increasing supply chain crisis currently resulting from this conflict, whilst to a certain extent also concealing it (Kilpatrick, 2022). A majority of SCRM practitioners focus exclusively on Tier 1, i.e., direct, suppliers in their risk assessments, not accounting for Tier 2, i.e., secondary suppliers in their SCN. Russia has less than 15,000 Tier 1 suppliers, however there are globally approximately 7.6 million Tier 2 supplier relationships with Russia (Dun & Bradstreet, 2022). Without a focus on the risks in the extended SCN, numerous organisations may be unaware of their reliance on, in this case, Russian suppliers. This lack of extended awareness may influence the SCN's anticipatory and adaptive capacities given the tight coupling of SCN members. Although a single network member may have all resilience attributes, they only become effective when these are inherent across the SCN (Pillay & Morel, 2020).

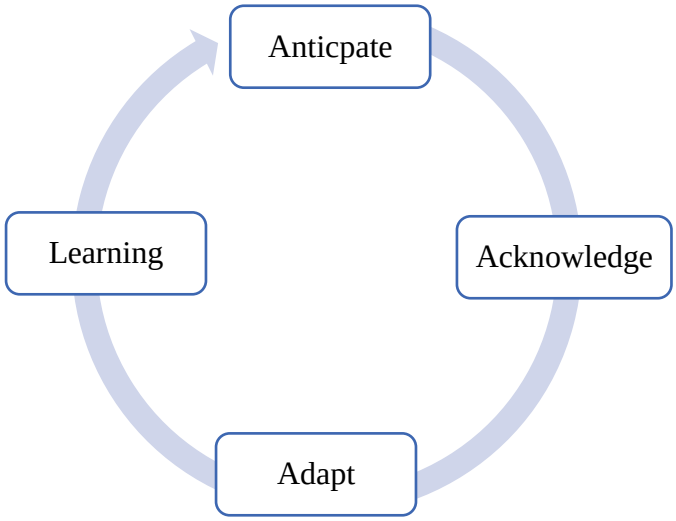
Organisations need to be able to adapt to changes and potential hazards not just after a disruption has occurred but also prior to and during a disruption (Pillay & Morel, 2020). The processes of change, including environmental degradation, globalisation, socio-economic processes and climate change, contributes to increase the dynamic nature of global societies (Becker et al., 2014). Followingly, Thoma et al. (2016) argued that a framework that enables systems to adapt dynamically to the changing conditions was needed. The use of resilience thinking provides a means for coping with the complex non-linear relations of TSCNs and maintaining control as the SCN is faced with continuous disruption (see e.g., Madni & Jackson, 2011). For a system to be in control of its entire operation, Sundström and Hollnagel (2011) argue that having Hollnagel's (2009) four cornerstones of anticipating, responding, monitoring and learning are appropriate. The TSCRM framework presented in Figure 1 therefore includes a modified version of these four resilience cornerstones: anticipate, acknowledge, adapt and learning (see Figure 2), which fit the complex, ambiguous, and unpredictable situations of global operations. The purpose of adding resilience principles to the framework is to improve the network members ability to anticipate, plan and recover from or adapt to disruptive events (see e.g., Thoma et al., 2016). Their inclusion provides agility when faced with changing conditions and flexibility when faced with unforeseen circumstances. This in turn creates conditions for minimising or preventing adverse consequences (Lay & Branlat, 2014).

Hollnagel's (2009) responding cornerstone includes the ability to adapt and recover from a given event, and mitigate, prepare, or prevent hazardous events. Given that the term responding in a broader context can be equated with a reactive response, the name is altered to *adapting* in order to capture the importance of proactive risk responses in a transboundary setting (see Figure 2). *Acknowledging* is here added to the resilience cornerstones of this thesis. Acknowledging critical risk aspects through evaluations of risks will, arguably, be important for prioritising

responsive strategies appropriate and sustainable enough to function effectively in a dynamic global context. Hollnagel's (2009) **"**monitoring" is here integrated with "learning". Experience and lessons learned facilitate knowledge building on what to monitor, and monitoring activities provide information on the impact from internal actions and the external environment, which the organisation can learn from. Through this modification, the goal is for the SCN to be able to avoid or prepare for accidents through anticipation, become more adaptive, improve the ability to recover from disruptive events, maintain operational activities by acknowledging current and future potential risks, and learn from the TSCRM process.

Figure 2

Adaptation of Hollnagel's four resilience cornerstones



Note. Adapted from Hollnagel (2009).

Manuj and Mentzer (2008a) argued that managing globally operating supply chains required organisations to follow a process from identification of risks, implementation of strategies, to monitoring and controlling the risk management process. Although the TSCRM phases are adapted to facilitate the TSC context, the process from risk identification to monitoring is accounted for in the framework development. The risk identification phase encapsulates the various risk drivers, sources of risk, and disruptive events presented in literature. Following the identification phase, the situational assessment encapsulates the current and future global risk landscape along with more traditional risk assessment approaches. The evaluation and prioritisation phase of the present framework is used to identify not just the most critical risks but also the resource capabilities of the organisation and network members to respond to these risks. The risk response selection phase provides an overview of diverse approaches for

managing risks within each of the five TSCN risk domains. In addition, it presents a taxonomy for response classifications alongside a selection process model and evaluation template to simplify the selection process. The risk response implementation phase further introduces a contingency planning taxonomy and template stressing the importance of multiple response considerations and contingency measures.

In the following subsections 3.1 to 3.5, the underlying constructs of the TSCRM framework are further elaborated on. Although the framework should be viewed as a continuous process with interdependencies between each phase, they will be discussed in a stepwise manner in the following subsections. Each phase and corresponding components are first defined and described followed by argumentation for their relevancy with use of examples where relevant. Additional models and generic templates for use in the risk management process are also provided to guide application whilst still enabling necessary industry and organisational adaptations.

3.1 Situational awareness

Before a more detailed risk identification process is conducted, a situational awareness of the TSCR domain is required to establish the internal and external parameters of the TSCRM process. Hence, it assists management in defining the TSCRM's scope and context. Situational awareness entails knowing when responsive actions require changing, recognising when environments are changing and understanding of the complexities and interdependencies which exist within a system or network (Herrera & Hovden, 2008). The situational awareness helps ascertain the concentration of risk drivers and sources at identifiable locations and acknowledges the broader reality of the risk. The focus and efforts towards managing transboundary risks differ between regions, which complicates detection and identification of disruptive risks (Kasperson & Kasperson, 2001). Manuj and Mentzer (2008b) emphasised that the physical geographical distances from globally located risk sources contributed to a more extensive and rapid impact from risk events. This perspective is supported by Blondin and Boin (2020) who maintained that TRM is complicated by the changing nature of threat agents, use of outsourcing, globalisation, and modern societies increased vulnerability to small disruptions.

Kasperson and Kasperson (2001) argued that explicit recognition of transboundary risks being neither a singular issue, nor a single-context situation is required before the management of transboundary risks can be meaningfully performed. Five TSCN risk domains are, therefore, defined and separated into the overarching macro and micro domains, each having risk drivers with attributed risk sources resulting in a disruptive event. The separation into macro and micro further enables both voluntary and involuntary transboundary risks, which may affect the SCN,

to be accounted for, thereby following the suggestion of Linnerooth-Bayer (2001). A distinguishing transboundary risk feature presented by Linnerooth-Bayer (2001) encompasses whether or not the transboundary risk is incurred voluntarily. Involuntary transboundary risks, such as the risk countries bear from nuclear power operations or energy developments of a neighbouring or nearby region, are pervasive and cannot be restrained by borders (Linnerooth-Bayer, 2001); contrasting voluntary transboundary risks, as with trade activities. The involuntary risks move across functional and geographical boundaries, have unclear ownership, and can amplify tensions between involved actors (Boin et al., 2017). Using these five TSCN risk domains 1) external stakeholders, 2) external environment, 3) regional characteristics, 4) SCN relations, and 5) SCN infrastructure, as a precursor to a more detailed risk identification may therefore contribute to greater awareness of global interactions and in the selection of risk management approaches suitable to global transboundary circumstances, networks, and risks.

3.1.1 Macro domain

The macro context refers to the external events and situations which may impact the SCN. According to Ho et al. (2015), risks in a macro domain have a greater potential for negative impact compared to those occurring in the micro domain. Understanding the macro SCN context is relevant to ensure that the concerns, impacts and objectives of externally influencing forces are taken into account in the evaluation of risks, and selection and implementation of risk responses (see e.g., de Oliveira et al., 2017). Without awareness to the macro environment it becomes challenging to establish the necessary knowledge to implement joint risk responses and acquire situational understanding of the broader risk domains (Löfstedet & Sjöstedt, 2001). Although not exhaustive, the following three domains: external stakeholders, external environment, and regional characteristics, are covered within the macro risk domain. These three domains are a result of factors existing outside the SCN and will arguably be an inevitable part of all organisations' supply chain operations that cannot be circumvented. I therefore find them to be particularly relevant.

External stakeholders

Stakeholders are "any group or individual who can affect or is affected by the achievement of the organisation's objectives" (Freeman, 1984, p. 46). In the context of this framework, the external stakeholder risk domain covers the local communities, external policy makers, the public and all other parties who are directly or indirectly impacted or affected by the operations of the SCN. An important aspect of managing transboundary risks is understanding how stakeholders perceive and construct transboundary risk issues within and across borders (Löfstedet & Sjöstedt,

2001). Stakeholders' interests and worldviews can significantly influence the way in which risk issues are perceived and framed (Cormier, Ledoux, & Magnan, 2011; Lupton, 2013). Moreover, stakeholders in different regions have different perceptions related to the legitimate practices of actors, such as multinational organisations, large corporations, and regulatory agencies (Renn & Klinke, 2001). Consequently, how different stakeholders react to the responses and management styles they are exposed to will be regionally varied, meaning that a response or action accepted in one region may meet resistance in a different region. Hence, the perception of the public, external policymakers and other stakeholders may conflict as a result of their views on areas, such as values and responsibilities (Löfstedet & Sjöstedt, 2001).

A further important consideration is the increased complexity and interaction between risk drivers and involved parties which make transboundary risk more challenging to manage than those that respect man-made borders (Boin et al., 2017). The influence from stakeholders' preferences, including their biases, heuristics, ethical considerations and engagement in local and/or global issues, have the potential to impact the SCNs operational activities (see e.g., Cormier et al., 2011; Jones, Harrison, & Felps, 2018). I therefore propose that the inclusion of an external stakeholder risk domain is relevant for TSCRM as it could contribute valuable insights into the stakeholders' reactions to organisational activities and response implementations. This assertion is congruent with aspects of stakeholder theory, which argues that improved performance may result from an organisation's socially oriented characteristics (Barnett & Salomon, 2006). Considering existing research demonstrating the importance of stakeholders for organisational performance (see, e.g., Berman et al., 1999; Mainardes, Alves, & Raposo, 2012), the inclusion of external stakeholders as a separate risk domain is, therefore, not perceived as particularly difficult to reconcile. By acknowledging the influence external stakeholders have in a transboundary environment, the TSCRM process becomes more open to adaptations and facilitates additional understanding on variations in cultural and social dynamics.

In global operations the relationship between stakeholders and the network members exist irrespective of whether they acknowledge the fact (Donaldson & Preston, 1995). Accounting for local knowledge and experience can therefore be vital when evaluating risk response actions, particularly when aiming to build trust (Vari & Linnerooth-Bayer, 2001). Thereby, having an amicable relationship with external stakeholders represents a valuable resource for the organisational members of supply chains (Mainardes et al., 2012). Controversial practices by network members may expose organisations to reputational, demand and supply risks across multiple operating segments and regions. Organisations perceived to be unjust or as having practices which are inappropriate may incur large economic penalties, loss of market shares,

lawsuits, and boycotts resulting from the mismanagement of their stakeholder relationships (Cormier et al., 2011; Jones et al., 2018). In this regard, trust in the motivations of the organisations involved is essential for obtaining public acceptance, avoiding dissension, and is fundamentally implicated in resolving potential issues (K'nIfe, 2007; Vari & Linnerooth-Bayer, 2001).

Additionally, trust can only be achieved between parties of a social relationship when the public perceives the organisation as acting competently, i.e., being consistent, within their areas of responsibility over time (Kasperson & Kasperson, 2001). Continuous violations of expectations will usually result in distrust from the external stakeholders (Vari & Linnerooth-Bayer, 2001). A lack of trust may then intensify the public's concern over the supply chains' operational activities and the perceived hazards associated with these activities, leading to hostilities and tensions (see Lupton, 2013). This lack of trust may result in the social amplification of risk, a crucial aspect of transboundary risks (Kasperson & Kasperson, 2001). Social risk amplification relates to the interaction between a risk event and the social, cultural, institutional and psychological processes which contribute to either increasing or dampening risk perceptions and shape the attitudes towards the risks (Lupton, 2013). Social amplification can trigger demands by stakeholders for additional risk responses or protective actions over that which the organisation would initially be willing to invest (Kasperson & Kasperson, 2001).

Additionally, if past conflicts, current tensions, and/or cultural differences are present between a network member and external stakeholders it may lead to protests, widespread media coverage and public concern. Public demonstrations and activism in response to a specific even or issue can, for instance, have the power to impact policy regimes (Löfstedet & Sjöstedt, 2001). This could then restrict international trade due to risk issues associated with trade activities, limit expansion endeavours of supply chains as a result of the publics perceived encroachment on a socially significant area, and/or set limits to the SCNs operating market (Löfstedet & Sjöstedt, 2001). The U.S. based Newmont mining corporation exemplifies this, being forced to close down their regional mining operations in Peru due to local protests in 2011 (Triscritti, 2013). Furthermore, if the local community ends up retaining the risks without receiving any benefits, such as with hazardous waste disposal on the African continent, it would likely generate tensions between the affected communities and the actor(s) responsible for the risk (Kasperson & Kasperson, 2001). Accounting for external stakeholders' perceptions and attitudes may therefore be advantageous to the TSCRM decision-making process when evaluating the selection and implementation of risk responses.

External environment

The external environment risk domain encompasses the wider setting in which the SCNs have to operate. This context covers market related factors including globalisation, global economies, international regulations and changing market conditions, and non-market related factors, such as natural and man-made hazards including earthquakes, viruses, bush fires, typhoons, human error, and malicious or accidental acts (Komatsubara, 2014). Man-made hazards can also be associated with border-impact risks. These risks are attributed to a region's activities, developments and industrial plants that affect local and neighbouring populations or systems, and can be a result of routine activities or accidents (Kasperson & Kasperson, 2001), an example being the Chernobyl disaster. The risks in the external environment domain are distinct in that a region's or multiple regions' activities may affect more or all other regions (Opitz-Stapleton et al., 2021). Numerous risk sources may combine within the external environment and alter the global setting through complex pathways making the exact nature of causes and interactions uncertain. This results in the risks becoming hard to discern and accommodate (Kasperson & Kasperson, 2001; Svedin, 2001). The spatial separation between the geographical location generating the risk and the region(s) affected by the risks' consequences can increase the affected parties risk exposure and exacerbate potential vulnerabilities (Kasperson & Kasperson, 2001). If parties are unaware of the potential hazards posed by risks in other areas they may be ill-prepared to face and respond to these events (Kasperson & Kasperson, 2001).

An effect of globalisation is the changes in climatic and economic environments resulting in greater SCRs (Chen, Sohal, & Prajogo, 2013). As a risk driver within the external environment risk domain, climate change introduces new risk sources and challenges for organisations including those related to the low carbon economy transition and physical asset security (Chen et al., 2013). Climate change may trigger disruptive events that propagate not only within but across borders, potentially impacting the operational activities of SCNs. Cross-border bushfires and water shortages may, for example, become more frequency due to the warmer temperatures and corresponding droughts (Opitz-Stapleton et al., 2021). This may then increase the SCRs related to lost production capacity and damage to organisational infrastructure. In addition, it may also damage or disrupt regional infrastructure, such as roads, bridges and power stations, which may further halt or delay resource extraction, production, or transportation, potentially resulting in cascading economic impacts throughout the SCN (Opitz-Stapleton et al., 2021).

In a similar manner, global treaties and regimes may restrict supply chain operations. International protocols and policies, such as the Kyoto Protocol, provide significant international influence into the structure of a nation's policies and industrial systems (Kasperson & Kasperson,

2001) by, for instance, limiting their use of fossil fuels and setting of carbon emission quotas. Global market conditions influenced by trade rules and regulations can then potentially reduce supply chains' flexibility by restricting their ability to adapt due to restrictions from, amongst other aspects, tariffs and import/export bans (Opitz-Stapleton et al., 2021). Moreover, political change and (in)stability provide further sources of risk for a TSCN. Transboundary situations, such as the Covid-19 pandemic and the Russia-Ukraine conflict, could easily enlarge and exacerbate existing risks along with new risks as with those related to natural resource availability and trade activities. Additionally, the movement of physical flows also require attention. The wide use of the canals-based supply chain routes, including the Panama and Suez Canal, has demonstrated the dependency modern supply chains have on these transport lanes, making supply chains highly reliant on the canals' efficient operation and accessibility. Consequences of a blockage along shipping route choke points was demonstrated when a cargo vessel blocked the Suez Canal in March of 2021. This blockage stopped 12% of trading vessels from utilising the shipping lane, impacting global trade and exposing vulnerabilities in modern supply chain practices (Lee & Wong, 2021). Correspondingly, accounting for the broader operating environment and how the dynamics of global conditions may increase risk exposure is deemed relevant for the TSCRM process. Such efforts could contribute to greater awareness and preparation, likely improving the effectiveness of response strategies.

Regional characteristics

The regional characteristics risk domain encompasses the less identifiable and more subtle effects, as with those related to national interests, standards, safety cultures, ideologies, history, regional policies and regulations, and local infrastructure and economic structures. The variations in the characteristics of the different regions, the SCN operates in, presents an avenue for additional SCR (see Renn & Klinke, 2001), requiring consideration when performing TSCRM. Differences in regional cultures, political structures, legal traditions, social values and interests can intensify the tensions and/or conflicts between international parties (Renn & Klinke, 2001). Transboundary insecurity, such as transnational terrorism and criminal networks, could, for instance, be exacerbated by poor local governance, resource scarcity and inequality (Opitz-Stapleton et al., 2021). This may in turn lead to adverse situations, including civil conflicts, and multi-country cooperation and political tensions (Opitz-Stapleton et al., 2021).

