The Role and Scope of Port Community Systems in Providing Data that Enhances Supply Chain Risk Management

A Case Study for Freight Forwarders in the Port of Rotterdam

Master Thesis

Author:	Sascha Treppte, 347378
University:	RSM Erasmus University, Accounting and Control
Supervisor:	Prof. Dr. Arnick Boons
	RSM Erasmus University, Accounting and Control
Co-Reader:	Dr. Rob Zuidwijk
	RSM Erasmus University, Decision and Information Sciences
Date of Completion:	September 9, 2011

Table of Contents

Preface

This thesis concludes my studies in the one-year MScBA program “Accounting & Control” at Rotterdam School of Management, Erasmus University. It is based on research conducted between March and August 2011.

I thank my coach, Prof. Dr. Arnick Boons for his guidance and support. His comments and critiques significantly contributed to the quality of my work.

I am also grateful to my co-reader, Dr. Rob Zuidwijk who introduced me to the CASSANDRA project and inspired me to do research on port community systems. His support in numerous brainstorm sessions influenced my approach to the topic. Further, his advice and productive comments on my ideas and results directly contributed to this thesis.

Finally, I am indebted to my interview partners for taking their time to answer my questions. This thesis would not have been possible without their participation.

The author declares that the text and work presented in this Master thesis is original and that no sources other than those mentioned in the text and its references have been used in creating the Master thesis.

Executive Summary

Given the increasing importance of supply chain risk management (SCRM) for operational success in global trade, efficient exchange of risk-relevant information among supply chain members has become a competitive advantage. Port community systems (PCS) facilitate the information exchange in and around port communities and, therefore, might contribute to risk management of supply chain members.

To further advance research on both topics and to assist different supply chain members in identifying relevant risk factors as well as appropriate sources for risk-relevant information, this thesis investigates the role and scope of PCSs in SCRM. In particular, it studies to what extent risk managers of freight forwarders can rely on PCSs to provide them with information relevant for SCRM regarding the cross-border maritime container transport.

First, the author performs desk research in order to review researchers' output on both topics. The results are used to derive relevant research questions and to develop interview questionnaires. Next, the author conducts semi-structured interviews with representatives of freight forwarders, Portbase as a PCS operator, and Dutch Customs. The answers are summarized to present freight forwarders' main processes in the cross-border maritime container transport as well as associated risk factors and information needs. Finally, the author compares forwarders' information needs with the information content of PCSs and other IT systems in order to conclude on the role and scope of PCSs in SCRM.

The results characterize the role of PCSs in SCRM of freight forwarders as to serves as a source for information used to prove the validity and accuracy of risk-relevant data provided by other supply chain members. In other words, PCSs solely represent a backup information source. Moreover, the systems' scope is limited with respect to four subject matters: risk management process, offered services, supply chain, and geographical focus.

Further, the author also discusses three general implications regarding risk management and PCSs. First, the coordination of demand and supply of risk-relevant information in the maritime container transport needs to be improved. Second, a global standardization of security and safety management might be beneficial. Third, general information technology advancements have eroded PCSs' business position to a certain extent. Consequently, system operators need to identify new niches and alternative business models to survive in the long-run.

List of Abbreviations

AEO	Authorized economic operator
B2B	Business-to-business
B2G	Business-to-government
BCM	Business continuity management
ECD	Empty container depot
EDI	Electronic data interchange
EPCSA	European Port Community Systems Association
ERM	Enterprise risk management
ETA	Expected time of arrival
FCL	Full container load
IS	Information system
IT	Information technology
PA	Port authority
PCS	Port community system
POD	Port of destination
POL	Port of loading
SCM	Supply chain management
SCO	Supply chain orientation
SCRM	Supply chain risk management
SWOT	Strengths, weaknesses, opportunities, and threats
TEU	Twenty foot equivalent unit container
TQM	Total quality management

List of Figures and Tables

1 Introduction

1.1 Problem Definition

SCRM is highly dependent on up-to-date information. For that reason, it builds on information technology (IT) to make information exchange timely, accurate, and efficient. Nowadays, most deep-sea ports have recognized the importance of IT and offer a PCS to facilitate the information exchange between companies operating in and around ports. However, it has not been researched whether, and if so to what extent, PCSs contribute to SCRM of port community members. Therefore, this thesis investigates to what extent risk managers of freight forwarders can rely on PCSs to provide them with information relevant for SCRM regarding the cross-border maritime container transport. For the purpose of this thesis, maritime container transport always includes pre-transport of the containers to and their follow-up transport away from the port.