Cultural values and biases play an important role for how individuals construct the risk problem and perceive risk information (Kasperson & Kasperson, 2001). Additional evaluation criteria are, for example, used by people in all cultures when considering different situations. Some criteria, including the capability to control risk, are usually present in most region, whilst

others are more specific to the regions culture or political systems (Renn & Klinke, 2001). How risk is handled and perceived will, therefore, be influenced by the social processes, cultural beliefs, assumptions and behaviours which individuals conform to, and the routine practices standardised within a region (see Linnerooth-Bayer, 2001). Understanding the way in which culture and social variations can influence potential sources of risk could then be crucial to the success of TSCRM activities as it may impact the efficacy of selected risk responses (see e.g., Löfstedet & Sjöstedt, 2001). I therefore propose that it is essential for the cultural and social attributes and values considered to be relevant within a region, to be accounted for when evaluating risk responses and implementation practices. Support for this view can be found in Thompson and Gyawali (2001) who maintained that understanding the influence from cultural and social differences was essential for TRM, especially as it relates to the formulation, adaptation, and implementation of risk management techniques.

The priorities and regulatory standards of regions may align in some but not all areas, and the inadequate implementation and coordination of regional and national policies can present a further risk to the SCNs operational activities (Opitz-Stapleton et al., 2021). The uncompromising resolve of a region to maintain existing practices, such as those related to GMOs, fossil fuel usage or the fur industry, can add to controversies of maintaining network relationships and inhibit attempts at a joint resolution (Vari & Linnerooth-Bayer, 2001). In addition, conflicting positions on issues between nations or political jurisdictions related to information sharing, the explaining of risks and recommendation of response implementations in a transboundary risk setting, can facilitate distrust, misperception, and confusion by the public (Kasperson & Kasperson, 2001). The influence of regional characteristics on TSCs can be illustrated by the bovine spongiform encephalopathy (BSE), i.e., mad cow disease, controversy regarding potentially contaminated UK beef where differences in regional policy and management practices, along with public perception, resulted in a world-wide ban on British beef products which adversely impacted the beef industry (see Kasperson & Kasperson, 2001). Differences in discourse and administrative procedures between the regional institutions and governments that the SCN is exposed to, may therefore result in different understandings of risks and management practices amongst the network members inhibiting coordinated risk management responses (Vari & Linnerooth-Bayer, 2001).

Similarly, the regional significance of certain social and political values, such as ethical work practices and use of renewable energy sources, can place additional restrictions on cooperation between network members by limiting sourcing alternatives and supplier flexibility (Löfstedet & Sjöstedt, 2001). Taking these aspects into account, I argue that further consideration should be

given towards the regional policy backgrounds and values, political relations, socio-political tensions, and the national history of the regions in which the SCN operates. Nations with a history of unrest and poor collaboration with neighbouring regions are generally less willing to enter into working relationships, potentially having an adverse impact on SCNs crossing between these regional borders (Löfstedet & Sjöstedt, 2001). Illustratively, a SCN with up- or downstream network members in Africa might have to account for the likelihood of increased political tensions or regional instability, which could result in financial and resource insecurity (see Opitz-Stapleton et al., 2021).

3.1.2 Micro domain

The micro context refers to the events which originate as a direct result of the SCNs internal activities and relationships. It covers the risk drivers and sources internal to the network. Understanding the micro, i.e., internal, context is relevant as these factors influence how the network members manage their risks and the interacting risks between network members (de Oliveira et al., 2017). Organisations interdependencies result in greater vulnerability or risk exposure for a network member when a disruptive event impacts another member either upstream or downstream. Moreover, the supply chain practices and characteristics change the network members exposure to risks. As a result new approaches for managing these risks are required (Bandaly et al., 2012). In essence the micro context covers the organisational risk environment; that which lies within the boundaries of the SCN and its members, such as production and labour uncertainties. Two micro domains are highlighted in this thesis: the SCN relations which is related to the collaborative relationships between network members, and the SCN infrastructure.

The supply chain network relations

The SCN relations risk domain is included as part of the TSCN risk domain for three main reasons. Firstly, the risks associated with the SCN relations arise from the interactions between the network members as a result of the dynamic network structures of modern supply chains (Norrman & Jansson, 2004). This may increase SCRs by complicating the network members' interactions. An effective TSCRM process can only be implemented if a sense of trust and community is present between network members and if institutional arrangements are in place, allowing the SCN to operate across borders (Linnerooth-Bayer, 2001). Good SCN relations are therefore required for effective and efficient TSCRM and successful implementation of risk responses. Secondly, SCN relations have mostly been neglected in previous framework developments. The importance of relational risks is supported by Jüttner et al. (2003), who found that SCN complexity weakened the organisation's ability to control and perceive the network

members beyond those in an organisation's Tier 1 supplier group. Thirdly, the different organisational cultures developed by organisations shape how risks are identified, assessed, and communicated (Kasperson & Kasperson, 2001). The individual adaptive actions taken by one network member might create or transmit additional risks along the network (Opitz-Stapleton et al., 2021); thereby influencing the performance of other network members, increasing their vulnerability to risk events (Bandaly et al., 2012; Manuj & Mentzer, 2008a). Thus, a network member's actions can influence the risk exposure of other members in an advantageous or adverse manner, impacting the level of success associated with implementation of management processes (Ritchie & Brindley, 2007a).

An important part of the SCN relations risk domain is the consideration towards collaborative relationships within the SCN. Effectively managing transboundary risks demands inter-organisationally coordinated responses to dynamically prepare and react to current and future events (Opitz-Stapleton et al., 2021). Opitz-Stapleton et al. (2021) argued that the key to addressing transboundary risk issues lies in the implementation and strengthening of coordinative activities. Without collaborative activities, effective management of transboundary risks would presumably become less likely, and the alignment of goals, risk attitudes and joint agreements become more challenging. Moreover, TSCs are dependent upon a high degree of coordination between information, goods, services, etc., both locally and across national boundaries (Manuj & Mentzer, 2008a). Lavastre et al. (2014) suggested that establishing a collaborative relationship amongst the network members is an efficient way to manage SCRs when focusing on inter-organisational risk management. Similarly, Petit, Fiksel and Croxton (2010) proposed that SCNs must endeavour to create strong cross-organisational collaborative relationships to effectively be able to manage the numerous interrelated operations which exist between network members both upstream and downstream. Datta (2017) provided support for this perspective, arguing that good collaboration is needed between trading partners and across organisations. The author argued that such collaborative efforts could facilitate the pooling of resources and improve resilience of the SCN (Datta, 2017).

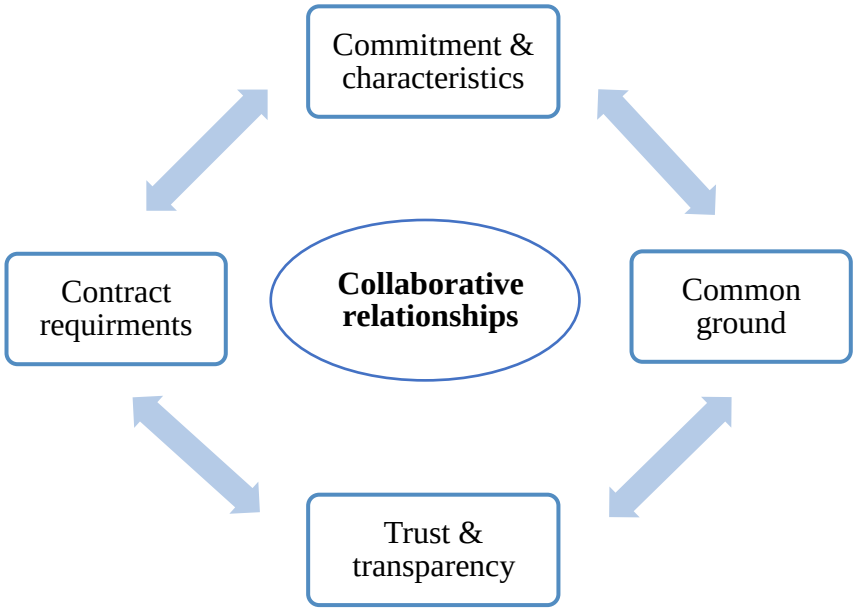
From the perspective of TSCRM, collaborative relationships could be particularly important for effectively managing the risk exposure shared among the individual network members and for implementing risk responses. This perspective corresponds to Manuj and Mentzer (2008a) who argued for the relevancy of maintaining amiable relationships with partnering members of the SCN, local communities and authorities. Hence, a strong collaborative relationship could facilitate the implementation of TSCRM practices throughout the SCN, by encouraging network members to incorporate transboundary management practices into their operations (Norrman &

Jansson, 2004). The application of this framework could then potentially assist international collaboration by building on and sharing knowledge, infrastructure, and strategies. Collaboration between network members may further reduce SCRs through improved risk awareness and risk responses, general communication, communication of failures, and joint problem solving (Chen et al., 2013).

The performance of the collaborative relationships are influenced by four features: the commitment and characteristics of network members, common ground, the contract requirements, and trust and transparency between network members (G. Li et al., 2015). These characteristics are presented in Figure 3.

Figure 3

SCN relation model



Note: Adapted from G. Li et al. (2015).

The c*ommitment and characteristics* feature is closely related to the risk exposure associated with TSCN relationships. The roles, motivations and capabilities of network members, have been suggested to influence the ability to recover from and the overall impact of a disruptive risk event (Datta, 2017). These cross-border partnerships may then strongly influence the stability of the network members' dynamic cooperation. Furthermore, risk exposure of large organisations tend to become greater with inter-organisational networking, and research has found that having small to medium sized enterprises (SME) as part of the SCN increases the overall SCRs (Ritchie & Brindley, 2007a). Generic characteristics of organisations, including sector, size, internal structure, maturity, and flexibility thereby inform and influence the TSCRM process.

Furthermore, early communication, consistent actions, and trust are important to demonstrate commitment towards the collaborative relationship and for establishing long-term relationships (Datta, 2017). Klein (2009) argued that long working relationships result in shared experiences and understanding about how situations should be handled and responded to. This could then improve the SCNs ability to adapt and recover from disruptive events.

Creating *common ground* can be important when selecting and implementing risk responses. Common ground is the set of history, beliefs and knowledge that individuals share between them, and that aids in their joint cooperation and understanding (Klein, 2009). This common understanding of the SCRs need to be shared within the organisation and across the SCN (see Klein, 2009). Local organisations in different geographical locations may have radically different approaches and priorities in their operations (Manuj & Mentzer, 2008a). Issue clarification can therefore represent an important strategic element in the development of transboundary collaborative relationships (Sjöstedt, 2001). Having a shared understanding, i.e., common ground, can enable managers to better predict the responses and actions of other network members to a specific disruptive event (Klein, 2009), which would, arguably, enhance the adaptability and flexibility of the SCNs' operations. A deliberate risk reconstruction can here be used to harmonise the differences in risk perceptions and interests into a common understanding about the given risks and risk contexts (Sjöstedt, 2001). Establishing common ground is, however, challenging, particularly due to the different experiences that colour individuals' understanding about situations (Klein, 2009). Individuals or actors who do not share a similar definition of a risk problem may, for instance, be less likely to agree to solutions or responses corresponding to that specific risk (Thompson & Gyawali, 2001). Monitoring common ground for breakdowns, including signs of confusion and resolving issues as they occur, becomes important. This requires proactive communication practices alerting other network members to new potentially disruptive events/developments (Klein, 2009).

Formalising *contract requirements* facilitates collaborative relationships. They reduce the ambiguity between trading partners by increasing the visibility regarding individual responsibilities (Datta, 2017), and contribute to improved performance (Lavastre et al., 2014). Risk-sharing contracts have been suggested by Wakolbinger and Cruz (2011) as a means to enhance the collaboration between network members by more effectively distributing the risks among the members. Datta (2017) further argues that collaborative relationships among the network members should formalise contracts that have detailed knowledge related to the specific network situations and that are adaptable to new information. This adaptability is important as different risk responses are required for different types of risk. As such, formalising contract

requirements, which acknowledge that the response strategies effective for dealing with one specific risk may have adverse consequences for other risks and other network members, is therefore warranted (Sjöstedt, 2001). These contracts also need to account for the interests, attitudes and cultural backgrounds of the parties involved to facilitate contractual compliance (G. Li et al., 2015). If the parties involved in the contract development process do not understand the differences existing between culturally different parties, it may have long-term repercussions for their collaborative relationship (Sjöstedt, 2001). Should these differences be concealed or unclear at the beginning of the contract development process it may result in misunderstandings and incorrect impressions which, down the line, complicates collaborative activities (Sjöstedt, 2001).

Such complications may lead to frustration, friction, or irritation causing noncompliance on the part of a network member, which affects the performance and efficiency of the SCNs' operations. Noncompliance may also be triggered by a perceived lack in sense of ownership. This lack in sense of ownership is triggered by supply chain trends, including outsourcing, focused factories and increased use of logistic partners, which complexify the network relationships and make lines of responsibility more opaque (Jüttner et al., 2003). An option for facilitating contract compliance is the inclusion of requirement guidelines into the contracts. This establishes the scope and expectations of the involved parties early on. Such requirements could include the responsibility of an organisation's supplier to e.g., identify back-up sites, regularly update risk management plans, train key personnel, and place similar requirements for and encourage proactive risk management from their own contractors and sub-suppliers (Norrman & Jansson, 2004).

Trust and transparency is reliant on the perceived commitment to an objective or goal, which in turn depends on access to accurate information and on how the objectivity and fairness of the decision-making process is perceived (Kasperson & Kasperson, 2001). Mutual trust between parties requires shared coordination and a shared societal context, achieved through the proactive engagement with network members (Petersen, 2019). Such engagement may include activities which incorporate various types of perspectives and knowledge in order to better inform the decision-making process by providing different situational interpretations or facilitating active participation by network members (Petersen, 2019). However, the unreflective application of a familiar risk management practice by a network member, without accounting for the different characteristics of the network member, could undermine the trust and viability of this member's relationship with other organisations in the SCN. Acceptance and implementation of transnational strategies are closely related to the perceived transparency and fairness of the decision-making process (Linnerooth-Bayer, 2001). Linnerooth-Bayer (2001) discussed how

different risk assessment and management practices impacted institutional credibility and trust using the UK's risk management of BSE as a case study. The lack of transparency and the diverging assessments of risk during this incident adversely influenced the publics' and other European countries trust in the UK's governing body (Linnerooth-Bayer, 2001). Hence, an important part of establishing collaborative relationships is transparency, this in order to build trust and avoid hidden agendas or the perception of having them (Renn & Klinke, 2001).

The supply chain network infrastructure

The SCN infrastructure risk domain encompasses a wide range of risk drivers associated with the performance of SCN related processes. Infrastructure here includes the information, transportation, financial and manufacturing systems along with other industry specific aspects. Risks within this domain may, for instance, be technical threats, which may include equipment failures, or logistic flow of information and materials. Other risks, such as for service supply chains, may include a demand influx which could adversely impact their performance and provision of reliable services (Komatsubara, 2014). The SCN infrastructure plays a crucial role in the efficient management of supply chains (Ho et al., 2015). Damages to major infrastructure, such as transportation, communications, or power systems, can disrupt the flow in SCN operational activities. This could in turn increase an organisation's exposure to SCRs, including production and export delays, and financial distress (Opitz-Stapleton et al., 2021). Having an emphasis on SCN infrastructure is therefore considered appropriate for a TSCRM process.

Communication and information sharing infrastructures, both of which rely on trust, are a particularly critical aspect of the SCN infrastructure risk domain given its importance for transboundary collaboration. Proper communication and information sharing structures provide a means for improved sensemaking of the dynamic transboundary operating environment (Steen & Pollock, 2022). Sensemaking refers to seeing what led up to current events and anticipating how the resulting actions taken will influence future events (Klein, 2009). Lavastre et al. (2014) found that for SCRM to be effective, it required long-term information sharing with partners. Additionally, Jüttner (2005) argued that a willingness to share risk-related information and view SCRs as joint risks, made up the foundation on which effective SCRM could be built. The importance of risk information sharing for TRM was further proposed by Prabhakar et al. (2021). The authors suggested that robust information systems were required in the risk assessment to facilitate the identification of effective preparedness, response, and mitigation efforts. This is in line with Datta (2017) who maintained that good information sharing structures promoted agility in the supply chain, improving responsiveness and joint problem solving. Moreover, the network members' information sharing improves the SCNs' visibility to vulnerabilities (Kleindorfer &

Saad, 2005). Within the TSC context, research has shown that the capacity of an individual to acquire, distribute and use external knowledge effects their ability to respond to SCRs (Datta, 2017). Without the proper distribution of knowledge and know-how among the network members, it may be difficult for them to honour their contractual commitments even if they aim to do so, which may result in unintentional non-compliance (Sjöstedt, 2001).

Communication can be an important tool for managing transboundary risks (Svedin, 2001). Conflicting perceptions and concerns are an inevitable aspect of managing transboundary risks, which arguably make adequate communication structures important. Asymmetry in information distribution, amongst network members, occurs frequently due to poor communication structures/practices, especially as the supply chains grow more complex (G. Li et al., 2015). Information about actual demand(s) might, for instance, be unknown to suppliers in the SCN regardless of the retailers being in possession of this information (Chu & Lee, 2006). As such, without effective communication, reduced transparency and increased distrust in the decision-making process could be expected (Löfstedet & Sjöstedt, 2001). The Covid-19 pandemic and the Russia-Ukraine conflict demonstrates not only the impact transboundary risks have and the importance of cross-border collaboration, but also the need for effective transboundary communication and information sharing mechanisms (Opitz-Stapleton et al., 2021). Basic preparedness requires communication along with the sharing of knowledge and information (Kasperson & Kasperson, 2001; Svedin, 2001). The collaborative importance of engaging in communication and information sharing across national borders in a TSC, therefore substantiates its inclusion in a TSCRM framework. Without proper information sharing and communication infrastructure, solutions and responses are not developed or implemented as the information for understanding the transboundary risks is not shared across borders (see Prabhakar et al., 2021).

3.2 Anticipate

Anticipation involves activities for predicting and preventing potential disruptions. This requires the risk to be identified and assessed (Pillay & Morel, 2020). The risk identification process and situational assessment are therefore attributed to the anticipation area of resilience. Awareness regarding potential risks and the ability to prepare for them is heightened through identifying and assessing risks (Kasperson & Kasperson, 2001). Moreover, the ability to anticipate future scenarios promotes the monitoring and preparedness of activities associated with the anticipated scenarios (Provan, Woods, Dekker, & Rae, 2020).

3.2.1 Risk identification process

The risk identification process is a critical risk management phase, especially when dealing with transboundary risks. Only those risks which have been identified and mapped out can be assessed, evaluated and responded to (Kern et al., 2012). Risk identification must cover not only direct operational risks but also the risk drivers and sources at every significant level along the SCN (Ho et al., 2015). The aim of the risk identification is therefore to discover all relevant SCRs. This implies the need for early judgements to decide the relevancy of a given risk (Kern et al., 2012). However, how this identification process should be performed differs between researchers. Some approaches suggested for the identification process include checklists, event and fault three analyses, and cause and effects analysis (see e.g., Tummala & Schoenherr, 2011). The purpose of this paper is to provide a guiding framework that is adaptable to differences in industry and sector practices as the preferences and requirements for selected identification approaches vary between industries. Providing a thorough overview of the different approaches suggested in prior research is therefore beyond the scope of this thesis.

Nevertheless, a brief description of the approaches mentioned has been provided. Checklists are used to record the frequency at which a failure is being attributed to a given event. From these checklists data collection can be standardised (Aven, 2015a). Event and fault tree analyses provide a graphical representation of all potential outcomes resulting from a given event (Aven, 2015a), including failures in the supply chain. Through these approaches, the potential events and corresponding responses resulting in the undesirable event can be mapped out. The cause and effects analysis involves the exploration of every potential interaction between the cause and the failure in order to facilitate the discovery of the root causes resulting in the undesirable event (Aven, 2015a). The reader is referred to Tummala and Schoenherr (2011) for additional information on these and other approaches.

The risk identification phase of the TSCRM accounts for global and domestic risks within and along the SCN including how the regional contexts interact with the SCN and a broadened scope beyond direct suppliers. Broadening the identification process beyond direct suppliers could be critical for understanding the big picture of a complex TSC. Identifying risk drivers and sources within this broader context enables managers to get a thorough and structured overview of the potential SCRs (Norrman & Jansson, 2004). In addition, clear risk identification and understanding of consequences related to the five different TSCN risk domains may facilitate the effective implementation of selected risk responses (Tummala & Schoenherr, 2011). A comprehensive risk identification process is also required to shed light on the intricacies of TSCs. The SCRs are interrelated: one risk can influence, lead to, or increase the exposure to other risks

within and along the SCN (Tummala & Schoenherr, 2011). The risk response actions of one network member can result in risks for other network members, such as inventory-related risks, which may be passed onto a third party or supplier (Bandaly et al., 2012). Thus, managing SCRs cannot be regarded as a set of independent approaches for responding to a specified risk. As such, understanding these variations and interrelations of SCNs is important (Tummala & Schoenherr, 2011). The identification phase of the TSCRM introduces a broader risk classification taxonomy for more detailed identification of external and internal SCRs by incorporating the TSCN risk domains from the situational awareness phase. It further includes SCN mapping and feedback processing and takes the management perceptions into consideration.

Risk classification

The classification of risks is considered a prerequisite for risk identification (Bandaly et al., 2012). Classification schemes aid in clarifying relevant dimensions of possible disruptive events which may affect the SCN, and provide a foundation for the assessment and evaluation process (Bandaly et al., 2012). Transboundary risks spread via many different pathways and are often not recognised given the challenges related to identifying these risks and assessing their trajectory and impact. Systemising a classification approach might simplify the identification process and elucidate how risks are related, what influences them and where they might originate by enabling more detailed risk profiles to be established, as shown later in Table 1. A two-step classification approach is proposed in this thesis consisting of a broader classification scheme covering intent (see Figure 4), and a classification process for understanding pathways (see Figure 5). Both originate in the previously described TSCN risk domains. Following Linnerooth-Bayer (2001), the broad classification scheme first distinguishes between voluntary (i.e., risks associated with the decision made, for example the localisation of manufacturing facilities) and involuntary (i.e., risks outside of the organisations control, such as climate change) risks. Based on the work of Sheffi & Rice Jr (2005), a sub-classification into three dimensions of intent is suggested consisting of: random events (e.g., earthquakes or war), intentional (incurring due to the intentional actions of external or internal stakeholders or other malicious actors) and unintentional (accidental events) risks.

A robust classification of transboundary risks in the identification process needs to address the pathways leading to a disruptive event to better understand the conditions leading to their development. The classification process presented in Figure 5 uses a four-dimensional classification taxonomy consisting of the risk domain, risk drivers, risk sources, and disruptive events, extending the frame of current identification processes. The purpose of such a classification process is to better distinguish the scope, i.e., pathways, of the identified risks

emanating from the five TSCN risk domains (see Figure 1) thereby specifying the overarching risks and the subsequent manifestations of that risk. It supports the emphasis on connections between precursor and proceeding events. A willingness to think across regional borders is considered by Prabhakar et al. (2021) as necessary when dealing with the TSCR's interconnective nature. This classification of the pathways between four risk levels could make the TSCR's origins easier to frame and their global situational context more comprehensible.

Figure 4

Broad classification scheme

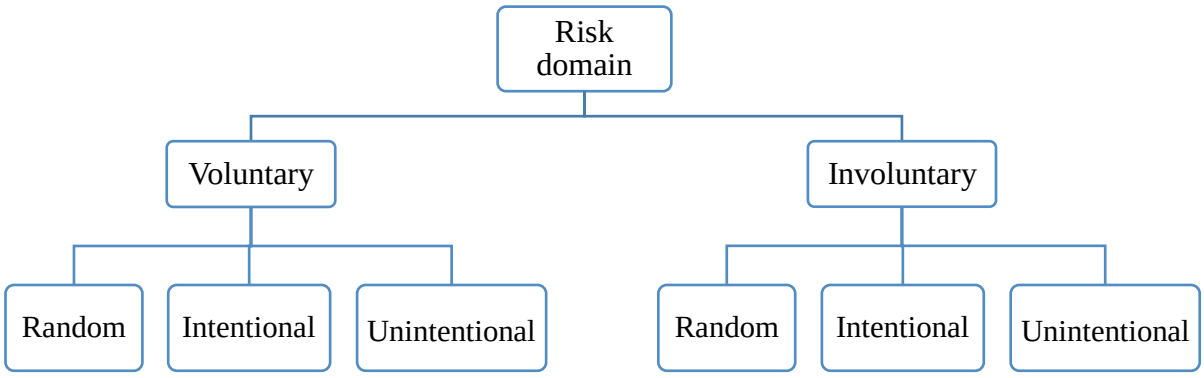
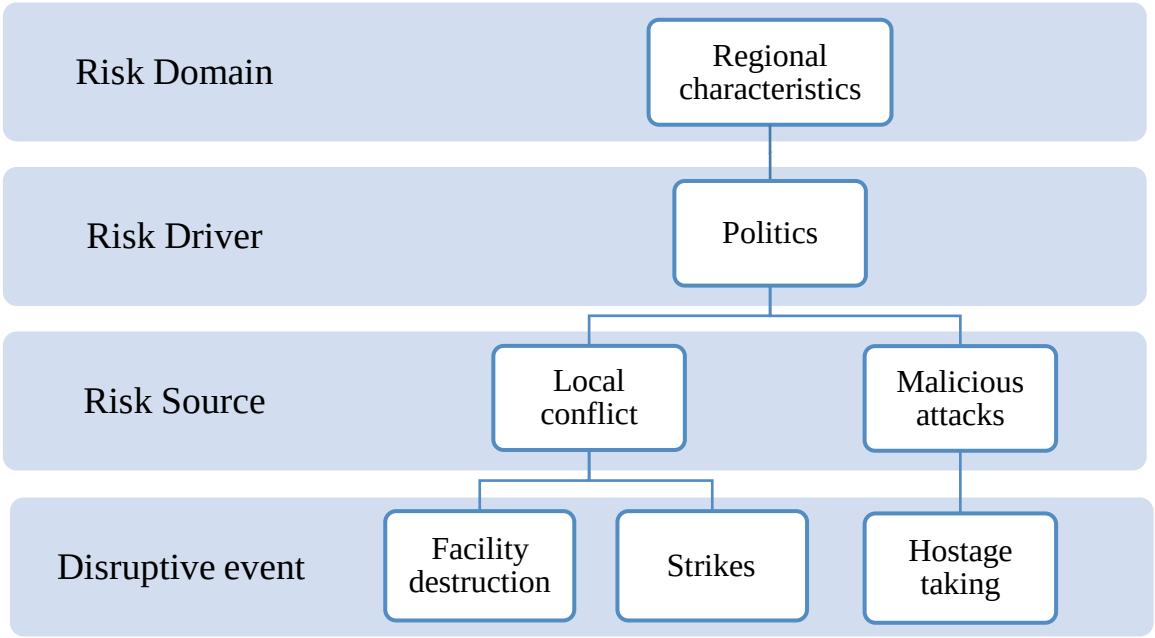


Figure 5

Classification process model exemplification



This risk driver may then be separated into different risk sources which manifests associated disruptive events. Risk drivers represent the second level of the classification process emanating

from one of the five TSCN risk domains. Transboundary risk drivers within these domains may consist of trade activities, political agendas, and financial actions. In Figure 5, regional characteristic represents one of the five TSCN risk domains. Within this domain, regional politics may represent a risk driver. The risk sources in Figure 5, local conflict and malicious attacks, represent the manifested risks attributed this risk driver. The sources of risk can be challenging to predict with certainty (Jüttner et al., 2003). Other suggested risk sources may relate to the export and/or import of climate-sensitive goods, boarder sovereignty, human displacement due to regional events, and international risk mitigation actions impeding national adaptation (Opitz-Stapleton et al., 2021). The different risk sources manifest associated disruptive events, here identified as facility destruction, strikes, and hostage taking, which impact the functioning of the supply chain by disruption the SCNs operational activity.

Various risk source categorisations are presented in literature including supply, demand, manufacturing, security, operations, information, transportation, financial, resource, and partnership collaboration (see e.g., Bandaly et al., 2012; de Oliveira et al., 2017; Ho et al., 2015; Manuj & Mentzer, 2008a; Norrman & Jansson, 2004; Pournader et al., 2020; C. S. Tang, 2006; Tummala & Schoenherr, 2011). However, within the four-dimensional classification taxonomy these risk sources would be considered drivers of risk as within such general classifications there are underlying risks which can be represented as sources of disruptive events, as shown in Figure 5. I will not provide an elaborate explanation of the various risk drivers, but rather limit a brief description to the four drivers: supply, security, information, and transportation. These are considered particularly relevant for the transboundary risks prevalent in TSCs as they disrupt the SCN operations, and the majority of these risks exist in relation to and influence each other. The risk drivers and sources mentioned in this paper are not exhaustive but illustrate the multitude of risks that could be present.

The supply risk driver is related to the distribution of every potential risk associated with the incoming supply that may compromise the SCNs ability to meet demand (see e.g., Manuj & Mentzer, 2008b). The supply risk driver may manifest associated risk sources, including critical resource dependency. This resource dependency may, as seen by the Russia-Ukraine conflict, result in disruptive events related to inventory and production losses. The security risk driver relates to the outcomes from disruptive events, beyond the organisations direct control, which may adversely compromise firm integrity, information systems and human resources, such as data breaches and currency fluctuations (see e.g., Ho et al., 2015; Manuj & Mentzer, 2008b). A data breach, as the one at Norkart in May of 2022 (Datatilsynet, 2022), might here represent a source of risk potentially resulting in reputational damage and financial penalties. The

information risk driver is associated with events likely to impact the systems and structures that are in place which allows the flow of information and knowledge between network members and external stakeholders (Manuj & Mentzer, 2008a). This driver may lead to misinformation, human errors, and performance loss, amongst other risk sources. The transportation risk driver encompasses the disruptions in the transport modes and providers which influence the import and export flows of the SCN (Manuj & Mentzer, 2008a). Risk sources, including the dependency on a single transport alternative, construction, road destruction or driver/fuel shortages, may emanate from this risk driver.

Table 1

Risk profile template

TSCN risk domain	*Risk driver*	*Risk source*	*Localisation (Domestic / Global/Both)*	*Upstream or Downstream*	*Voluntary / involuntary*	*Random, intentional, unintentional*
External stakeholder						
External environment						
Regional characteristics						
SCN relations						
SCN infrastructure						

Viewing previously defined risk sources as risk drivers provides an opportunity for additional specifications of the SCRs and may contribute to greater understanding of their underlying causes and interactions. I argue that this two-step classification approach facilitates the implementation of more suitable, flexible, and efficient responsive actions allowing them to better cope within a dynamic global operating environment. This perspective is supported by Opitz-Stapleton et al. (2021), who argued that failure to expand the thinking from local to global creates cross-border risks. To further simplify the identification process, a generic risk profiling template is proposed and presented in Table 1. This generic template for profiling risks incorporates the elements from the two-step classification approach providing a structured overview of the classified risks

highlighting their pathways and intent in a systematic manner. The organisations exposure to risk is also dependent on geographical location (Ritchie & Brindley, 2007a). To account for this, the table includes a dimension for sorting the risk's origin into global and domestic. Although some of the drivers and sources may be local to a specific network member, they may still have an impact throughout the SCN (Ritchie & Brindley, 2007a). The up- and downstream column is therefore added for simple overview of where within the SCN a risk may emanate from.

Supply chain network mapping

Following the classification of risk, SCN mapping is recommended to get a better understanding for the dynamics and interactions inherent in transboundary risks. The SCN mapping is a tool that provides a structured approach for mapping the drivers and sources of risk used to get a better understanding of the potential consequences related to a specified risk (Norrman & Jansson, 2004). It also accounts for the industry characteristics (Bandaly et al. 2012). The SCN mapping approach visually depicts the supply chain and the flow of information, resources and goods throughout the entire network (Tummala & Schoenherr, 2011). A strategic supply chain map may assist management in their modification of supply chains (Tummala & Schoenherr, 2011) through its visual overview of the SCN. Being able to adapt, i.e., appropriately modify supply chains, is needed for effective management of TSCRs as transboundary risks can have regional, multi-country or international implications for the SCN as a whole (Opitz-Stapleton et al., 2021). Suggested techniques for SCN mapping are the logical diagrams of event and fault tree analyses, both representing the proposed failure sequences which may cascade through complex systems (Norrman & Jansson, 2004).

The SCN mapping helps identify key supply chain locations, i.e., those locations where an interruption majorly disrupts the operational flow of the supply chain. Locations, such as the main distribution centre, main transportation terminal, or the chains single raw material supplier, exemplify some possible key locations which cannot be substituted easily. Approaches for identifying key locations are specified in Knemeyer, Zinn and Eroglu (2009) to which interested readers are referred. Accounting for network-related interactions and dependencies is important for understanding the ability each network member has for absorbing or amplifying the impact from a disruptive event (Jüttner et al., 2003). SME are more fragile, with greater risk exposure, in changing and complex global environments compared to larger and multinational organisations. SMEs face greater competition and are often less prepared to respond to disruptive events due to restricted resource availability, size and sensitivity to external business environments (Bak, Shaw, Colicchia, & Kumar, 2020).

The risk exposure of multinational organisations, heavily dependent on interacting with SMEs, may then be affected should the SMEs not have the adaptive capacity to change in line with market conditions, such as exchange rates and price fluctuations. This could potentially have significant consequences for the SCN (Bak et al., 2020). It is therefore important to understand the capabilities and limitations of network members at every significant level of the SCN, given the high reliance each member has on the successful operations of the others. Hence, identification of network risks requires a thorough understanding of the SCN's structure, complexities, dynamics and horizontal interactions which cannot be covered through traditional risk management practices (Jüttner et al., 2003). Comprehensive mapping and classification of risks can then assist the identification of risks and the differing degrees of impact associated with these risks (see e.g., Ho et al., 2015). However, visibility across the entire SCN is challenging. Control towers, a cloud-based tool for establishing end-to-end visibility across SCNs, can be implemented as a means to improve visibility and better understand the risk contexts and where the risks lie (Kilpatrick, 2022). By organising and distributing data in a consistent format, control towers can provide proactive alerts, timely visibility and keen insights by using technology infrastructures, such as AI and advance analytics (Kilpatrick, 2022). This in turn improves situational awareness and the identification of risks across the extended SCN. Through such efforts, the ability to anticipate, prepare for and adapt to disruptions is enhanced (Kilpatrick, 2022).

Feedback processing

Part of a comprehensive identification process for TSCRM is the incorporation of feedback processing. Feedback processing entails the identification of past and current information regarding risk responses, risks, trends and unfolding situations which may facilitate current and future identification, classification, and management of risks. It involves the monitoring and analysis of areas, including internal and external communication, processes, information, and responsive actions. The severity of a disruptive event is influenced by the length of time taken by the organisation to become aware of the risk and understand its disruptive impact (Craighead, Blackhurst, Rungtusanatham, & Handfield, 2007). Part of resilience thinking is the ability to anticipate long-term threats (Lay & Branlat, 2014). For the SCN to be able to adapt and adjust to unfolding events it needs to be able to recognise early signals in its operating environment along with the implications from the network members' actions (Herrera & Hovden, 2008). It therefore requires a proactive ability to recognise future risk-related issues and vulnerable points along the extended supply chain (Norrman & Jansson, 2004). Using feedback processing to inform the risk management process would, arguably, enable anticipatory thinking and proactive TSCRM.

Feedback processing contributes to the flexibility required for effective implementation of risk responses (Lay & Branlat, 2014). By analysing the feedback from the SCNs operating environment and overall actions, relevant risks can be recognised and assessed, and response strategies implemented earlier (Kern et al., 2012). Using feedback processing to develop abilities that facilitate early predictions of disruptive events may therefore be advantageous. However, limited resource availability necessitates what Kern et al. (2012) refers to as observation fields to focus the scope of the feedback processing. These observation fields encompass known risk drivers and sources along with the most critical supply chain areas. Given the complexity of TSCs, the development of such observation fields requires knowledge about the most critical areas within the TSCN risk domains, so that resources are focused appropriately (see Kern et al., 2012). Such knowledge can be obtained from the SCN mapping. By including feedback processing into the construct of the TSCRM framework's risk identification phase, regular monitoring and greater awareness of new potential risks and areas along the SCN with greater risk exposure is promoted.