1.2 Background

SCRM was a seldom studied field of research before the beginning of the 1990s (Svensson, 2000). The complexity of supply chains, however, has been increasing due to globalization, outsourcing, lean processes, and numerous other supply chain trends (Pfohl et al., 2010; Jüttner, 2005, Norrman and Jansson, 2004). Academia often equates complexity with vulnerability, i.e. the exposure to disruptions (Waters, 2007; Christopher and Peck, 2004; Cranfield School of Management, 2003). According to Pfohl et al. (2010), supply chain disruptions can be triggered on both the supply- and demand side. Possible sources are e.g. terrorist attacks, natural disasters, and changes in consumer behavior. Over the last two decades, numerous highly visible supply chain disruptions have changed the perception of SCRM (Sodhi et al., 2011; Norrman and Jansson, 2004). This year's major earthquake as well as the subsequent tsunami and nuclear crises in Japan are contemporary examples. Supply chain disruptions negatively affect cost and quality of products as well as the image and long-term stock performance of companies. In the worst case, they can represent existential threats to individuals, companies, or industries (Sodhi et al., 2011; Pfohl et al., 2010). Hendricks and Singhal (2005) estimate the average abnormal stock returns of firms that experienced disruptions between 1989 and 2000 to be almost -40%. Another well-known consequence of supply chain complexity and vulnerability is the bullwhip effect. It describes "increasing fluctuations of order patterns from downstream to upstream supply chains" (Christopher and Lee, 2004, p.388). In other words, supply chain members accept slack in their operations in order to have a buffer against disruptions. Such buffers, however, are costly and highly inefficient (Christopher and Lee, 2004). Consequently, a fundamental consensus about the importance of SCRM has been emerging in research as well as in business practice over the last decade (Sodhi et al., 2011; Pfohl et al., 2010). The increasing research interest in SCRM is reflected in the number of books published on the topic (Wu and Blackhurst, 2009; Waters, 2007) as well as the growing body of literature that has been reviewed by numerous authors (Sodhi, et al., 2011; Tang, 2006). In business practice, consulting firms and other industry experts have published surveys and reports on SCRM (McKinsey, 2008; IBM, 2008).

Ports serve as nodes and hubs in complex global supply chains. Their operational efficiency affects the competitiveness of the entire chain. However, ports' operational and economic success is largely determined by developments that go beyond the control of port management (Van Baalen et al., 2008). For that reason, ports have to build their competitive advantages on a rather small circle of influence. According to different researchers, the standardization, automation, and rationalization of inter-firm information exchanges affect the operational efficiency of ports. Moreover and most importantly, these tasks lie within the ports' influence (McMaser and Wastell, 2005; Wrigley et al., 1994). Therefore, IT capabilities function as an important differentiator among ports. Consequently, most deep-sea ports operate a PCS which facilitates the information exchange between participating companies in and around a port (Van Baalen et al., 2008). Despite their strategic importance for deep-sea ports, researchers have only contributed few studies concerning PCSs (Rodon and Ramis-Pujol, 2006).

1.3 Motivation and Research Questions

This thesis is mainly motivated by the complexity and fuzziness of the intersection between the two nascent research areas of SCRM and PCSs. Moreover, the topic is of high relevance in praxis and politics. The European Commission is funding numerous pan-European research projects regarding SCRM in the maritime container transport – e.g. INTEGRITY and CASSANDRA. The former studied intermodal global door-to-door container supply chain visibility from 2008-2011 (Integrity, 2011; RSM, 2008). The latter kicked-off at the beginning of June 2011 and has been studying how information systems facilitate risk assessment of businesses and governments in the cross-border maritime container transport (TNO, 2011). This thesis is strongly connected to the current research project CASSANDRA. The author focuses on PCSs as information platforms in SCRM in the cross-border maritime container transport. To the author’s knowledge, no previous academic study has analyzed whether companies are using PCSs to facilitate their risk management. Decision criteria, information needs, and, if applicable, the extent of PCS utilization in risk management of cross-border maritime container transport are unknown. Therefore, the prevailing research question of this thesis reads as follows and is presented as research question five in the main text:

What is the role and scope of PCSs in providing data that enhances SCRM of freight forwarders regarding the cross-border maritime container transport?

“Role and “scope” are defined following the Oxford Dictionaries. A role is “the function assumed or part played by a person or thing in a particular situation” (Oxford Dictionaries, 2011a). Scope is defined as “the extent of the area or subject matter that something deals with or to which it is relevant” (Oxford Dictionaries, 2011b). In order to conclude on role and scope of PCSs in SCRM, the author addresses sub-questions presented as research questions one to four in the main text.

RQ 1: What are the main risks and their sources faced by freight forwarders in the cross-border maritime container transport?

RQ 2: What are the information needs of freight forwarders to manage the risks of cross-border maritime container transport?

RQ 3: What information is provided by PCSs to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

RQ 4: What information is provided by alternative information systems to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

The author focuses on containerized maritime transport rather than bulk or general cargo as more than “90% of world trade involves containers aboard ships, amounting to about 20 million containers trips annually” (Lee and Whang, 2005, p.1). Moreover, the container revolutionized the transportation industry through cost reduction by standardization (Van Baalen et al., 2008). Nowadays, a twenty foot equivalent unit (TEU) container – 20 x 8 x 8.5 feet – is a standard measure in transportation (Brandenburg et al., 2010). It is that standardization which enables intermodal transport, i.e. “the movement of containers from point of origin to point of delivery using different modes of transport, such as ships, trains, and trucks, without handling the goods themselves during transshipment” (Van Baalen et al., 2008, p.85).

The analysis of cross-border rather than domestic transport is motivated by numerous aspects. First, deep-sea shipping almost always involves crossing international borders. Besides the transfer of physical goods, it also comprises the transfer of information and money. This draws government attention (e.g. customs) in at least the exporting and importing countries and thus adds more stakeholders to the supply chain. Second, international transport over large distances is exposed to a larger variety of risk sources than domestic trade. Third, cross-border trade often involves operations in significantly different legal jurisdictions (Wrigley et al., 1994).