Managements risk perception

Managers risk perceptions, i.e., how the risks are understood and perceived by the individual, are important for understanding the focus and scope of the risk identification in global environments (Bandaly et al., 2012). Similar to other risks, transboundary risks are socially constructed, meaning that what a manager perceives the risks to be and what they really are can't be fully and unambiguously distinguished (Thompson & Gyawali, 2001). Socio-cultural settings are not standardisable, nor transferrable between regions, due to their unique characteristics (Lupton, 2013). The social context in which organisations operate will then impact how individuals construct their views relating to the severity of a particular risk (Linnerooth-Bayer, 2001). How knowledge and information is presented will influence how a situation is perceived and thereby determine the level of commitment taken by individuals when investing in their risk responses (Sjöstedt, 2001). Hence, the perception and construction of risks influence management practices (Linnerooth-Bayer, 2001). Perceptual differences, influencing risk management, are suggested by Douglas (1992) and Lupton (2013) to be linked to the variations between individuals and groups, including their diverging interests, norms, cultures and sociological structures. As such, the risk perceptions of different managers are affected by different aspects, including the managers' mental models, previous experiences, national socio-cultural values, attitudes towards risk taking and other personal factors (Bandaly et al., 2012).

The attention a risk is given will followingly vary amongst the different societies and cultures of the SCN, reflecting the values and concerns of each network member (Lupton, 2013). The

identification and following assessment is therefore not a straightforward process as the different managers have risk perceptions which vary from one another. Decision-makers have a tendency to only take a partial view of the situation at hand and the corresponding risks, meaning that they may seek to focus on addressing those risk related issues most salient to them (Ritchie & Brindley, 2007a). By emphasising certain risks over others, each individual manages to define the issue in a manner which conforms with the response option they wish to implement (Thompson & Gyawali, 2001). Interpretations and signals are often disregarded or attenuated if they contradict the values of the individual or are inconsistent with their beliefs (Kasperson & Kasperson, 2001).

Furthermore, the capacity to recognise potential risk factors is also dependent upon various organisational factors including the history of the organisation i.e., their experience to the process, the current operational environment and goal of the organisation (Klein, 2009; Ritchie & Brindley, 2007b). As such, the industries in which managers operate further influence their approach to managing and interpreting SCRs. Managers need to acknowledge these perceptual variations in industry mindsets and aim to take them into consideration during the TSCRM process (e.g., Manuj & Mentzer, 2008a). In this regard, it may prove advantageous to implement a team-based approach to the risk identification in TSCRM. Manuj and Mentzer (2008a) argued that for TSCs, the use of cross-functional teams leverages the diversity intrinsic to the individual team members. The TSCRM process thereby becomes conscious of and sensitive to the biases and perceptual differences present between network members and managers. In addition, it may reduce the supply chain vulnerabilities by contributing to a more inclusive classification and mapping of the SCRs (Jüttner et al., 2003). Awareness to the perceptual differences between managers within the same organisations and other network members is therefore considered relevant for the TSCRM process.

3.2.2 Situational risk assessment

Following the risk identification, a situational risk assessment is proposed for the TSCRM framework to determine the criticality, i.e., impact and severity, of the identified risks. It is necessary to have an understanding of what contributes to the occurrence of a risk. This requires additional attention on the risks inter-relatedness and triggers (Kern et al., 2012). The objective of the situational risk assessment phase is to provide the required in-depth information and understanding about each risk, including their effect on and relevancy for the organisation and the SCN as a whole. The outcome of the assessment phase feeds into the evaluation and prioritisation of which risks should be focused on and to what extent, enabling more effective risk responses (see Kern et al., 2012). The situational risk assessment suggested in this thesis

includes four main areas: 1) a traditional risk assessment, 2) a vulnerability assessment, 3) global scenario planning, and 4) a future trend prediction. Expanding the assessment phase beyond a traditional risk assessment allows the TSCRM framework to comprehensively accommodate for the dynamic and complex global environment. Key vulnerabilities and the identified risks' causes, severity, impact and global interaction are here accounted for at every significant link along the SCN, in addition to future global trends. Having a broad understanding of the identified SCRs both at network level and on a global scale, and an awareness of potential future trends that could significantly influence the SCNs operational activities would, arguably, facilitate the implementation of appropriate and flexible long-term risk responses.

Traditional risk assessment

There are several ways in which a risk assessment can be conducted including (in)formal, qualitative and quantitative (Fan & Stevenson, 2017). Within SCRM research the assessment of risk entails, in particular, the evaluation of two variables: the likelihood of a disruptive event and the impact severity from a disruptive event (Bandaly et al., 2012). These two variables are generally agreed to be the basic risk dimensions in SCRM literature (Bandaly et al., 2012). Impact here refers to the consequence resulting from the realisation of the risk, covering not only tangible impacts but non-regulated intangible impacts as reputation, credibility and trust (Fan & Stevenson, 2017). Understanding the impact severity informs the decisions when determining appropriate risk response strategies. During the risk assessment process the likelihood and impact severity magnitudes are quantified. Both objective information and probability distributions may be utilised in the assessment (Lavastre et al., 2014). Historical data can be used to measure the risks likelihood and impact severity, and for understanding the distribution of the risk probabilities. Additionally, impact can be determined using performance metrics some of which are return loss, time delay, and lost market shares (see e.g., Bandaly et al., 2012).

A challenge when using objective information, such as historical data in the risk assessment process, is that it may not always be available, reliable or adequate (Manuj & Mentzer, 2008a). Access to relevant or enough data may, for instance, not be present for rare or infrequent events, such as tanker spills, nuclear reactor meltdowns and outsourcing manufacturing activity to a different regional area. Subjective knowledge, judgements and beliefs are therefore needed in situations where objective data is lacking or unavailable (Lavastre et al., 2014). This combination of subjective and objective data may contribute to a more robust risk assessment by providing more data in which the assessment can be made (Fan & Stevenson, 2017). Qualitative assessment approaches, including expert focus groups or the Delphi method, may, in these instances, provide the necessary subjective data to assign probabilities when objective data is insufficient (Manuj

& Mentzer, 2008a). The Delphi method allows individuals to obtain a consensus regarding the situation at hand by repeatedly interviewing knowledgeable individuals, most commonly through the use of questionnaires, and incorporating previous responses into the subsequent interviews (Manuj & Mentzer, 2008a). This method encourages the participant to reconsider and/or adjust their initial responses based on the replies of others (Manuj & Mentzer, 2008a).

The risk exposure calculator is another qualitative assessment method, developed by Simons (1999), used to examine the likelihood of an organisation being surprised by a disruptive event. Using three types of internal pressure: information management, culture and growth, managers are asked to rate the level of pressure from a risk on a scale from 1 (low) to 5 (high) using their subjective knowledge base. This method, although not precise, provides a directional result regarding the level risk exposure (Simons, 1999). An additional method relying on both subjective and objective data is simulations. Simulations may be utilised to model the disruptive effects associated with a specific risk event and visualise how they may propagate throughout the SCN using both subjective and objective data (Knemeyer et al., 2009). These and other qualitative models are useful in situations where there is insufficient data for probabilistic models to build on, or where only an intuitive understanding of the aspect, sector or industry being assessed is present (see e.g., Lavastre et al., 2014; Manuj & Mentzer, 2008a). Using methods that combine subjective and objective data contributes to data diversity and takes localised sources of knowledge into account.

Vulnerability assessment

Part of the situational risk assessment includes locating the most vulnerable areas of the SCN and understanding the form of impact an adverse event may have. This is achieved through a vulnerability assessment. Supply chain vulnerability occurs when risk response strategies are outweighed by the risks, thereby adversely affecting the performance and sustainability of the SCN (Jüttner et al., 2003). Supply chain vulnerability can be separated into two categories: structural (relating to the supply chains tangible and physical configuration) and infrastructural (relating to the supply chains intangible and procedural configuration) (Bandaly et al., 2012). The complexity of TSC structures along with globalisation, greater demand uncertainty and volatility, and increasing rates of innovation, significantly influence the vulnerability of modern supply chains by exposing the network members to greater risk (Bandaly et al., 2012; Negri et al., 2021). In these TSCs the network members' risk exposure becomes greater making them more vulnerable to natural and man-made hazards (Bandaly et al., 2012). In addition, the increased use of modern supply chain practices introduces further vulnerabilities into the SCN. These practices may include greater customer responsiveness by organisations, centralised

decision-making, outsourcing, and use of Just-in-Time (JIT) inventory management. As an exemplification, the use of JIT practices may expose the SCN to reduced response time and buffer inventories, fewer supply options, and loss of control over the supply chain due to its focus on cost reduction through minimisation of inventory levels (Schlegel & Trent, 2014). This may then impact an organisation's manufacturing and export activities increasing their supply risks. The consequences of JIT practices was demonstrated during the semiconductor shortage where low buffer inventories led to a lack of resources, disrupting organisational activities in industries as with the automotive industry (Voas et al., 2001).

The vulnerability assessment needs to account for various aspects including regional conditions, the geographic dispersion of network members, sourcing practices (i.e., supplier selection), and industry specifics. Export and import bans may, for instance, as a result of regional conditions or activities, be triggered by the emergence of new diseases and/or a growing frequency of diseases in crop and livestock. This in turn may make an agricultural supply chain more vulnerable to political and climate related developments, such as trade risks, which may increase exposure to financial risks (Opitz-Stapleton et al., 2021). Assessing vulnerabilities related to geographical dispersion is particularly relevant within a TSC context. Supply chains with greater geographical dispersion have more diversification opportunities and operational flexibility which make them less vulnerable to disruptions (Bandaly et al., 2012). Production can, for instance, be switched between facilities in different regions as a way to offset changes in exchange rates, mitigating the exchange rate risks. It may also clarify further vulnerabilities related to single source dependence or reliance on singular transport routes by highlighting the presence of these dependencies within the SCN (Bandaly et al., 2012). Assessing the vulnerabilities associated with information sharing structures is also relevant. Kleindorfer and Saad (2005) identified increased supply chain vulnerability resulting from inefficient information sharing practices as one of two key SCRM issues. By removing distorted information, the supply chain becomes better prepared to respond to changing conditions. In addition, uncertainty is reduced by providing more accurate information on inventory levels, demand and sales forecasts, and to base strategic decisions on (Bandaly et al., 2012).

Global scenario planning

The interactions occurring between the different SCR impacts suggests that disruptive events are seldom isolated. Global scenario planning covers the interactions and impacts from international disruptive events which may affect the SCN. It motivates organisations to assess various global scenarios based on their type of risk exposure to a given event (Kilpatrick, 2022). Global scenario planning is particularly relevant in modern globalised environments where the effects of an event

may become ubiquitous worldwide (see Kasperson & Kasperson, 2001). Although a situation may not be directly linked to the SCN, the actions taken by external actors can result in additional SCRs and adverse trade flow impacts (see e.g., K'nIfe, 2007). Opitz-Stapleton et al. (2021) suggested that the adaptations made within a country or by a few countries would have repercussions for the national and international conduct of other countries in sectors including trade, finance, and climate mitigation. Changes in technologies, including the creation and application of GMOs, widen the potential impacts and repercussions associated with innovative activities beyond the national borders where they originate (Kasperson & Kasperson, 2001). The controversy surrounding UK's risk management of BSE in the 1990s (see Kasperson & Kasperson, 2001), demonstrated the dramatic transboundary response to a regional event which threatened beef industry SCNs.

When performing global scenario planning the four categories: trigger, transmission, scale, and pathways, may be used when assessing the causes and spread of transboundary risks to direct the planning process. The trigger category relates to understanding how a particular risk is brought on by assessing whether the event was triggered as a result of a shock, a slowly onsetting factor, or a response action (Opitz-Stapleton et al., 2021). Transmission encompasses the assessment of how the risks are spread throughout the TSCN. Risks can be transmitted directly between two entities, or by cascading through a system. The scale category relates to the scope of a risk's spread, covering whether it is regional, systemic, or tele-connected i.e., causally linked between two or more distant systems (Opitz-Stapleton et al., 2021). As a final stage the pathways are mapped out using the TSCN risk domains as overarching categories. Propagation across different pathways is dependent upon elements, such as capacity, vulnerability and the exposure interdependencies among and between regions, in addition to the time taken before the impact affects a specific location, network member or the SCN in its entirety (Opitz-Stapleton et al., 2021).

If the SCN has operations in conflict or unstable areas, it may also be relevant to perform a conflict-sensitivity analysis as part of the global scenario planning process to gauge how sensitive the SCN is to disruptions resulting from regional instability. Global scenario planning would, arguably, have been useful in preparing or monitoring of the Russia-Ukrainian conflict, making management aware of its potential impact on resource supply chains, as for semiconductor manufacturers that required mineral resources provided by Tier 2 suppliers in Russia. Assessing the international trends and situational developments and exploring their potential impacts would here presumably improve SCNs adaptability and anticipation capabilities. When operating in a global environment the duration and magnitude of a disruption is uncertain as is the impact both

in type and scale for the SCN. The approaches taken for production and delivery of goods including innovative activities, the disposal of biproducts and other potentially hazardous materials, stresses the relevancy of assessing transboundary risks on regional and international level. By broadening the assessment scope to encompass the dynamic interactions occurring outside the SCNs, it may allow organisations to make better medium- to long-term determinations regarding risk response strategies.

Future trend predictions

Future trend predictions are an important aspect of anticipatory thinking involving the process of recognising and preparing for potential future disruptions or challenges (Rankin, Lundberg, & Woltjer, 2014). Rather than basing response implementations on past successes, these trend predictions enable organisations to assess and anticipate the oncoming, developing and changing shape of risks prior to their occurrence and prepare for the corresponding impacts (Hollnagel et al., 2006). The presence of imperfect knowledge, knowledge gaps and constantly changing operating environments can make trend prediction challenging (Hollnagel et al., 2006). Analysing repetitive patterns may provide useful information. Exactly where, when and at what magnitude a disruptive event, such as a hurricane, will occur is generally unknown to managers, however, they can obtain information regarding what conditions may lead to its occurrence, and where and when such events are most frequent (Knemeyer et al., 2009). This enables them to anticipate where a future hurricane could develop. Chaos theory may also provide additional guidance particularly useful for risks with extreme severity, that are unpredictable and highly uncertain. Chaos theory maintains that predicting a broad range of phenomena cannot be achieved and attempting to forecast future events is therefore daunting (Knemeyer et al., 2009). This theory provides insight to managers regarding where, when and how the use of controls and predictability logic is possible, and the scale to which these ought to be directed (Knemeyer et al., 2009).

Some trends may be more salient for a wider range of organisations. Consequences of climate change are relevant aspects that all organisations may need to account for in future trend predictions as they can have broad implications within a number of sectors, areas, and industries. An agriculture supply chain might have to account for climate change related trends, including water and land degradation. This might in the future increase the risk exposure of their agricultural production similar to the impact water shortage has shown to have on rice production (see e.g., Opitz-Stapleton et al., 2021). This increased risk exposure can result in responsive actions which impact TSCNs. As an exemplification, the transboundary risks related to food imports have prompted certain countries, such as Nigeria and Chad, to promote food self-

sufficiency through agricultural reform, reducing their reliance on food imports (Opitz-Stapleton et al., 2021). This centralisation of the supply chain, moving from global to domestic suppliers, would then affect the current international network members which are part of this food SCN potentially increasing their exposure to financial risks (Opitz-Stapleton et al., 2021).

The green transition, i.e., the move from a carbon based to a sustainable economy, could be a relevant area of focus for a trend prediction. For the energy sector, a future trend prediction may potentially cover policies and developments in renewable energy sources. These sources are sensitive to climate extremes, such as heat waves and droughts (Opitz-Stapleton et al., 2021). A hydropower facility's supply of energy might then be particularly vulnerable to climate extremes. Should this facility be part of a TSCN, then a disruption of the energy production in source region could potentially have corresponding disruptive implications for the energy supply for other border regions. Moreover, extreme events including those related to war and natural disasters might damage transportation infrastructure further disrupting the flows along the supply chains (Opitz-Stapleton et al., 2021). Given the increasing rate and destructive capability of natural hazards, a future trend prediction should also account for the climate proofing of the SCNs' key infrastructure, as with the use of flood barriers around buildings, or shock absorbers under buildings to counteract the effect of earthquakes (Opitz-Stapleton et al., 2021).

Similarly, an assessment of trends in price distortions caused by natural hazards for global trade might be relevant. This could include the future implications on livestock and cotton production in Africa due to a greater frequency in droughts. Increased drought frequency may spur cross-border migration of livestock and workforces, intensifying resource competition and potentially exacerbating risks related to regional instability and spread of transboundary diseases in livestock (Opitz-Stapleton et al., 2021). Such degradation of resources might intensify the competition for resources and place additional strain on a supply chains operations and performance. Being aware of relevant trends and having the capacity to anticipate potential future changes would arguable be a beneficial contribution to the situational assessment and overall adaptability of the risk responses.

3.3 Acknowledge

Before a decision about a specific risk response can be made it is first necessary to understand the risk achieved through identification and situational assessments, and then acknowledge the risk. Risk acknowledgement triggers responsive actions: it's about accepting the risk context and drawing the required conclusions to facilitate appropriate actions (Amundrud & Aven, 2015). This acknowledgement is particularly relevant when dealing with global and transboundary

issues which are complex and uncertain environments with ambiguous interactive links. The acknowledgement of risk is achieved once the knowledge about the risk has been recognised (Amundrud & Aven, 2015). This knowledge is obtained through the evaluation and prioritisation phase of the TSCRM process providing insight and awareness to the risks deemed most relevant.

3.3.1 Risk evaluation and prioritisation

The objective of the risk evaluation and prioritisation phase of the TSCRM framework is to provide additional decision-making support based on the previous assessments through the evaluation of the response requirements for the risks and how the responses should be prioritised (de Oliveira et al., 2017). The risk evaluation and prioritisation phase includes two broad aspects: risk acceptance and risk ranking. Through risk acceptance, the acceptability limits of a risk is evaluated. The risk ranking compares the risk exposure and resource requirements for each risk with an established set of risk criteria, whilst also accounting for the risk context. This comparison forms a basis for risk prioritisation. The evaluation and prioritisation phase's focus on risk ranking and acceptance is considered appropriate for the transboundary scope of the present framework when accounting for the challenge of obtaining sufficient data for non-linear and dynamically complex systems, where cause and effect are separated through space and time (see Becker et al., 2014). This is supported by Tummala and Schoenherr (2011) who maintained that risk ranking and acceptance were particularly practical in cases where sufficient data was lacking or objective assessments challenging.