Freight forwarders represent an appropriate exemplary focal group for several reasons. First, they take an important role in the cross-border maritime container transport. According to Murphy et al., a freight forwarder is “an international trade specialist who can provide a variety of functions to facilitate the movement of cross-border shipments” (1992, p.2). Besides the arrangement of transportation services, freight forwarders are also responsible for the proper declaration and settlement of the content of containers (David and Stewart, 2008; Virtuele Haven, 2001; Murphy and Daley, 2001). Second, Martin and Thomas (2001) as well as Murphy and Daley (1999) indicate that IT (e.g. PCSs) plays a vital role in the freight forwarding industry. Consequently, freight forwarders represent a user group of PCSs. Third, freight forwarders, due to their broad remit, are exposed to a variety of different risks. The management of these risks is analyzed in the context of this thesis. Findings can then be tested for other focal groups that show similar characteristics as freight forwarders regarding the involvement in cross-border maritime container transport

1.4 Contribution

The findings of this thesis are of great interest to both researchers and practitioners. They will shed light on information needs of freight forwarders concerning SCRM. Further, they can be tested for other focal groups that show similar characteristics as freight forwarders regarding the involvement in cross-border maritime container transport and the use of PCSs. Contributions to the pan-European research project CASSANDRA are multifaceted. First, the thesis provides desk research on the state of the art supply chain risk management. Second, it discusses PCSs as a visibility platform and touches upon other information systems. Third, the thesis analysis parts of the maritime container transport supply chain with focus on freight forwarders. From a practical point of view, the findings can possibly improve the SCRM of containerized maritime cargo transport and thus prevent monetary or reputation losses. Finally, PCS operators can use the findings and implications of the thesis to improve and adjust their service offerings to customer needs.

1.5 Reading Guide

The remainder of this thesis is structured as follows: Chapter 2 provides an overview of the related theory. It discusses SCRM and PCSs in detail. Chapter 3 presents the research methodology. In chapter 4, the author outlines his results. Chapter 5 discusses the results and concludes this thesis.

2 Theory

2.1 Supply Chain Risk Management

2.1.1 Supply Chain

The nature of supply chains has been debated heavily and a variation of definitions exists (Waters, 2007; Peck, 2006). In 1998, the Chartered Institute of Logistics and Transport of the UK defined a supply chain as “a sequence of events intended to satisfy a customer” (as cited in Waters, 2007, p.37). Such a definition could include almost anything. Further, it is questionable whether the term “chain” is appropriate. Peck (2006) and Burgess et al. (2006) propose the term “network” rather than chain in order to represent the complex systems of networks inherent in supply chains.

In order to develop a better understanding of the above-presented issues and to lay a profound basis for this thesis, the author discusses supply chains in more detail.

Taking the view of a single organization, supply chains move tangibles (e.g. goods) as well as intangibles (e.g. information) in three different ways: (1) from suppliers into the organization; (2) within the organization; (3) from the organization to its customers. As organizations do not work in isolation, tangibles and intangibles move through numerous organizations, which each act as customer and supplier. From a focus organization’s point of view, suppliers and customers can be arranged in tiers. Direct suppliers and customers of the focus organization are referred to as first-tier; the first-tiers’ suppliers and customers as second-tier, and so on. At the ends of the supply chain stand the original sources and final users of tangibles and intangibles. The supply chain for a single tangible or intangible can have numerous configurations and comprise thousands of different organizations. Moreover, each single organization can deal with numerous tangibles and intangibles (Waters, 2007; Mentzer et al., 2001). That complexity supports the proposition of Peck (2006) and Burgess et al. (2006) to refer to supply networks rather than chains. For the purpose of this thesis, however, the author agrees with Waters (2007) in recognizing that this difference reduces to semantics rather than content, and keeps the term “supply chain”. Nevertheless, the complexity of supply chains is recognized.

Having discussed its semantics, the author can now focus on the definition of a supply chain. Due to the above explained multi-tiered complexity of supply chains, definitions tend to frame the term from specific perspectives (Peck, 2006). From a network-based perspective, Aitken (1998) defines a supply chain as “a network of connected and interdependent organisations, mutually and co-operatively working together to control, manage and improve the flow of material and information from suppliers to end users” (as cited in Peck, 2006, p.128). Taking a value-based perspective, Christopher (1998) defines a supply chain as “the network of organisations that are linked through upstream and downstream relationships in the different processes and activities that produce value in the form of products and services in the hands of the ultimate customer” (p.12). Both of these definitions provide a more focused view than the one by the Chartered Institute of Logistics and Transport as presented above. Peck (2006) combines the definitions and concludes that “supply chains comprise flows of materials, goods and information (including money), which pass within and between organisations, linked by a range of tangible and intangible facilitators, including relationships processes, activities and integrated (information) systems” (p.128). Further, Peck (2006) claims that academic debates over the definition of a supply chain have not dispelled functional legacies. Therefore, the “supply chain”, in practice, means different things to different people (Peck, 2006). This is problematic, as the identification of supply chain risks is significantly hampered in absence of a common understanding of the term “supply chain” (Haywood and Peck, 2003). Given that, for the purpose of this thesis, a supply chain is defined in a rather general way without taking a specific perspective or unit of analysis. This should allow for the identification of supply chain vulnerabilities. The author, therefore, follows Mentzer et al. (2001) who define a supply chain as “a set of three or more entities (organizations or individuals) directly involved in the upstream and downstream flows of products, services, finances, and/or information from a source to a customer” (p.4).