Risk acceptance

Once classified, acceptable risk levels for the identified SCRs should be established. The current framework operates under the assumption that TSCRs are unavoidable, meaning that they cannot be completely eliminated, but rather fall within the organisations limits of (un)acceptability and tolerability. Values for risk exposure, which are determined for each of the risks identified and assessed in the previous sections, can be established via their impact severity and likelihood, and used to determine the risk acceptance level (Tummala & Schoenherr, 2011). However, a standard guideline determining the level of risk an organisation should accept does not exist as acceptability levels are context dependent (Fan & Stevenson, 2017). The acceptability level may, as an example, be associated with an individual's or actor's willingness to take on risks. A method that can be used to determine whether risks are acceptable, unacceptable, or tolerable is the ALARP principle, inferring that risks should be reduced to levels which are as low as reasonably practicable (Aven, 2020). Risks considered to be acceptable may not be critical and/or be considered too small to warrant expending time and resources on implementing risk responses

(Fan & Stevenson, 2017). The accepted risks should be monitored, however, to ensure that the impact severity of the SCR does not escalate, exceeding the initial acceptability threshold (Fan & Stevenson, 2017). If the initial value for risk exposure changes, then a new acceptability evaluation is needed, which in turn may require considerations towards additional risk response actions.

Unacceptable risks, in general, adversely impact operations, potentially resulting in production loss, factory shutdowns, reduced work force, etc., (Tummala & Schoenherr, 2011). An unacceptable risk may potentially be if upstream suppliers are unable to deliver essential components, as seen during the semiconductor shortage of 2020. This shortage caused significant production delays for the automotive and other industries whose products were dependent upon this component (Voas et al., 2001). Risks are not limited to being either acceptable or unacceptable. Tolerable risks are those risk which have a risk exposure value, calculated by multiplying the risk's occurrence likelihood and impact severity, between what is acceptable and unacceptable, and which may not require immediate response implementation. An example of a tolerable risk may be a late delivery that does not result in delays or interruptions of operational flows (Tummala & Schoenherr, 2011). Similar to the acceptable risks, they should be monitored and improvements made if there is sufficient resource availability (Tummala & Schoenherr, 2011). It may prove useful to map the risks based on their acceptability and risk magnitude. This could provide better insight into the different types of SCRs and help in determining which risks require response implementation (see e.g., Tummala & Schoenherr, 2011). By including that risk impacts cannot be fully eliminated, managers are implored to rethink responsive strategies and resource prioritisations. It is, however, recognised that establishing an accurate demarcation guideline for acceptability of risk requires cross-functional teams and the use of all relevant information such that it encompasses different perspectives, knowledge and data (Tummala & Schoenherr, 2011). This process may be both resource demanding and challenging to achieve for complex global systems.

Risk ranking

Risk ranking helps identify the risks which are most significant/critical to the organisation, and supports decision-makers when deciding which risks to respond to (Fan & Stevenson, 2017). The risk ranking is based on resource availability and risk exposure values. An organisation's risk responses are limited by an organisations resource availability. Scarce resources therefore need to be accounted for when evaluating the risks to ensure efficient allocation of the available resources. If an organisation's scarce resources, such as human capital, financial capacity, physical assets, and infrastructure, are not accounted for then the effectiveness of the response

strategies may be lower than intended. This reduced effect may result from the allocation of resources to one risk response having implications for other investments or lead to less resources spent on other already implemented response activities (Abrahamsen et al., 2018). A systems approach for identifying the presence of scarce resources, such as that proposed by Sørskår, Abrahamsen and Abrahamsen (2017), can, for example, be used to provide additional decision support. Key when considering resource usage is, therefore, the evaluation of trade-offs between the resources utilised in the different alternatives being considered and the risks potential impact (Abrahamsen & Asche, 2010).

A risk matrix, using the results of the prior assessments, is an approach used to rank risks (Norrman & Jansson, 2004). The purpose of the risk matrix is to provide a better understanding of the potential impacts of the identified risks. Risk can here be classified through the use of four types of impact severity: insignificant, minor, major, and extreme, and different level of corresponding likelihood. An exemplification of a potential risk matrix is presented in Figure 6. A low risk exposure is attributed those risks with infrequent occurrence and low impact severity, whilst a very high exposure is attributed those risks which are considered almost certain to occur and that have an extreme impact severity, i.e., consequences which are significantly problematic or detrimental to the supply chains operation (Lavastre et al., 2014). Different response actions are then required for different levels of risk exposure (see Figure 6; Norrman & Jansson, 2004).

Figure 6

Evaluation matrix exemplification

Likelihood	Almost assured						**Risk exposure**	**Risk response required**
	Probable						Very high	Response, monitoring, & contingency planning needed.
	Improbable						High	
	Rare						Moderate	Monitor, but response optional.
		Insignificant	Minor	Major	Extreme		Low	No response required. Monitoring advised.
		Impact severity						

Note. Adapted from Norrman and Jansson (2004).

Another alternative for ranking risk is the classification of risk exposure values used to separate risks into similar risk exposure ranges. As an exemplification a risk exposure value range

between 10 and 6 may classify a risk as moderately critical and may include customs delays and temporary labour strikes at production facilities (see Tummala & Schoenherr, 2011). More critical risks could be grouped within the value range of 16 to 11 and include warehouse or facility destruction risks or the risk of stolen/lost shipments. The specific values and ranges used may vary between industries and organisations, some may choose to use exposure values in their classification which are based on a pareto analysis, i.e., an approach where 20 percent of the risk is responsible for 80 percent of the impact/failure (Tummala & Schoenherr, 2011).

Following the evaluation of risk exposure and resource availability, a set of risk criteria are devised. These may include dimensions, such as management capacities, supplier reliability, research and development, transportation timeframe, and costs. These criteria vary between organisations and industries influenced by organisational strategies, industry standards, sector regulations and policies, etc. (Datta, 2017). The comparison of exposure values and resource availability with the criteria is undergone to support and provide further information on which the risk ranking can be based (X. Li & Barnes, 2008; Renn, 2008; Sinha et al., 2004). By viewing criteria alongside exposure values and resource availability, an initial risk's ranking may be altered. Transportation risks may have initially been evaluated as moderate but when compared with a risk criterion for transportation timeframe which limits access to transportation providers capable of delivery within a specified timeframe, the risk may receive a higher ranking due to a greater dependence on a limited number of transporters.

The risk context would presumably also impact the final outcome of the ranking process. Political instability may, as an example, have adverse impacts on human capital and infrastructure resources through consequences, such as hostage taking and destruction of road/transport routes, respectively. Risks related to supplier reliability may initially, based on the comparison of risk criteria with risk exposure and resources, have a low ranking where the context in which the supplier operates is ignored. If the region the supplier is based in becomes unstable, then accounting for the context, as with the supplier's geographical location, could potentially alter the ranking to moderate or high by influencing the level of risk exposure. By taking the context into consideration the preliminary ranking may, therefore, change.

3.4 Adapting

Adapting relates to the inherent ability to learn, adopt novel approaches, be flexible and generalise responses (Steen & Pollock, 2022). Developing adaptive capacities towards risks is required to respond to and manage SCRs (Pournader et al., 2020). Two aspects are important for developing adaptive capacity. The first is the ability to anticipate and predict future scenarios; a

process comprised of organisational orientation within its operating environment (Pournader et al., 2020). The second is the ability to make trade-offs between options; a process dependent upon organisational practices (Provan et al., 2020). Flexibility, the ability to react or change without great consequence to organisational operations or resources, is an important feature of adaptability and a critical requirement for managing complexity (Manuj & Mentzer, 2008a). Being able to effectively adapt response strategies to changing conditions extends the global reach of organisations and improves their responsiveness (Manuj & Mentzer, 2008a). The risk response selection and implementation phases are here attributed to the resilience aspect of adapting. Selection of risk responses requires organisations to think proactively about potential future risks and response requirements, whilst implementation decisions are essentially a trade-off between managing different risks and maintaining performance (Jüttner et al., 2003). The scarcity of resources requires trade-offs to be made between the cost and effect of the required responses. Thorough consideration is therefore required in the selection and implementation consideration of risk responses in TSCRM.

3.4.1 Risk response selection

Risk responses help reduce the severity of supply chain disruptions, and appropriate risk responses need to be selected for each relevant risk (Pournader et al., 2020). Risk response selection entails the evaluation and selection of either singular or multiple response strategies for the purpose of modifying the risks. This is achieved through risk planning i.e., the development of response plans, and the analysis of previous responsive actions and residual risks (de Oliveira et al., 2017). For the selected risk response to be both appropriate and effective it is dependent upon detailed knowledge regarding the specific risk, its causes and impacts (Kern et al., 2012). This means that the selection process is reliant on the understanding obtained from the careful and correct assessment and evaluation of risk being performed in previous phases (see Kern et al., 2012). The risk response selection also requires the costs and resources associated with implementation to be accounted for. Organisations should ensure that the benefits from reducing or eliminating the risks do not exceed the corresponding costs and organisations resource availability (Bandaly et al., 2012). Consideration towards how much the risks should be reduced and at what cost, and how, if relevant, the costs can be shared between network members is therefore relevant (see Sjöstedt, 2001). These cost and resource considerations are covered in the risk planning. Risk planning occurs prior to the final selection and incorporates the evaluation of the different response strategies' requirements and effects.

Risk response plans can be developed once the identification, impact severity and likelihood evaluation of the risks have been performed (Tummala & Schoenherr, 2011). When coping with disruptions or conditions which interrupt normal operations, different responses may prove effective. However, with finite resources and dynamic risk environments it is not practical nor feasible for an organisation to implement response strategies for all the identified risks (Abrahamsen & Asche, 2010). The risk planning starts by examining the resource demand and required costs for each of the response strategies needed to manage the identified SCRs (Tummala & Schoenherr, 2011). Followingly, the risk response plans are evaluated. This evaluation can be performed in different ways. One method is to use a comparison of the relative costs for each response alternative as the basis for the evaluation (Tummala & Schoenherr, 2011). Another technique which may be applied to a supply chain context for systematically evaluating risk responses is the hazard totem pole (HTP) analysis (Tummala & Schoenherr, 2011). Using a combination of the risk's severity, cost, and likelihood, the HTP method can establish ranking categories for the selection process. Three letter codes and numerical values are here formed to denote the various category levels, and a HTP reference index determined. The code and index are subsequently used to visualise the associated severity of impact, likelihood and cost of implementation (Tummala & Schoenherr, 2011). For further information and descriptive models of this evaluation approach the reader is referred to Tummala and Schoenherr (2011).

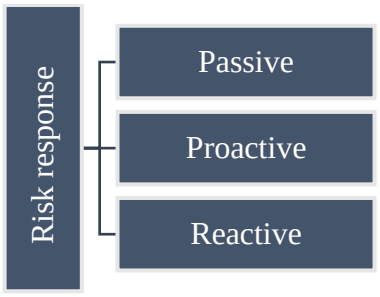
Taxonomy and risk response strategies

To facilitate the risk response selection process, a taxonomy is developed for categorise the different risk response strategies that have been presented in literature. This taxonomy categorises the response strategies into three distinctive approaches: the passive, proactive, and reactive approach (see Figure 7). A passive approach encompasses monitoring and acceptance of risks. The proactive approach is related to the capacity for long-term learning and adapting. It corresponds to two goals of risk response strategies: to reduce or limit the occurrence likelihood and to eliminate or greatly reduce the risk exposure (Bandaly et al., 2012). A reactive approach implies a short-term or instant responsive action for the purpose of recovering from a disruption (Madni & Jackson, 2011). The reactive approach is to a greater extent related to the third goal of risk responses which is to reduce impact. Establishing a structured, common and consistent way to classify risks responses facilitates communication and understanding (Sinha et al., 2004). Such a division also ensures less redundancies when selecting and implementing responses by clarifying the intended effect that the selected response strategies are meant to have (see Sinha et al., 2004). Thus, the distinction between the three risk response approach categories enables the evaluation of different strategies based on their intended purpose.

The SCRs can be reduced or eliminated in different ways, such as by using information technology, effective collaborative relationships between network members, dual or multiple sourcing (i.e., selecting two or multiple suppliers), performance-based contracts, and supplier redundancies (Tummala & Schoenherr, 2011). All of these methods fall within the purview of the various risk response strategies and terms noted in literature (e.g., de Oliveira et al., 2017; Manuj & Mentzer, 2008a). In the following, eight risk response strategies are briefly outlined, and sorted based according to the risk response approach categorisation scheme (see Figure 7). These include postponement, acceptance, control, prevention, avoidance, mitigation, sharing and transfer, and recovery. It is noted that the different response strategies are closely related to one another (Manuj & Mentzer, 2008a). A mitigation strategy may, for instance, be attributed both the proactive and reactive approaches.

Figure 7

Risk response approach categorisation scheme



The postponement of risk is a strategy attributed to the passive approach. Postponement is a flexibility strategy allowing the organisations to adapt to the uncertainties in the operating environment by waiting until the timing is better, as for instances when component costs are lower or a region's political stability improves (Jüttner et al., 2003; Manuj & Mentzer, 2008a). With postponement the actual commitment of resources are delayed in order for the organisation to maintain their flexibility. (Manuj & Mentzer, 2008a). Another strategy attributed the passive approach is acceptance. As previously noted, some risks might be considered too small or not critical enough to warrant expending time and resources on risk responses. In addition, if the risks associated with implementing a risk response are perceived to be high, organisations may be reluctant in committing scarce resources to cope with the given risk (Sjöstedt, 2001). These risks are retained based on well-reasoned/informed decisions (de Oliveira et al., 2017). However, the exposure from these risks may change over time requiring a proactive monitoring strategy.

There are several response strategies that can be attributed to the proactive approach. One such strategy is control. Organisations may respond proactively by seeking to control the

eventualities posed by a given risk. Control strategies may include buffer inventory, stock piling, maintaining excess capacity in storage and transport, and imposing contractual requirements (Jüttner et al., 2003). Such control strategies increase the predictability of contingencies from the different sources of risk (Jüttner et al., 2003). Another proactive strategy is prevention. Preventative actions, requiring the prioritisation of urgent risks before other less urgent risks, are part of what it means to be proactive and involves the ability to prepare(Kern et al., 2012). This in turn reduces the likelihood and risk exposure of a disruptive event and contributes to prompt reactions (Bandaly et al., 2012; Negri et al., 2021). A preventative strategy may, as an example, encompass the use of a diverse supplier base for the purpose of reducing the organisations risk exposure from single supplier dependency (Bandaly et al., 2012). A risk avoidance strategy is similarly proactive in the sense that the root cause of a risk is removed (Fan & Stevenson, 2017). An avoidance response is often selected when the risks associated with a given geographical area, product market, supplier or customer base are considered unacceptable or unreliable (Jüttner et al., 2003). In such instances the managers are aware of the situation and decide to avoid some or all of the risk by not initiating or stopping the activity contributing to the risk (Manuj & Mentzer, 2008a). The avoidance then significantly reduces or eliminates the associated risk exposure (Bandaly et al., 2012). However, avoidance is not always a viable solution for responding to risks. This is due to the uncertainty associated with the occurrence of the risks having unforeseen or unknown likelihoods (Negri et al., 2021).

The risk mitigation strategy may then be a more appropriate proactive approach. Similar to that of avoidance, the mitigation strategy seeks to reduce and, if possible, eliminate, risk exposure, thereby avoiding at least part of the risks (Bandaly et al., 2012). This strategy is usually suitable for those operational risks having low impact and high occurrence likelihood (Fan & Stevenson, 2017). A key part of a mitigation response is the identification of potential losses associated with the disruptive event in order to understand what mitigative actions are needed. Once identified, risk mitigation can be achieved by building different forms of reserve, including responsiveness, supplier redundancies and inventory (Chopra & Sodhi, 2004). Mitigating risks in supply might, for instance, consist of selecting multiple suppliers for the various critical components in order to hedge against risks, such as poor resource quality and insufficient supply quantity (Manuj & Mentzer, 2008a). Hedging as part of mitigation ensures that a single event does not end up simultaneously affecting all members of the SCN with the same level of impact. Hence, mitigation through multiple sourcing contracts reduces risk exposure by spreading the risks (Jüttner et al., 2003).

Risk sharing and transfer strategies are also proactive approaches. These strategies assign the risk to another party or spread all or part of the risk among parties (Fan & Stevenson, 2017). The transfer of SCRs can be achieved through various means including contracting alternatives. Designing and using flexible contracts with underlying clauses, i.e., a contract portfolio, in supply chains can encourage retailers with varying degrees of risk aversion to select specific and unique contracts. This can motivate retailers to increase their order quantity to maximise their expected value by providing them options that allow them to choose between different import quantities (Manuj & Mentzer, 2008a). Contract portfolios then enables the transfer of risk from a manufacturer onto a greater number of retailers. Such flexible contracts account for potential alterations in global conditions and operating environments. They not only transfer the associated risks but also functions as a control mechanism (Manuj & Mentzer, 2008a). When the transfer of risk is not possible, a risk sharing strategy, which involves joint agreements, may prove useful. Interest-based bargaining is such a strategy. Here the parties in a collaborative relationship work to fine a mutually beneficial solution which satisfies the needs of all involved (Vari & Linnerooth-Bayer, 2001). Through such a strategy collaboration is promoted and the relationship between network members maintained. Hence, adopting a risk sharing strategy could lead to more effective collaboration and control of network members (G. Li et al., 2015). The value of promoting collaboration is emphasised by Tummala and Schoenherr (2011) arguing that close collaboration with other network members is one of the most successful methods used for managing SCRs.

Recovery is a strategy attributed the reactive approach. Once a disruption impairing the organisations ability to conduct day-to-day operations has occurred, a recovery strategy can be implemented enabling a hastier return to normal operations (Ho et al., 2015). This is achieved by setting and identifying the main areas, objectives and activities involved in the recovery process, and developing a recovery plan including the specific ways and techniques for dealing with presenting issues. Another reactive approach is mitigation. A mitigation strategy may in certain circumstances be a reactive strategy when used to reduce the risk exposure resulting from an unexpected ongoing event. Mitigation used proactively prepares organisations for disruptions, but we cannot prepare for all risks associated with unknown and unexpected events, as seen during the Covid-19 pandemic. In such instances new or changed risk exposures would require mitigative responses in line with the current events, i.e., a reactive approach.

TSCRM selection process

There are few guidelines in literature for selecting appropriate risk response strategies (Manuj & Mentzer, 2008a). This makes it challenging to create a general approach appropriate for setting

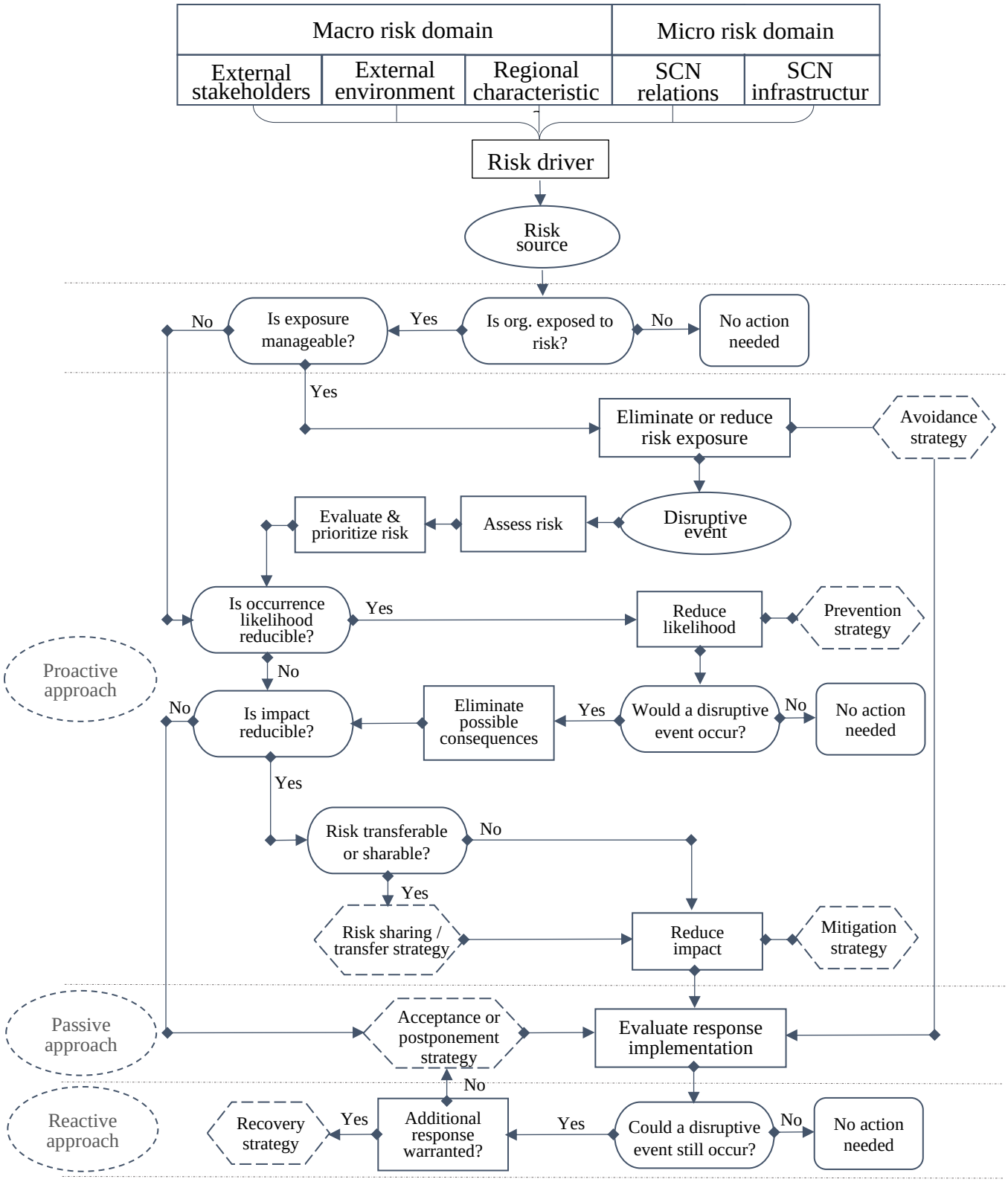
comprehensive risk responses. Therefore, using the identification and risk response taxonomies presented in this thesis, and building on the planning process devised by Bandaly et al. (2012), a TSCRM selection process is proposed and presented in Figure 8 to facilitate the appropriate selection of risk responses. Through the application of this process managers are guided through a simulation-like set of logical steps that enable them to devise a comprehensive strategy for managing the SCRs. For each the identified risks emanating from one of the five TSCN risk domains a systematic process is used with different stages leading to a given response approach.

The process starts with an evaluation of the level of risk exposure resulting from a specific risk source which leads to a disruptive event. The manageable risk exposure follows a process leading to proactive response strategies. For risk exposure which cannot be managed or considered too demanding to manage, an additional evaluation is taken for whether the likelihood of occurrence can be reduced. A passive approach is then taken if neither the exposure nor the occurrence likelihood can be managed. Each response strategy is placed in the process model at the position which is in line with the timing the given response strategy should be implemented. If a residual risk, which may lead to a disruption, is present following response implementations, then additional action might be warranted. The estimated costs for an additional response strategy would be compared with the estimated costs associated with the risks impact on the organisation, i.e., evaluate whether the risk exposer level is acceptable or not. A recover strategy is implemented as part of a reactive approach when the residual risk is considered unacceptable. This selection process must be re-evaluated following the implementation of the different strategies due to the changes, both long-term and short-term for the organisation.

Alongside the TSCRM selection process an evaluation and response prioritisation template is proposed as a means to facilitate the risk planning associated with the risk response selection process. The template presented in Table 2 aims to provide a structured support for evaluating the selected response and give a simple indication of how the different responses align with the overall supply chain strategy and standard industry practices. This evaluation and response prioritisation template may also be useful within other areas of the TSCRM process as it incorporates information from the previous TSCRM phases. Firstly, it may facilitate monitoring activities following implementation of risk response by providing information about what considerations the implementation decision was based on. By knowing what went into a decision, it may be easier to evaluate the resulting outcome. Secondly, it may be used as an additional data source in the feedback processing to improve understanding of the final possessing results.

Figure 8

TSCRM selection process



Note. Adapted from Bandaly et al. (2012).

Table 2

Template for assessment evaluation and response prioritisation

	Evaluation and response prioritisation template				
	Risk domain:				
	Risk source:				Id No:
	Date:				
Disruptive event	*Event description*				
	Cause				
	Network location				
Risk estimation	*Resource requirements*				
	Impact likelihood				
	Impact severity				
Standard industry/sector risk management practice					
Response strategies	*Ranking*	*Description*	*Response category*	*Cost*	*Proposed effect on exposure*
	1				
	2				
	3				
	4				
	5				
Impact on society and stakeholders	*Response strategy*	*Equity problem*			
Responsible agent:					
Evaluation status:					
Updated:					

Note. Adapted from Norrman and Jansson (2004).

For each disruptive event within a TSCN risk domain, an area is provided in the template in Table 2 where a description of the event, its causes and location within the network can be noted. The resource requirements, impact likelihood and impact severity results from the risk assessment and evaluation are incorporated into the table under the header of “risk estimation”.

Followingly, a section is attributed the standard SCRM practices within a specific industry/sector. Industry/sector practices can result in valuable inputs or impose constraints on the risk management process (Manuj & Mentzer, 2008a). It can therefore be useful to recognise the presence of industry specific mindsets. Explicit consideration to these practices provides additional insight into the organisations decision-making process by encouraging broader thinking beyond the current scope of standard approaches. This may then motivate additional consideration towards other approaches which have less industry/sector experience or that otherwise would be ignored (Manuj & Mentzer, 2008a). The next section of the template notes the different risk responses that have been selected in the "description" column, ranking them according to their anticipated effect. The risk response approach categorisations (passive, reactive or responsive) are then noted to highlight the broader aim of each response. Similarly, the costs and the presumed effect that the selected response will have on the overall risk exposure are mapped out enabling a simple overview of cost and effect comparisons.

Before implementing a response, consideration should be taken towards the potential harm on the SCN, local societies, stakeholders, and other potentially affected parties resulting from the organisations response activities. Equity problems are therefore included. Equity here refers to the fairness associated with the process by which a given policy or decision is enacted, and the outcomes associated with it (Kasperson & Kasperson, 2001). Through the inclusion of equity problems Kasperson and Kasperson (2001) propose that inferences and understanding about the obligations and responsibilities toward those adversely affected and how to meet these responsibilities are gained. The goal of the proposed template is not to apply it towards every identified risk, as this would be both impractical and resource demanding for organisations. Rather, the template is applied to those risks identified during the evaluation and prioritisation phase as most relevant or in need of consideration.

For easy overview, comparison, and control of the actions taken by the organisation it may be practical to aggregate key information from the templates into an overview table. Such a table may, for instance, include the most and least critical risks identified by the risk evaluation process, industry specific risk management practices, proposed risk response, its cost, proposed effect, and the equity problem considered to most likely to impact the successful implementation of the intended risk response. Least critical risks are included to provide an indication of minor risks that may be reduced or eliminated from the responsive actions taken to deal with the most critical risks. It also ensures the awareness of risks which are relatively less consequential (Manuj & Mentzer, 2008a). Table 3 provides a simple exemplification of the suggested overview table.

Table 3

Simple overview table to support response selection

	Type of disruption	*Risk management practices in industry*	*Risk response strategy*	*Cost*	*Proposed effect*	*Most critical equity problem*
Most critical						
Least critical						

3.4.2 Implementation of appropriate risk response strategies

Implementing response strategies requires commitment and discipline as the effect of the selected risk response may vary depending on the extent to which it is implemented (Bandaly et al., 2012). Changes in structures and/or procedures are often needed which harmonise with the trends in global environments (Manuj & Mentzer, 2008a). Managers have to consider numerous risks and strategies in their TSCRM prior to implementation, and then understand how the general approaches for risk response should be adapted to the specific circumstances of the organisation during implementation (Chopra & Sodhi, 2004). The transboundary nature of SCRs subject the different network members to varying degrees of exposure from a diverse range of risk types (Knemeyer et al., 2009). This can make it challenging to understand the effect of different implementation approaches on the SCN and how they should be adapted. The use of cross-functional teams may then be useful. Cross-functional teams consist of individuals with a wide range of expertise from various areas of the SCN. This enables them to better foresee potential implementation issues (Knemeyer et al., 2009). However, obtaining the required expertise is not always straightforward and may not be readily available. In such cases the expertise ends up residing with a third-party, for example when operations are outsourced (Knemeyer et al., 2009).

Implementation of risk responses in TSC requires consideration towards the complexity of SCNs. The dynamic international economic, legal and political environment, along with conflicting objectives within the buyer-supplier relationships and issues with power and control, add to the complexity of TSCs (Pournader et al., 2020). Organisations constantly expand, consolidate or test different configurations of up-and downstream network members as a means to manage the complexity inherent in their operating environment (Manuj & Mentzer, 2008a). These changes can then influence the effect of implemented risk responses, which in turn adds

to the organisations complexity. The implementation of certain risk responses without consideration towards how it affects complexity may increase the overall SCN system complexity and exacerbate the risk exposure by affecting the interactivity and tight coupling of the network system (Bandaly et al., 2012). Managing the complexity is, therefore, a relevant aspect for the implementation of risk responses given that it can result in sub-optimal interactions between network members and systems (Manuj & Mentzer, 2008a). In addition to the use of cross-functional teams and considerations towards complexity, the risk response implementation phase of the TSCRM framework involves contingency planning. Contingency planning can be applied as a means to facilitate understanding of response limitations enabling the organisation to map out contingency measures and, through this, recover more effectively by efficiently implementing new responses.

Contingency planning

Contingency planning encompasses the plans and actions needed after a disruptive event has occurred which then enables the organisation to achieve a steady state. If the consequences of a risk cannot be avoided, mitigated or responded to in another manner, a contingency plan can be created to provide an understanding of what to do if something occurs (Norrman & Jansson, 2004). It is important to plan for the eventuality that a risk may be realised regardless of the initial response implemented (Manuj & Mentzer, 2008a). After resources have been spent on initial risk responses there may still be residual risks, albeit with lower impact severity. The risks might then emerge in a modified form making the original risk response strategy less effective than initially presumed (Tummala & Schoenherr, 2011). Therefore, as part of contingency planning, contingency measures are used to note alternative strategies. Mapping out contingency measures is an important part of successful and adaptive response implementation and provides awareness towards global situations and critical links in the SCN. Contingency measures cover the eventuality of implementation failures and what should be done in an event where, for example, a joint response agreement is not honoured by all parties involved, i.e., their obligations are not honoured as a result of compliance failures (Sjöstedt, 2001). This way more than one solution is accounted for thereby acknowledging the uncertainty and scale of the potential risks (Thompson & Gyawali, 2001).

Certain contingency measures, as with moving a production facility, may address all corresponding risks, whilst others, such as infrastructure reinforcement, may only address a couple or one risk(s) (Thompson & Gyawali, 2001). Two approaches for selecting contingency measures are, building redundancies and/or adding flexibility into the supply chain thereby implementing a layered approach to the management of SCRs (Knemeyer et al., 2009). Adding

redundancies, although it increases the costs associated with risk responses, may involve the use of buffer inventory, investment in key locations to offset consequences of disruptions, infrastructure reinforcement (e.g., constructing a protective wall to reduce exposure to flooding), and dual sourcing (Knemeyer et al., 2009). Adding flexibility, as an approach for selecting contingency measures, may present a competitive advantage by building the organisations ability to respond quickly to unfolding events. Such flexibility may include alternate transportation routes, reduced dependence on key areas by redesigning the supply chain, and business interruption insurance (Knemeyer et al., 2009). However, the approach for selecting contingency measure may change along with changes in organisational commitment, the risk context, evaluation assumption, etc.

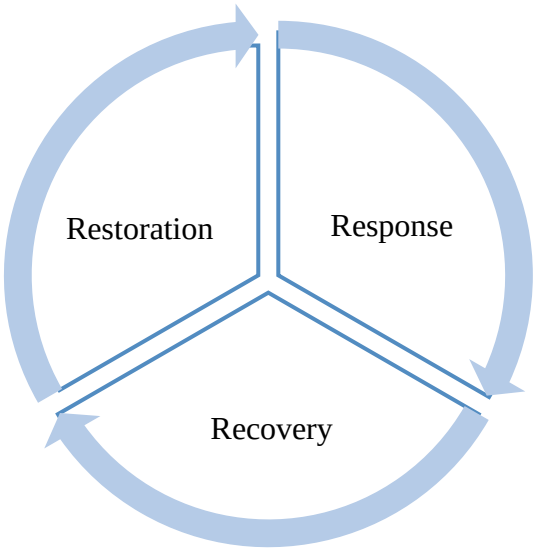
Through contingency planning the subjectivity and assumptions made in the prior evaluation of selected responses are noted (Tummala & Schoenherr, 2011). These assumptions are not necessarily valid in the future. Committing fully to one response solution can therefore be problematic, locking the organisation in its current path making it inflexible and less adept at managing complexity (Thompson & Gyawali, 2001). Without contingency plans, and the awareness gained from them, organisations and the SCN may become exposed to prolonged disruptions potentially resulting in halted production. The Russia-Ukraine conflict exemplifies how essential contingency planning can be. Complex logistical challenges has followed as a result of these recent global events, some of which include container shortages, restricted air space over Russia and the Ukraine, causing air-freight lanes and availability to change and record spikes in freight rates, rising oil prices, and longer lead times (Kilpatrick, 2022). This conflict has thereby disrupted traditional supply routes and SCNs. However, the use of contingency plans allowed some organisations within the semiconductor industry to increase their critical resource stockpiles from Russian supply sources prior to the Russia-Ukraine conflict thereby mitigating the risks associated with sourcing dependencies (Kilpatrick, 2022). Contingency planning can, therefore, be an important feature for ensuring adaptability required for global operationality.

In the endeavour to make contingency planning for TSCRM more salient, this thesis introduces a contingency planning process consisting of three successive phases: response, recovery, and restoration (see Figure 9), and a contingency planning template (see Table 4). The response phase addresses the organisations required reactions to a situation in order to control the activity or its outcome. Different scenarios are discussed and response plans developed for those deemed most hazardous (Manuj & Mentzer, 2008a). Depending on the SCN in question, a response plan may also address overall inventory policy thereby motivating the organisation to establish a strategic stock policy for critical materials (Kilpatrick, 2022). The recovery phase

covers the actions needed to resume the business operations, processes and functions which are critical or essential to the organisation (Norrman & Jansson, 2004). It may, for instance, be relevant to identify back-up services or providers such that the organisation can handle potential delivery disruptions, or to establish additional transportation plans that can be used if primary transport routes are disrupted (Kilpatrick, 2022). Additional providers with the capacity to handle the given transport needs on short notice can be quickly activated prior to the disruption making the organisation more adaptable (Manuj & Mentzer, 2008a). Lastly, the restoration phase involves the planning and implementation process for accomplishing full-scale operations and return to normal service levels (Norrman & Jansson, 2004). As a successive process, the activities performed during the response and recovery phases contribute to the restoration of normal operational activity. If overseas transport only occurs through shipping, then having a plan in place for the use of air freight would, arguably, be advantageous for the organisations ability to recover from disruptions, secure critical capacity and restore normal operations should shipping lanes become compromised.

Figure 9

Phases in the contingency planning process



The contingency planning template in Table 4 exemplifies a simple method for identifying and describing actions taken within each of the three phases for a specific risk source within a TSCN risk domain. Similar to Table 2, the contingency planning template includes the cost requirements, proposed effect the measures have on the risk exposure and the potential equity problems. As with the initial response selection process, the cost requirement and proposed effect on risk exposure are used to evaluate whether the contingency measure should be considered. If

the costs exceed the effect, i.e., risk reduction/elimination, the contingency measure has on the risk exposure, it should be excluded (Knemeyer et al., 2009). In addition to these elements, three additional aspects are introduced: contingency measures, resource availability and impact on the risk's occurrence likelihood.