Mentzer et al. (2001) argue that supply chains exist regardless of whether or not they are managed. Section 2.1.2 discusses what exactly the management of supply chains comprises and why it is so important.

2.1.2 Supply Chain Management

Supply chain management (SCM) is a field of research itself. Burgess et al. (2006) conducted a key word search of the exact phrase in the ABI/Inform Global Proquest database and identified 3,511 relevant articles in 31 journals covering a sampling period from 1998 to mid-2003. Further, Stock et al. (2009) revealed 166 unique definitions of SCM since the mid-1980s.

Given that and the purpose of this chapter to define supply chain risk management, the author provides a general overview rather than an exhaustive literature review of SCM.

The concept of SCM was first mentioned in business literature in the 1960s (Guinipero et al., 2008). Forrester (1968) related the success of industrial companies to the "interactions between flows of information, materials, manpower and capital equipment" (p.8). It was not until 1982, however, that Oliver and Webber introduced the term SCM and it took another 15 years for the first theoretical and empirical research questions to be addressed (Lambert et al., 1998). According to Burgess et al. (2006), SCM is still an evolving field. Rather than using existing standard definitions, researchers still try to develop new ones based on narrow functional knowledge in fields like purchasing, logistics, and IT. The two most recent literature reviews by Burgess et al. (2006) and Guinipero et al. (2008) point out the definition by Mentzer et al. (2001) as the most recognized in the field of SCM. For that reason, the author briefly outlines the concepts and definitions of the 2001 paper by Mentzer et al.

Mentzer et al. (2001) classify a representative sample of existing definitions of SCM into three categories: a management philosophy, the implementation of a management philosophy, and a set of management processes. They acknowledge the benefits of these categories but also conclude that, in literature, the term SCM is used to describe two different concepts. Consequently, they distinguish between supply chain orientation (SCO) and SCM. The first is the "strategic-level recognition of the need for co-ordination and collaboration throughout the supply chain" (Peck, 2006, p.129). The second is the functional implementation of SCO through e.g. information sharing, cooperation, (long-term) relationship building, risk and reward sharing, and interfunctional coordination. Such interfunctional coordination needs to comprise all traditional business functions such as marketing, research and development, logistics, etc. (Mentzer et al., 2001). Therefore, logistics, which is at the core of this thesis, is only one of the functions contained in SCM (Peck, 2006; Mentzer et al., 2001). According to Mentzer et al., SCM can only be successful if true SCO is present across three or more adjacent firms. They define true SCO as the management of both, upstream (towards suppliers) and downstream (towards customers) supply chain activities. In other words, a single firm may have SCO and implement individual supply chain tactics, but will not succeed in SCM unless its two adjacent partners in the supply chain also recognize the need for the coordination of these tactics. SCO is seen as a prerequisite for SCM but has antecedents itself (Mentzer et al., 2001). SCO can only be achieved if the single companies develop relationship trust and commitment (Morgan and Hunt, 1994). Further antecedents of SCO are, inter alia, top management support, interdependence, and organizational compatibility (Mentzer et al., 2001). The above outlined concepts are summarized in Figure 1.

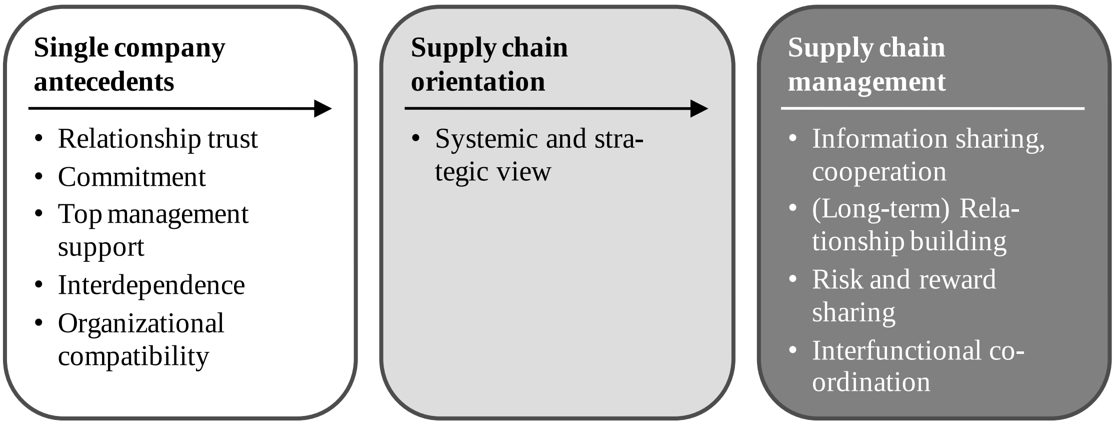
Single company antecedents
• Relationship trust
• Commitment
• Top management support
• Interdependence
• Organizational compatibility
Supply chain orientation
• Systemic and strategic view
Supply chain management
• Information sharing, cooperation
• (Long-term) Relationship building
• Risk and reward sharing
• Interfunctional coordination

Figure 1, Supply chain management and its antecedents (Source: Mentzer et al., 2001)

For the purpose of this thesis, the author follows Mentzer et al. (2001) in recognizing SCO and SCM as two distinct but interlinked concepts. Logistics is considered as a subset of SCM and comprises activities such as integrated transport, storage, distribution, etc. (Waters, 2007; Peck, 2006).