Table 4

Template for contingency planning

	Contingency planning template					
	Risk domain:					
	Risk source:				Id No.	
	Date:					
	Responsible agent:					
	Resource availability					
Contingency plan selection		*Contingency measure*	*Impact on society and stakeholders (Equity problem)*	*Cost*	*Proposed effect on exposure*	*Impact on the risk's occurrence likelihood*
	Response					
	Recovery					
	Restoration					
Status:						
Updated:						

Note. Adapted from Norrman and Jansson (2004).

In Table 4 the different contingency measures which may be applied within each of the three phases: response, recovery and restoration, are noted to indicate the intended purpose of the specific contingency measure. The impact on occurrence likelihood is introduced to present the effect each contingency measure is expected to have on the likelihood of the disruptive event occurring following its implementation (Knemeyer et al., 2009). The organisation's resource

availability will influence what contingency measures are implemented and the extent of their implementation (Fan & Stevenson, 2017). Understanding where the best place is to deploy an organisation's scarce resources and when outdated or ineffective strategies should be changed, is important to ensure that the implemented response strategies align with the evolving SCR environment (Fan & Stevenson, 2017). The contingency planning template therefore also covers resource availability. Once the contingency planning is completed, the proposed template may function as a decision support tool and used for the purpose of monitoring and following-up the success of the implementation activity.

3.5 Learning

Organisational learning occurs when continuous dialog and inquiry is promoted along with seeking feedback, the transfer of knowledge and skills, errors analysis, and communication (Manuj & Mentzer, 2008a). Learning is particularly important for TSCs; where operating environments are constantly changing resulting in a steady stream of new and unexpected conditions and situations, respectively (see e.g., Hollnagel, 2014a). Learning requires that the gaps in understanding are addressed to further develop the insight and knowledge needed to meet future challenges (Steen & Pollock, 2022), thereby enhancing the anticipatory and adaptive capabilities of network members. To address the gaps in understanding and be able to learn, information and experiences are required. This can be obtained through continuous monitoring and review of organisational activities. Hollnagel (2014a) maintained that a primary function of monitoring is its contribution to improved response capabilities, which in turn provides experiences that are needed to improve learning.

Having a capacity to learn makes it easier to recognise what combinations of events or situations generate vulnerabilities and risks (Rankin et al., 2014). In addition, it keeps the supply chain prepared for and/or out of danger when disruptive events impact complex supply chains (Datta, 2017). Learning is not just achieved by assessing past failures but is also achieved by understanding how similar situations were handled successfully in the past. This can then be used improve response precision, time, and the cues and indicators being monitored (Hollnagel, 2014a). Successful responses, adaption that failed, and failing to adapt all provide key information on the complexities of a transboundary global environment (Rankin et al., 2014). Learning from both successful and failed responses and management approaches is, therefore, vital for understanding situational contexts and to acknowledge what requirements are needed to successfully achieve effective and appropriate adaptations (Steen & Pollock, 2022).

3.5.1 Continuous monitoring and review

Having a resilient approach to TSCRM entails a need for continuous adjustments to changing conditions and following up situations, improvements, and action plans (Madni & Jackson, 2011). Continuous monitoring is a tool that can be used to assure that the implemented response strategies are effective and efficient. The constraint of limited resources means that all eventualities cannot be prepared for, and situations will occur where the organisation will not know how to respond. In such instances it is critical to learn and to assess whether these instances are unique or likely to reoccur, using this to improve future responses (Hollnagel, 2014a). The purpose of continuous monitoring is to detect changes in internal and external environments, risk criteria and risk exposure, learn from previous errors and successes, and gain insight into the SCN's ability to adapt to these changes and what their limits are (de Oliveira et al., 2017; Hollnagel et al., 2006). These activities enable organisations to obtain additional new information about emerging risks and types of disturbances existing within the given SCN's operating environment. This supports the risk identification phase as it contributes to a better recognition of new risks and unusual or suspicious situations/factors (Kern et al., 2012).

Monitoring is required not only in the present but also in the short- and long-term because the modifications made to systems and SCN structures in order to cope with current situations may have unanticipated future implications (Rankin et al., 2014). A U.S. based organisations decisions to mitigate financial risks by outsourcing manufacturing to China would initially alter the SCN structure. This alternation would then, presumably, have unanticipated implications for the organisation following the U.S. ban on Chinese products. Immediate monitoring requires observation of real-time performance to assess the strategy effect and make required adjustments (Rankin et al., 2014). Short-term monitoring is used to identify and report potential adaptations in need of further investigation, whilst long-term monitoring covers pattern and impact identifications and relies on the short-term monitoring to provide relevant data (Rankin et al., 2014). Long-term monitoring allows for the identification of trends and their impacts over time which can guide assessments and predictions of how future changes and circumstances may affect the SCN and individual network members (Rankin et al., 2014). The TSCRM process must, therefore, be reiterated, revised, and updated continually both in the short- and long-term to account and accommodate for changes in the organisations' global operating environment (see Tummala & Schoenherr, 2011).

The review of organisational activities can be undertaken using feedback from current implementation actions and critical aspects in the extended SCN (Kern et al., 2012). By reviewing feedback, relevant information and knowledge can be obtained which may facilitate

learning (Komatsubara, 2014). This information and knowledge can then be used in a new situational assessment to evaluate new implementation requirements (Rankin et al., 2014). Feedback on progress and consequences enables judgements of whether progress is being made or if adjustments are needed (Klein, 2009). Based on the review of organisational activities, corrections can be made in prior responses and new assessments made on what additional actions should or could be taken (Rankin et al., 2014). The review of current activities and feedback contributes to enhanced monitoring and provides greater access to data which is important for strengthening responses (Opitz-Stapleton et al., 2021). The continuous monitoring and review of the TSCRM process makes it easier to elucidate potential areas for improvement and enable responsibilities of involved parties to be more clearly defined. Based on feedback and what is learned, the continuous monitoring and review phase provides decisional support. It assess and evaluates trends, controls the risk, analyses the effectiveness and utility of current responses, and makes adjustments, if needed, within different stages of the TSCRM process (see Kern et al., 2012; Tummala & Schoenherr, 2011).

4 Discussion

This thesis used a conceptual approach in the development of an integrative framework for managing transboundary risks in a supply chain context. The work in this thesis addressed the transboundary risk aspect which currently has received modest literary focus within SCRM. In addition, this paper has emphasised the limited literature on TSCRM and sought to extend it by conceptually developing an anticipatory and adaptive framework for managing TSCRs. Using current knowledge on SCRM, TRM and resilience theory as a basis for the developed framework, the present paper is able to highlight key features needed for effectively operating within a transboundary environment. Furthermore, information sharing, communication, risk perceptions and trust are viewed as important aspects of the TSCRM process which are highly dependent on collaborative relationships.

Based on current findings, traditional methods for managing SCRs are presumed to be less applicable for anticipating, adapting, and responding to transboundary risk events (see Manuj & Mentzer, 2008b). Having an anticipatory and adaptive process is required for dealing with risks in TSCs. These risks might initially be constrained within national borders but over time spread to other geographical domains (Boin et al., 2017; Svedin, 2001). The spread of transboundary risks between different areas substantiates inclusion of the five TSCN risk domains presented in the TSCRM framework (see Figure 1). Although not exhaustive, the suggested risk domains account for a broad range of potential risk drivers and sources. However, it should be noted that several political, social, and cultural issues and perspectives are involved in a TSC perspective (Kasperson & Kasperson, 2001). This emphasises the importance of consolidating TRM and SCRM into a single framework which can account for the variations in these issues and perspectives.

The consolidation of TRM and SCRM has further merit when accounting for the increased interdependencies of social and global networks and international operations by modern organisations (see Manuj & Mentzer, 2008a). To accommodate for the complexities inherent in TSCs, a generic presentation was used to construct the individual framework phases. This generic presentation enables the TSCRM process to be modified to the specific requirements of different industries. The different contexts and needs of organisations make developing risk management procedures for TSCs, which satisfies all requirements for all organisations, unachievable (see de Oliveira et al., 2017). Providing a generic flexible framework is, therefore, important. Moreover, utilising the TSCRM framework's adaptive phases as a guide, the changes in TSCN structures and implications of these changes can be addressed, suggesting that context can influence the

TSCRM outcome. This is congruent with Ritchie and Brindley (2007a) who proposed that the context in which risk management frameworks are applied is central to the value they provide.

This paper addresses the need for holistic work on SCRM as highlighted by Fan and Stevenson (2017). Taking a holistic approach, arguably, enables special focus to the complex, non-linear and diffuse TSCR causes and interactions by accounting for these aspects within each phase of the TSCRM framework. The TSCR influence could then be described at the various phases of the TSCRM process improving organisations' ability to prepare through greater awareness of transboundary issues and developments. Each of the TSCRM phases are closely linked and dependent upon the accurate completion of prior phases for successful TSCRM. In the present framework, situational awareness and monitoring are required for precise risk identification which in turn is needed for the effective assessment and evaluations that the selection of risk responses depend upon. Monitoring both the risk response implementation and the situational context they are applied to is then needed in order to ensure that the selected responses function as intended. This continuous feature highlights the integrative nature of the present framework supporting the notion presented by Kern et al. (2012), that the management of SCRs should be an ongoing process requiring constant adaptations and integration of lessons learned.

4.1 Theoretical implications

The primary theoretical contribution of this thesis is the development of the TSCRM taxonomy and conceptual framework to adaptively manage and anticipate TSCRs. Both SCRM and TRM researchers have acknowledged the need for additional focus on transboundary risks and the importance of having a global risk management perspective (see Kasperson & Kasperson, 2001; G. Li et al., 2015; Manuj & Mentzer, 2008a). The inclusion of new elements that enable the TSCRM process to account for global cross-border aspects provides added knowledge and awareness towards the transboundary context of TSCs. The emphasis on TRM expands the applications of TRM terminology towards SCRM and seeks to enrich the SCRM field. Additionally, theory on resilience is included in the proposed TSCRM framework to establish a framework more adept at recognising and managing the complexities of transboundary risks. The recognition towards greater complexity and interconnectivity of globalisation and reliance on TSCs substantiates the relevance of transboundary and resilience developments to SCRM practices. Hence, this thesis also extends the application of resilience theory within SCRM beyond the perspectives provided in existing research.

The causes of transboundary risks are complex and encompass a broad range of drivers, sources, and events underlying the five proposed TSCN risk domains of external stakeholders,

external environment, regional characteristics, SCN relations, and SCN infrastructure. As such, the taxonomy for risk identification is extended by introducing the two-step classification approach. This approach is believed to be unique and more comprehensive due to its holistic nature, considering both external and internal TSCN risk domains, accounting for different types of risk driver, sources, and corresponding risk events in a broader perspective than that proposed by previous studies. Moreover, the situational assessment encompasses the additional dimensions of global scenario planning and future trend predictions extending the assessment process beyond the scope of traditional risk assessment elements.

A final theoretical contribution is attributed to the implication of the dynamics and importance of appropriate collaborative relationships to SCRM. It establishes the necessities of accounting for interaction effects both with external stakeholders as well as with other SCN members when selecting and implementing risk responses. A constant flow of interactions, knowledge, and information persists between the different phases and are influenced by indirect and direct effects from the SCNs environment. It should therefore be recognised that all the proposed phases of this framework are interdependent and interactive. Lastly, although it is acknowledged that implementing such a dynamic approach to TSCRM would be both challenging and resource intensive for organisations, it attributes attention towards the importance of establishing collaborative SCNs and having a risk perspective that accepts risks as inevitable.

4.2 Practical implications

Through the development of a TSCRM framework, this thesis' practical implications are three-fold. Firstly, it offers an integrative framework for TSCRM decision-making processes with additional support from templates, tables, models, and classification and categorisation schemes aiming to assist management in their approach to TSCRM. The proposed templates and tables serve as additional tools for management and can be adapted in accordance with organisational and industry requirements. It thereby provides a practical guide adaptable to the specific circumstances to which it is applied, by serving as a decisional support tool that can accommodate the unique situations, judgements and the tacit knowledge that are part of the decision context. The application of the present framework may, therefore, provide management with a flexible approach with which risks in TSCs can be managed.

Secondly, the proposed approach encourages managers to move beyond the present boundaries of their mental models, and typical risk management and intuitive thinking. The present framework provides an understanding of five complex and dynamic TSCN risk domains through the situational awareness phase. In addition, the development of a two-step risk

classification approach may enable the creation of a more comprehensive risk profile and a detailed risk identification is then accomplished. The framework may thereby provide managers with greater understanding of the risk elements. Furthermore, the selection and implementation of risk responses appropriate to the TSCR context may be facilitated through the TSCRM selection process and accompanying evaluation and prioritisation template. The framework thereby presents managers with practical tools which, alongside the risk response categorisation scheme, enable the consideration of response strategies within a broader SCN frame, aid their understanding of the responses' intended purpose, and may further promote awareness towards the responses' external impacts through the inclusion of equity problems.

Thirdly, the TSCRM process may promote additional strategic and innovative thinking. Through the use of contingency planning, considerations towards and the inclusion of alternative courses of action may contribute to broaden managers situational awareness and understanding of consequences and interactive effects. As such, the TSCRM framework provides a practical base for making comprehensive and appropriate decisions by encouraging the management to consider multiple strategies, outcomes, and solutions across the extended SCN when making TSCRM decisions. Additionally, the resilience focus of the TSCRM framework could provide a structured guide promoting additional strategic and innovative considerations towards the organisational requirements for resilient operations, i.e., their ability to adapt and cope to diffuse external disruptions. Thus, it could facilitate the adoption, fine-tuning, and exploration of new/additional response strategies within a transboundary risk domain by supply chain managers.

5 Conclusion

This thesis explored the nature of transboundary risks in the supply chain context addressing the need for greater attention on management of TSCRs by introducing the TSCRM taxonomy and corresponding framework. Incorporating the resilience principles of anticipation, acknowledgement, adapting, and learning, along with guiding templates and tables, the TSCRM framework modifies traditional risk management ideas to accommodate for the anticipatory and adaptive management needs of TSCNs. Both internal and external risk domains, drivers and sources were identified, assessed, and evaluated in this framework, encompassing network members at different stages of the SCN. Through this and the attention given to collaborative relationships, the framework emphasises the importance of network related interactions and considerations towards network related risks. The SCRM is then expanded from the organisations' own areas to its suppliers and sub-suppliers. Furthermore, the seven phases of the TSCRM framework are introduced as a continuous process, accommodating for the constantly changing operating environment of TSCNs. Viewing TSCRM as a continuous process ensures long-term strategic thinking and greater awareness to vulnerabilities and changing risk exposures during the selection and evaluation of risk response strategies along with contingency measures.

5.1 Limitations and Future research

The TSCRM framework and its articulation within the present thesis are subject to limitations which may aid in directing and structuring future research. Using a conceptual methodological approach to develop a generic TSCRM framework limits the potential for assessing its practical application within different industries, sectors and regions. A study on the flexibility and adaptability of this framework in practice could therefore present an avenue for future research. The framework may then be applied to different industries, such as automotive and agriculture, public and private sectors, and across different regions, to provide insights into specific biases, requirements, and prioritisations which may influence their risk management approaches. Moreover, the general focus of proposed frameworks has been directed towards supply chain flows of a physical character, i.e., product supply chains. It may therefore be interesting to examine the TSCRM frameworks applicability for service supply chains in particular, such as banks. Thus, additional qualitative and quantitative research should be used to validate the framework developed in this thesis.

Though the present framework acknowledges the relevancy of managers' risk perceptions, it is not empirically addressed. I therefore encourage new research to extend the scope of the

present paper through qualitative study. A suggested direction for such qualitative studies is semi-structured interviews with managers from different stages in the SCN aimed at examining the effectiveness and applicability of the TSCRM framework from the perspective of different network members. Through this methodological approach the influence of the managers' risk perceptions and degree of focus given by managers in different geographical regions to specific transboundary risks may be examined in detail. Moreover, how transboundary risks are accounted for at different levels of the supply chain may then be expanded upon. Furthermore, while this thesis addresses the complexities of modern globalised operating environments, the effect of modernisation and globalisation complexities on the management of TSCRs has not been examined. Assuming that new risks may become more prevalent in line with the growing complexity of modern societies, a study examining these effects could provide insight into new developments and innovative ways for managing TSCRs. By using the developed TSCRM framework as a base, a firm starting point for additional empirical research within this area is offered. New research is encouraged to improve upon the contribution of this thesis by testing the framework within different contexts using varied methodological approaches.

References

Abrahamsen, E. B., & Asche, F. (2010). The insurance market's influence on investments in safety measures. *Safety Science*, *48*(10), 1279–1285.

Abrahamsen, E. B., Moharamzadeh, A., Abrahamsen, H. B., Asche, F., Heide, B., & Milazzo, M. F. (2018). Are too many safety measures crowding each other out? *Reliab. Eng. Syst. Saf.*, *174*, 108–113.

Amundrud, O., & Aven, T. (2015). On how to understand and acknowledge risk. *Reliability Engineering and System Safety*, *142*, 42–47. https://doi.org/10.1016/j.ress.2015.04.021

Aven, T. (2015a). *Risk Analysis* (2nd ed.). John Wiley & Sons, Ltd.

Aven, T. (2015b). What is Risk? In *Risk Analysis* (Second Edi). Chichester, West Sussex, United Kingdom: John Wiley & Sons, Ltd.

Aven, T. (2020). The Science of Risk Analysis: Foundation and Practice. In *The Science of Risk Analysis*. https://doi.org/10.4324/9780429029189

Bak, O., Shaw, S., Colicchia, C., & Kumar, V. (2020). A Systematic Literature Review of Supply Chain Resilience in Small-Medium Enterprises (SMEs): A Call for Further Research. *IEEE Transactions on Engineering Management*, 1–14. https://doi.org/10.1109/TEM.2020.3016988

Bandaly, D., Satir, A., Kahyaoglu, Y., & Shanker, L. (2012). Supply chain risk management I: Conceptualization, framework and planning process. *Risk Management*, *14*(4), 249–271. https://doi.org/10.1057/rm.2012.7

Barnett, M., & Salomon, M. (2006). Beyond dichotomy: The curvilinear relationship between social responsibility and financial performance. *Strategic Management Journal*, *27*(11), 1101–1122.

Becker, P., Abrahamsson, M., & Tehler, H. (2014). An emergent means to assurgent ends: Social resilience for safety and sustainability. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 1–12). Boca Raton, FL: CRC Press.