The motive of SCO and SCM is to increase the competitive advantage of the entire supply chain (Mentzer et al., 2001). This is achieved through lower costs and higher profitability as well as improved customer value and satisfaction (Waters, 2007; Mentzer et al., 2001). A close coordination between suppliers and distributors is required. In other words, the competitive battle is fought between supply chains rather than single companies (Guinipero et al., 2008; Mentzer et al., 2001; Lambert and Cooper, 2000).

The importance of SCO and SCM is driven by existing and, at the same time, stimulates the introduction of new trends in supply chain management (Waters, 2007). Such trends increase the chances for differentiation and thus provide conditions upon which companies base their competitive advantages (Pfohl et al., 2010). Unfortunately, at the same time, most of them are also drivers of supply chain risk (Pfohl et al., 2010; Craighead et al., 2007; Jüttner, 2005; Kleindorfer and Saad, 2005). Examples for trends in the supply chain comprise, inter alia, globalization, outsourcing, centralization, and lean processes (Pfohl et al., 2010; Jüttner, 2005). Due to the scope of this thesis, benefits associated with these trends are not discussed. Associated risks are outlined in section 2.1.3.

2.1.3 Risk

Risk in General

The concept of risk has its source in the mathematics associated with gambling and first arose in the seventeenth century. It was not until the nineteenth century, however, that risk emerged in the study of economics (Gerber and von Solms, 2005). Nowadays, the term “risk” is used rather vaguely and has different meanings and interpretations depending on the research perspective and business function (Zsidisin, 2003a; Baird and Thomas, 1990). Large bodies of risk-related literature can be found in the fields of decision theory, finance, marketing, and management (Wagner and Bode, 2006). Depending on where and when it is applied, the term “risk” is used to suggest chance or probability, to describe the mean value of an outcome, or to express an expected value (Pfohl et al., 2010; Waters, 2007; Jüttner et al., 2003; Zsidisin, 2003a). Given that, it is essential for any risk-related study to define the term appropriately (Wagner and Bode, 2006).

As indicated above, the term “risk” is used rather loosely. Peck (2006) points out that “risk” and “uncertainty” are terms that are used interchangeably, but technically mean different things. Waters (2007) goes one step further and distinguishes between ignorance, uncertainty, risk, and certainty. In the case of ignorance, a decision maker has absolutely no knowledge about future events (Waters, 2007). Uncertainty prevails if possible future events can be listed, but the probabilities of their occurrence cannot. In the case of risk, possible future events as well as the probabilities of occurrence are known (Waters, 2007; Knight, 1937). Certainty is referred to if decision makers know exactly what will happen in the future (Waters, 2007).

Risk related literature reveals a persistent tension regarding the possible outcomes of risk (Mitchell, 1995). Following classical decision theory, risk is the “variation in the distribution of possible outcomes, their likelihoods and their subjective values” (March and Shapira, 1987, p.1404). The definition covers both a downside and an upside potential of risk (Wagner and Bode, 2006; Peck, 2006; Zsidisin, 2003a). This implies that taking risks is not automatically negative, but can also be beneficial. A classical economical principle relates risk to profit – the greater the risk, the greater the potential profit (Pfohl et al., 2010; Waters, 2007). Most insurance companies and dictionaries, however, only consider the downside potential of risk (Wagner and Bode, 2006). The Oxford Dictionaries (2011c) define risk as “a situation involving exposure to danger" Common human perception seems to be in line with that notion of risk (Wagner and Bode, 2006). March and Shapira (1987) found that managers tend to only focus on the downside potential of risk. Little attention is paid to risks concerning positive outcomes. This view has been adopted in several definitions of risk. Harland et al. (2003), for example, define risk as a "chance of danger, damage, loss, injury or any other undesired consequences" (p.52).

The discrepancy of how people should react and how they do react as observed by March and Shapira (1987) can be related to discrepancies between natural and social scientists regarding the definition of risk (Peck, 2006). Natural scientists consider risks to be objective. Risks are evaluated by scientific assessment methods and thus are non-judgmental. Social scientists, however, consider risks as subjective and perceived. Decisions are based on values, beliefs, and opinions. In other words, people modify their behavior and thus their risk exposure based on subjective perceptions (Peck, 2006; Gerber and von Solms, 2005). Different risk behaviors and rationalities towards risk are discussed by utility and prospect theory which distinguish between risk aversion, neutrality, and seeking (Fiegenbaum and Thomas, 1988; Kahneman and Tversky, 1979; Fishburn, 1970).

Zsidisin (2003b) recognizes that risk, due to its multidimensional nature, is interpreted by academics and practitioners alike in many different ways.

Supply Chain Risk and Vulnerability

In contrast to the general risk literature, the term "risk" has a purely negative connotation with reference to supply chains (Peck, 2006; Wagner and Bode, 2006; Harland et al., 2003). This is reflected in general definitions of supply chain risk. Gaonkar and Viswanadham (2007) describe supply chain risk as "the distribution of the loss resulting from the variation in possible supply chain outcomes, their likelihood, and their subjective values" (p.2). In their 2006 paper, Wagner and Bode define the term as "the negative deviation from the expected value of a certain performance measure, resulting in negative consequences for the focal firm" (p.303). An often cited definition by Jüttner et al. (2003) frames supply chain risk with reference to the integrity of the flow of supply chains (Pfohl et al., 2010). To them, supply chain risk comprises "any risks for the information, material and product flows from original supplier to the delivery of the final product for the end user" (Jüttner et al., 2003, p.200). Pfohl et al. (2010) expand the 2003 definition by Jüttner et al. with a reference to outcome deviations. Further, they align their definition with the network levels of a supply chain. To them, supply chain risks “involve risks that can be attributed to disturbance of flow within the goods-, information-, and financial network […] They might have negative effects on the goal achievement of single companies and the whole supply chain, respectively, with regard to end customer value, costs, time, or quality” (p.34).

For the purpose of this thesis, the author concurs with the negative connotation of supply chain risk and applies the most complete definition as provided by Pfohl et al. (2010).

Supply chain risks only materialize with the occurrence of a harmful event (Waters, 2007). In other words, exceptional and anomalous situations in comparison to everyday business lead to the existence of supply chain risks (Manuj and Mentzer, 2008; Wagner and Bode, 2006). Such events can be labeled “supply chain disruptions” (Wagner and Bode, 2006) and are associated with a probability of occurrence. Further, they are characterized by their severity as well as direct and indirect negative effects for a single firm or the entire supply chain (Wagner and Bode, 2006; Kleindorfer and Saad, 2005). Disruptions can materialize from various areas and, for the purpose of this thesis, are labeled “supply chain risk sources” (Wagner and Bode, 2006; Jüttner et al., 2003). Possible supply chain risk sources are discussed in section 2.1.4.

As discussed above, supply chain risk sources lead to the materialization of risks. They are, however, not the only determinant of the final result. The susceptibility of supply chains to harm of supply chain risk sources is of relevance as well. This introduces the concept of vulnerability (Waters, 2007; Wagner and Bode, 2006). According to Peck (2005), vulnerability is a relatively new area of research. However, several authors have made contributions. Christopher and Peck (2004) define vulnerability as “an exposure to serious disturbance” (p.3). Further, they equate vulnerability with something that is likely to be lost or damaged. Svensson discussed supply chain vulnerability in numerous papers. He differentiates between atomistic and holistic vulnerability. In the case of an atomistic vulnerability approach, the risk of only a limited part of the supply chain is taken into account. If the entire supply chain is considered, he refers to a holistic vulnerability (2000, 2002). Barnes and Oloruntoba (2005) frame vulnerability in the context of maritime supply chains as “as a susceptibility or predisposition to […] loss because of existing organizational or functional practices or conditions” (p.519).

For the purpose of this paper, the author applies the definition of Barnes and Oloruntoba (2005) in the context of an atomistic perspective (Svensson, 2000, 2002). The atomistic perspective is chosen as this thesis focuses on risk management of freight forwarders – single members of supply chains. A selection of practices or conditions that drive supply chain vulnerability is discussed in the following section.

Drivers of Supply Chain Risk

A discussion of supply chain risk would not be complete without an overview of supply chain risk drivers. As indicated in section 2.1.2, certain trends in SCM increase the vulnerability and thus the risk of supply chains. This is usually not a result of planned change, but rather an undesired side effect due to one of two reasons. First, managers might simply not consider risks of new SCM approaches. Second, individual risks are often highly interconnected. As a result, methods and actions designed to increase efficiency or to mitigate a risk end up exacerbating the supply chain's overall vulnerability (Waters, 2007; Kleindorfer and Saad, 2005; Chopra and Sodhi, 2004). Especially with reference to SCM trends, Peck (2006) concludes, that "there is not clear consensus as to whether supply chain vulnerability is simply a symptom of poor SCM […] or whether it is the unintended downside consequence of its successful application" (p.139). In the following, the author provides a brief overview of repeatedly cited antecedents and drivers of supply chain vulnerability. The list is not exhaustive and due to the scope of this thesis, benefits associated with these trends are not discussed.

Cost pressure has motivated many companies from highly industrialized countries to partially or completely move their production to low cost countries and to procure internationally. This is referred to as globalization which further comprises the internationalization of the sales market (Pfohl et al., 2010). It is one of the most recognized supply chain risk drivers. Supply chain vulnerability is increased due to a higher structural complexity of supply chains. Companies have to deal with increased uncertainty, reduced control, problems related to cultural differences, as well as poorer transparency and visibility. Coordination expenses increase as materials have to be moved through longer supply chains (Pfohl et al., 2010; Waters, 2007; Wagner and Bode, 2006; Norrman and Jansson, 2004; Jüttner et al., 2003).

Another driver of supply chain risk is outsourcing. It allows access to global markets and thus contributes to the globalization of supply chains (Harland et al., 2003). In general, the degree of company-internal value-added decreases as companies transfer processes to other members of the supply chain (Pfohl et al., 2010). This is practiced especially in areas with less competence which are better handled by other, specialized organizations (Waters, 2007; Borge, 2001). Outsourcing generally leads to a fragmentation of the supply chain. Business transaction become more complex and firms might face situations in which they only have insufficient control over key processes (Pfohl et al., 2010; Waters, 2007; Jüttner et al., 2003; Harland et al, 2003).

Regarding centralization, it is again cost pressure that forces companies to focus on fewer production and distribution locations. Moreover, the supplier base is reduced and inventory levels are decreased. As a result, important resources depend on single organizations and divisions (Pfohl et al., 2010; Wagner and Bode, 2006). Companies become less flexible and therefore more vulnerable to change. Further, there is an increased vulnerability to downtimes in production of single companies and divisions (Pfohl et al., 2010; Waters, 2007; Jüttner et al., 2003).