Becton, L., Davis, P., Sundberg, P., & Wilkinson, L. (2022). Feed safety collaborations: Experiences, progress and challenges. *Transboundary and Emerging Diseases*, *69*(1), 182–188. https://doi.org/10.1111/tbed.14297

Bergström, J., Henriqson, E., & Dahlström, N. (2014). Some thoughts on how to align the theoretical understanding of team performance with resilience engineering theory. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 127–137). Boca Raton, FL: CRC Press.

Blondin, D., & Boin, A. (2020). Cooperation in the face of transboundary crisis: A framework for analysis. *Perspectives on Public Management and Governance*, *3*(3), 197–209. https://doi.org/10.1093/ppmgov/gvz031

Boin, A., t' Hart, P., Stern, E., & Sundelius, B. (2017). *The politics of crisis management* (2nd ed.). Cambridge University Press.

Booth, L., Fleming, K., Abad, J., Schueller, L. A., Leone, M., Scolobig, A., & Baills, A. (2020). Simulating synergies between climate change adaptation and disaster risk

reduction stakeholders to improve management of transboundary disasters in Europe. *International Journal of Disaster Risk Reduction*, *49*, 101668. https://doi.org/10.1016/j.ijdrr.2020.101668

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.

Chopra, S., & Sodhi, M. S. (2004). Managing risk to avoid supply chain breakdown. *MIT Sloan Management Review*, *46*(1), 53–62.

Chu, W. H. J., & Lee, C. C. (2006). Strategic information sharing in a supply chain. *European Journal of Operational Research*, *174*(3), 1567–1579.

Colicchia, C., & Strozzi, F. (2012). Supply chain risk management: A new methodology for a systematic literature review. *Supply Chain Management*, *17*(4), 403–418. https://doi.org/10.1108/13598541211246558

Cormier, D., Ledoux, M. J., & Magnan, M. (2011). The informational contribution of social and environmental disclosures for investors. *Management Decision*, *49*(8), 1276–1304. https://doi.org/10.1108/00251741111163124

Craighead, C. W., Blackhurst, J., Rungtusanatham, M. J., & Handfield, R. B. (2007). The severity of supply chain disruptions: design characteristics and mitigation capabilities. *Decision Sciences*, *38*(1), 131–156.

Datatilsynet. (2022). Datalekkasje hos Norkart. Retrieved June 8, 2022, from https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2022/datalekkasje-hos-norkart/

Datta, P. (2017). Supply network resilience: A systematic literature review and future research. *International Journal of Logistics Management*, *28*(4), 1387–1424. https://doi.org/10.1108/IJLM-03-2016-0064

de Oliveira, U. R., Marins, F. A. S., Rocha, H. M., & Salomon, V. A. P. (2017). The ISO 31000 standard in supply chain risk management. *Journal of Cleaner Production*, *151*, 616–633. https://doi.org/10.1016/j.jclepro.2017.03.054

Dee, S., Neill, C., Singrey, A., Clement, T., Cochrane, R., Jones, C., … Nelson, E. (2016). Modeling the transboundary risk of feed ingredients contaminated with porcine epidemic diarrhea virus. *BMC Veterinary Research*, *12*(1), 1–12. https://doi.org/10.1186/s12917-016-0674-z

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of Management Review*, *20*(1), 65–91.

Douglas, M. (1992). Risk and blame. In *Essays in Cultural Theory*. London, UK: Routledge.

Dun & Bradstreet. (2022). *Russia-Ukraine Crisis: Implications for the global economy and businesses*.

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*(June 2020). https://doi.org/10.1016/j.ijpe.2020.107972

Elmsalmi, M., Hachicha, W., & Aljuaid, A. M. (2021). Prioritization of the best sustainable supply chain risk management practices using a structural analysis based-approach. *Sustainability (Switzerland)*, *13*(9). https://doi.org/10.3390/su13094608

Fan, Y., & Stevenson, M. (2017). A review of supply chain risk management: definition, theory, and research agenda. *International Journal of Physical Distribution and Logistics Management*, *48*(3), 205–230. https://doi.org/10.1108/IJPDLM-01-2017-0043

Freeman, E. R. (Ed.). (1984). *Strategic Management: A Stakeholder Approach*. Pitman.

Gouda, S. K., & Saranga, H. (2018). Sustainable supply chains for supply chain sustainability: impact of sustainability efforts on supply chain risk. *International Journal of Production Research*, *56*(17), 5820–5835. https://doi.org/10.1080/00207543.2018.1456695

Hamel, G., & Välikangas, L. (2003). The quest for resilience. *Harvard Business Review*, *81*(8), 52–65.

Herrera, I. A., & Hovden, J. (2008). Leading indicators applied to maintenance in the framework of resilience engineering: A conceptual approach. *3rd Resilience Engineering Symposium*, (October). Antibes-Juan Les Pins, France.

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

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, *4*, 1–23. https://doi.org/10.1146/annurev.es.04.110173.000245

Holling, C. S. (1996). Engineering resilience vs. ecological resilience. In P. Schulze (Ed.), *Engineering within ecological constraints* (pp. 31–44). Washington, DC: National Academy Press.

Hollnagel, E. (2009). The four cornerstones of resilience engineering. In C. P. Nemeth, E. Hollnagel, & S. Dekker (Eds.), *Preparation and Restoration* (pp. 117–133). Farnham and Burlington: Ashgate.

Hollnagel, E. (2014a). Becoming resilient. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 179–192). Boca Raton, FL: CRC Press.

Hollnagel, E. (2014b). Resilience engineering and the built environment. *Building Research and Information*, *42*(2), 221–228. https://doi.org/10.1080/09613218.2014.862607

Hollnagel, E., Woods, D. D., & Leveson, N. (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate.

Jones, T. M., Harrison, J. S., & Felps, W. (2018). How applying instrumental stakeholder theory can provide sustainable competitive advantage. *Academy of Management Review*, *43*(3), 371–391. https://doi.org/10.5465/amr.2016.0111

Jüttner, U. (2005). Supply chain risk management: Understanding the business requirements from a practitioner perspective. *The International Journal of Logistics Management*, *16*(1), 120–141.

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/10.1080/1367556031000162701 6

K'nIfe, K. (2007). Accommodating uncertainty and minimizing risk. In T. A. Smith & O. Jones (Eds.), *Tourism Marketing: Insights from the Caribbean* (pp. 64–89). IDEAZ.

Kasperson, J. X., & Kasperson, R. E. (2001). Border crossings. In J. Linnerooth-Bayer, R. E. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 207–242). London: Earthscan Publications Ltd.

Kern, D., Moser, R., Hartmann, E., & Moder, M. (2012). Supply risk management: Model development and empirical analysis. *International Journal of Physical Distribution and Logistics Management*, *42*(1), 60–82. https://doi.org/10.1108/09600031211202472

Kilpatrick, J. (2022). Supply chain implications of the Russia-Ukraine conflict. Retrieved May 2, 2022, from Deloitte website: https://www2.deloitte.com/xe/en/insights/focus/supply-chain/supply-chain-war-russia-ukraine.html

Kırılmaz, O., & Erol, S. (2017). A proactive approach to supply chain risk management: Shifting orders among suppliers to mitigate the supply side risks. *Journal of Purchasing and Supply Management*, *23*(1), 54–65. https://doi.org/10.1016/j.pursup.2016.04.002

Klein, G. (2009). *Streetlights and Shadows: Searching for the keys to adaptive decision making*. MIT Press.

Kleindorfer, P., & Saad, G. (2005). Managing disruption risks in supply chains. *Production and Operations Management*, *14*(1), 53–68.

Knemeyer, A. M., Zinn, W., & Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management*, *27*(2), 141–153. https://doi.org/10.1016/j.jom.2008.06.002

Komatsubara, A. (2014). Resilience must be managed: A proposal for a safety management process that includes a resilience approach. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 97–111). Boca Raton, FL: CRC Press.

Lavastre, O., Gunasekaran, A., & Spalanzani, A. (2014). Effect of firm characteristics, supplier relationships and techniques used on Supply Chain Risk Management (SCRM): an empirical investigation on French industrial firms. *International Journal of Production Research*, *52*(11), 3381–3403. https://doi.org/10.1080/00207543.2013.878057

Lay, E., & Branlat, M. (2014). Noticing brittleness, designing for resilience. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 139–155). Boca Raton, FL: CRC Press.

Lee, J. M., & Wong, E. Y. (2021). Suez Canal blockage: an analysis of legal impact, risks and liabilities to the global supply chain. *MATEC Web of Conferences*, *339*, 1–14. https://doi.org/10.1051/matecconf/202133901019

Li, G., Fan, H., Lee, P. K. C., & Cheng, T. C. E. (2015). Joint supply chain risk management: An agency and collaboration perspective. *International Journal of Production Economics*, *164*, 83–94. https://doi.org/10.1016/j.ijpe.2015.02.021

Li, X., & Barnes, I. (2008). Proactive supply risk management methods for building a robust supply selection process when sourcing from emerging markets. *Strategic Outsourcing: An International Journal*, *1*(3), 252–267. https://doi.org/10.1108/17538290810915308

Lidskog, R., Uggla, Y., & Soneryd, L. (2011). Making transboundary risks governable: Reducing complexity, constructing spatial identity, and ascribing capabilities. *Ambio*, *40*(2), 111–120. https://doi.org/10.1007/s13280-010-0123-3

Linnerooth-Bayer, J. (2001). Introduction. In J. Linnerooth-Bayer, R. E. Löfsted, & G. Sjöstedt

(Eds.), *Transboundary risk management* (pp. 1–30). London: Earthscan Publications Ltd.

Löfstedet, R. E., & Sjöstedt, G. (2001). Transboundary environmental risk management in the new millennium: Lessons for theory and practice. In J. Linnerooth-Bayer, R. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 305–323). London, UK: Earthscan Publications Ltd.

Lupton, D. (2013). *Risk* (Second). New York: Routledge.

Madni, A. M., & Jackson, S. (2011). Towards a conceptual framework for resilience engineering. *IEEE Engineering Management Review*, *39*(4), 85–102. https://doi.org/10.1109/EMR.2011.6093891

Mainardes, E. W., Alves, H., & Raposo, M. (2012). A model for stakeholder classification and stakeholder relationships. *Management Decision*, *50*(10), 1861–1879. https://doi.org/10.1108/00251741211279648

Manuj, I., & Mentzer, J. T. (2008a). Global supply chain risk management. *Journal of Business Logistics*, *29*(1), 133–155.

Manuj, I., & Mentzer, J. T. (2008b). Global supply chain risk management strategies. *International Journal of Physical Distribution and Logistics Management*, *38*(3), 192–223. https://doi.org/10.1108/09600030810866986

Nadin, R., & Roberts, E. (2018). Moving towards a growing global discourse on transboundary adaptation. *Resilience Scan April–June 2017: A Review of Literature, Debates and Blogs on Resilience*, pp. 11–19. Retrieved from https://www.odi.org/sites/odi.org.uk/files/resource-documents/11259.pdf

Negri, M., Cagno, E., Colicchia, C., & Sarkis, J. (2021). Integrating sustainability and resilience in the supply chain: A systematic literature review and a research agenda. *Business Strategy and the Environment*, *30*(7), 2858–2886. https://doi.org/10.1002/bse.2776

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution and Logistics Management*, *34*(5), 434–456. https://doi.org/10.1108/09600030410545463

Opitz-Stapleton, S., Cramer, L., Kaba, F., Gichuki, L., Borodyna, O., Crane, T., … Seck, E. (2021). *Transboundary climate and adaptation risks in Africa: Perceptions from 2021*.

Petersen, K. (2019). Managing risk across borders: Ethical implications of engaging information technology for transboundary disaster collaboration. *Proceedings of the International ISCRAM Conference*, *May*(May), 298–305.

Petit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: development of a conceptual framework. *Journal of Business Logistics*, *31*(1), 1–21.

Pillay, M., & Morel, G. (2020). Measuring resilience engineering: An integrative review and framework for bench-marking organisational safety. *Safety*, *6*(3). https://doi.org/10.3390/safety6030037

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

Prabhakar, S. V. R. K., Issar, R., Bakar, A., & Yokoo, M. (2021). Mitigating transboundary risks by integrating risk reduction frameworks of health and DRR: A perspective from COVID-19 pandemi. In *Environmental Resilience and Transformation in Times of COVID-19* (pp. 63–76). https://doi.org/10.1016/c2020-0-02703-9

Provan, D. J., Woods, D. D., Dekker, S. W. A., & Rae, A. J. (2020). Safety II professionals: How resilience engineering can transform safety practice. *Reliability Engineering and System Safety*, *195*(August 2018), 106740. https://doi.org/10.1016/j.ress.2019.106740

Rankin, A., Lundberg, J., & Woltjer, R. (2014). A framework for learning from adaptive performance. In C. P. Nemeth & E. Hollnagel (Eds.), *Resilience engineering in practice, Volume 2: Becoming resilient* (pp. 79–95). Boca Raton, FL: CRC Press.

Reason, J. (1997). *Managing the risks of organizational accidents*. Brookfield, VT: Ashgate.

Renn, O. (2008). Risk Governance: Coping with uncertainty in a complex world. In R. E. Löfsted (Ed.), *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Renn, O., & Klinke, A. (2001). Public participation across borders. In J. Linnerooth-Bayer, R. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 245–277). London, UK: Earthscan Publications Ltd.

Ritchie, B., & Brindley, C. (2007a). An emergent framework for supply chain risk management and performance measurement. *Journal of the Operational Research Society*, *58*(11), 1398–1411. https://doi.org/10.1057/palgrave.jors.2602412

Ritchie, B., & Brindley, C. (2007b). Supply chain risk management and performance: A guiding framework for future development. *International Journal of Operations and Production Management*, *27*(3), 303–322. https://doi.org/10.1108/01443570710725563

Rose, A. (2018). Distributional considerations for transboundary risk governance of environmental threats. *International Journal of Disaster Risk Science*, *9*(4), 445–453. https://doi.org/10.1007/s13753-018-0205-6

Schlegel, G. L., & Trent, R. J. (2014). Supply chain risk management: Setting the stage. In *Supply chain risk management: An emerging dicipline* (pp. 1–24). https://doi.org/10.1007/978-3-319-76663-8_3

Sheffi, Y., & Rice Jr, J. B. (2005). A supply chain view of the resilient enterprise. *MIT Sloan Management Review*, *47*(1), 41–48.

Shirali, G. A., Azadian, S., & Saki, A. (2016). A new framework for assessing hospital crisis management based on resilience engineering approach. *Work*, *54*(2), 435–444. https://doi.org/10.3233/WOR-162329

Simons, R. (1999). How Risky is Your Company? *Harvard Business Review*, *77*(3), 85–94.

Sinha, P. R., Whitman, L. E., & Malzahn, D. (2004). Methodology to mitigate supplier risk in an aerospace supply chain. *Supply Chain Management*, *9*(2), 154–168. https://doi.org/10.1108/13598540410527051

Sjöstedt, G. (2001). International negotiation and the management of transboundary risks. In J. Linnerooth-Bayer, R. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 279–304). London, UK: Earthscan Publications Ltd.

Sodhi, M. S., Son, B. G., & 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

Sørskår, L., Abrahamsen, E. B., & Abrahamsen, H. B. (2017). On the use of economic analyses when evaluating new technology in helicopter emergency medical services. *ESREL Conference*.

Steen, R., & Pollock, K. (2022). Effect of stress on safety-critical behaviour: An examination of combined resilience engineering and naturalistic decision-making approaches. *Journal of Contingencies and Crisis Management*, (March 2021), 1–13. https://doi.org/10.1111/1468-5973.12393

Sundström, G., & Hollnagel, E. (Eds.). (2011). *Governance and control of financial systems: A resilience engineering approach*. Farnham, UK: Ashgate.

Svedin, U. (2001). Foreword. In J. Linnerooth-Bayer, R. E. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management*. London, UK: Earthscan Publications Ltd.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*(2), 451–488. https://doi.org/10.1016/j.ijpe.2005.12.006

Tang, O., & Musa, S. N. (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

Tavana, M., Nazari-Shirkouhi, S., & Farzaneh Kholghabad, H. (2021). An integrated quality and resilience engineering framework in healthcare with Z-number data envelopment analysis. *Health Care Management Science*, *24*(4), 768–785. https://doi.org/10.1007/s10729-021-09550-8

Thoma, K., Scharte, B., Hiller, D., & Leismann, T. (2016). Resilience engineering as part of security research: definitions, concepts and science approaches. *European Journal for Security Research*, *1*(1), 3–19. https://doi.org/10.1007/s41125-016-0002-4

Thompson, M., & Gyawali, D. (2001). Transboundary risk management in the South: A Nepalese perspective on Himalayan water projects. In J. Linnerooth-Bayer, R. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 183–205). London, UK: Earthscan Publications Ltd.

Tredgold, T. (1818). XXXVII. On the transverse strength of timber. *Philosophical Magazine Series 1*, *51*(239), 214–216. https://doi.org/10.1080/14786441808637536

Triscritti, F. (2013). Mining, development and corporate–community conflicts in Peru. *Community Development Journal*, *48*(3), 437–450.

Tummala, R., & Schoenherr, T. (2011). Assessing and managing risks using the Supply Chain Risk Management Process (SCRMP). *Supply Chain Management*, *16*(6), 474–483. https://doi.org/10.1108/13598541111171165

UNISDR. (2017). *Words into action guidelines: National disaster risk assessment. Cross-border risk assessment*.

Vari, A., & Linnerooth-Bayer, J. (2001). A transborder environmental controversy on the Danube: The Gabcikovo-Nagymaros sam system. In J. Linnerooth-Bayer, R. Löfsted, & G. Sjöstedt (Eds.), *Transboundary risk management* (pp. 155–181). London, UK: Earthscan Publications Ltd.

Voas, J., Kshetri, N., & DeFranco, J. F. (2001). Scarcity and global insecurity: The semiconductor shortage. *IT Professional*, *23*(5), 78–82. https://doi.org/10.1109/MITP.2021.3105248

Wakolbinger, T., & Cruz, J. M. (2011). Supply chain disruption risk management through strategic information acquisition and sharing and risk-sharing contracts. *International Journal of Production Research*, *49*(13), 4063–4084.

Westrum, R. (2006). A typology of resilience situations. In E. Hollnagel, D. D. Woods, & N. Leveson (Eds.), *Resilience engineerng: concepts and precepts* (pp. 55–66). Aldershot, UK: Ashgate.