A fourth driver of supply chain risk is the focus on lean production and just-in-time approaches. Designed to reduce waste in supply chains, they decrease or eliminate inventory as well as capacity and time buffers. These usually alleviate the effects of disturbances and delays in the supply chain. With lean processes, that mitigating effect is missing, exposing companies to the full impact of any disturbance (Pfohl et al., 2010; Zsidisin et al., 2005).

As a final risk driver, IT dependence is touched upon. Business in general and SCM in particular heavily rely on complex networks of integrated IT systems. The systems in a supply chain are as vulnerable to disturbances as their weakest link. A failure of the IT infrastructure within or between organizations can cause substantial damage. Moreover, data security is an issue. Sensitive data might be exposed through leakages or hacked by externals (Pfohl et al., 2010; Waters, 2007; Harland et al., 2003)

The above discussed examples accentuate the importance to explicitly consider possible adverse side effects of managing the supply chain if those are not to be captured (Rice et al., 2003). A systematic approach to supply chain risk management facilitates the exploitation of chances of SCM trends and preservation of control over associated risks in a balanced way (Pfohl et al., 2010; Kleindorfer and Saad, 2005).

2.1.4 Supply Chain Risk Management

After only about a decade of research on SCRM as of 2010, the area is still relatively new. In July of that year, a simple key word search of the exact phrase without a subsequent relevance check generated 1,400 research articles opposed to 151,000 for SCM (Sodhi et al., 2010). Consequently, SCRM has rather unclear boundaries (Sodhi et al., 2011; Pfohl et al., 2010; Wagner and Bode, 2006). This is reflected in the diversity of definitions as well as in differing perceptions of scope among researchers (Sodhi et al., 2011). The author covers the definition of SCRM within this section and returns to the differing perceptions of scope in the discussion on supply chain risk sources.

As indicated above, no generally accepted definition of SCRM has been developed (Sodhi et al., 2011). According to Norrman and Lindroth (2002), SCRM is the collaboration of all partners in the entire supply chain in order to develop a shared risk management process which enables them to deal with risks and uncertainties resulting from logistics activities and resources. Jüttner et al. (2003) define SCRM as “the identification and management of risks for the supply chain, through a coordinated approach amongst supply chain members, to reduce supply chain vulnerability as a whole” (p.6). Kajüter (2003) specifies the term “collaborative approach” and defines SCRM as “a collaborative and structured approach to risk management, embedded in the planning and control processes of the supply chain, to handle risks that might adversely affect the achievement of supply chain goals” (p.327). In 2010, Pfohl et al. widen the definition of SCRM and explicitly include supply chain security management as a subset. Following Closs and McGarrell, supply chain security management is defined as “the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism and to prevent the introduction or unauthorized contraband, people or weapons of mass destruction into the supply chain” (Closs and McGarrell, 2004, p.10).

A diversity of definitions does not only exist in academia. Sodhi et al. (2011) make out a definition gap among company executives as well. Moreover, they state that without a clear definition of SCRM, mutual learning between academia and praxis as well as access for researchers to the industry to conduct applied research will deteriorate. Given that, Sodhi et al. (2011) propose a basis for a generally accepted definition of SCRM. Their view is that SCRM has two parents: SCM (including SCO) and enterprise risk management (ERM). SCRM widens the scope of ERM from the focal firm’s immediate surroundings to the entire supply chain. Further, it accentuates the importance of risk analyses regarding supply chain management practices. Therefore, SCRM has traits from both parents without being a strict subset of either. Furthermore, this emerging area of research is more than the simple overlap between its two parents.

Even though this view has not yet been validated, its fundamentals can be made out in other researchers' approaches to SCRM. Waters (2007) as well as Jüttner et al. (2003) base their literature reviews on SCM and ERM in order to discuss and define SCRM. Further, Peck (2006) refers to SCRM as sitting on the intersection of several fields of academic research.

Despite a missing generally accepted definition of SCRM, several frameworks for the management of supply chain risks have been developed. Before discussing such frameworks, the author wants to recognize works by Peck (2006), Lee and Whang (2005) as well as Christopher and Rutherford (2004), who discuss total quality management (TQM) as a means to reduce risk. Peck (2006) describes TQM and process control methodologies as ways of managing and eliminating risks. Christopher and Rutherford (2004) apply an "Agile Six Sigma" (p.27) approach to reduce risks in supply chains. Since that methodology is rooted in hard statistical data, it is in line with classical risk management approaches (Peck, 2006). According to Lee and Whang (2005), TQM comprises prevention, quality management, source inspection, process control, and a continuous improvement cycle which are all components of the successful and effective management of supply chain risks. TQM, however, is not a focus topic of this thesis. Therefore, it is not discussed in detail, but mentioned if relevant.

As indicated above, SCRM literature has yielded frameworks for the management of supply chain risks. Waters (2007) suggests a structured approach of three steps: (1) identifying risks, (2) analyzing risks, and (3) responding to risks. These steps are framed by two core concepts: SCRM prerequisites and monitoring and control (Figure 2).

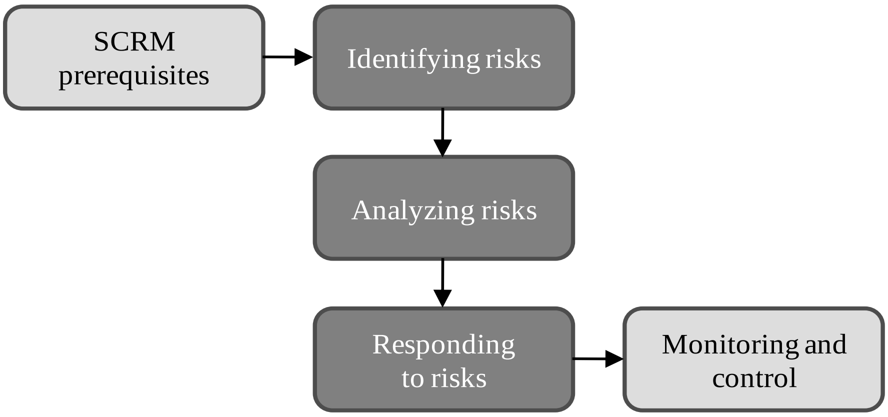

Figure 2, Framework for supply chain risk management (Source: Waters, 2007)

The author applies Waters' (2007) framework, with slight modifications, consistent with many other frameworks developed in SCRM literature (Pfohl et al., 2010; Manuj and Mentzer, 2008; Kleindorfer and Saad, 2005; Norrman and Jansson, 2004; Jüttner et al., 2003; Harland et al, 2003; Kajüter, 2003).

Waters (2007) first outlines the framework with regard to ERM before extending it to the entire supply chain for integrated SCRM. The general principles and core activities are essentially the same. The process in SCRM, however, is more complicated. The author describes the framework from the SCRM perspective.

SCRM Prerequisites

SCRM prerequisites are factors that enhance the successful implementation of a SCRM philosophy. If these are not given, SCRM is severely hampered (Pfohl et al., 2010).

Most importantly, organizations need to develop an understanding of risk in general and supply chain risk in particular. The importance of risk has to be acknowledged, especially among senior management. SCRM is doomed to fail without top management support (Waters, 2007; Christopher and Peck, 2003). Risk management needs to begin within the organization. Only when ERM is in place, managers should extend the scope to SCRM. A reasonable approach to extending the scope starts in isolated parts of the supply chain and then expends along the chain (Pfohl et al., 2010; Waters, 2007; Kleindorfer and Saad, 2005). Moreover, organizations need to take a strategic view on SCRM by defining a supply chain-wide risk strategy. Such a strategy creates awareness throughout the supply chain by outlining the chain members’ attitude towards risk, their aims, methods, and procedures (Stemmler, 2010; Waters, 2007; Kajüter, 2003; Harland et al., 2003). In other words, a risk strategy assures a mutual comprehension of potential risks (Pfohl et al, 2010). It allows the members of a supply chain to analyze and evaluate identified risks irrespective of the firm-specific attitude towards risk (Pfohl et al., 2010; Jüttner, 2005; Kajüter, 2003). The risk strategy has to be taken into consideration when making essential decisions concerning the supply chain (Pfohl et al., 2010). In order to be able to define a supply chain-wide risk strategy, companies within the chain have to have a close and fair relationship (Pfohl et al., 2010). Organizations have to achieve cooperation and mutual trust. This requires the sharing of ideas, methods, and information (Pfohl et al., 2010; Waters, 2007; Christopher and Peck, 2004; Lee and Whang, 2005). Risk information on all nodes and connections within the supply chain will only be exchanged if the organizations are not running risk of opportune behavior by other members of the chain (Jüttner, 2005). For a successful SCRM in specific and thus for the supply chain performance in general, Kajüter (2003) accentuates the importance to openly communicate identified risks among chain members. Moreover, he calls for cooperation between participating companies also with respect to control procedures in order to guarantee that organizations complement rather than negatively affect each other.

The above listed prerequisites for SCRM show many congruities with SCM (including SCO). This again underlines the close relationship of the two areas of research as discussed in the previous section.

Identifying Risks

According to Waters (2007) and most other researchers, the identification of risks is the initial step of SCRM. The author discusses general implications on how risks can be identified as well as possible risk sources.

Despite the importance of the activity, researchers mainly cover it as part of a wider discussion regarding SCRM only. They usually do not focus on procedures for risk identification (Sodhi et al., 2011). Nevertheless, the author was able to identify some general implications. First, organizations should map the entire supply chain to identify structural factors and gain insights on processes, ownership, relationships, and responsibilities (Cheng and Kam, 2008; Waters, 2007; Harland et al., 2003). Second, risk areas have to be defined in order to identify key risks. This should be done in a top-down and a bottom-up approach, respectively (Kajüter, 2003). A complete list of key risks can only be obtained if the organizations consider direct risks to their operations, risks to other entities, and risks caused by the linkage between organizations in the supply chain (Jüttner, 2005). Third and in accordance with one of the prerequisites to SCRM, risks have to be identified by each firm individually and then reported to all members of the supply chain (Kajüter, 2003). At this stage, it is important to take into consideration that risks relevant on an individual-firm basis might not be relevant for the entire chain. The same applies vice versa (Kajüter 2003). Finally, Waters (2007) proposes specific tools for the identification of risks. He groups them into three different approaches: analyzing past events, collecting opinions, and analyzing operations. Examples for tools are cause-and effect diagrams, interviews, and process charts respectively.

The nature of risk sources is multi-dimensional and dynamic as they are inseparably linked to the supply chain structure (Jüttner, 2005; Zsidisin et al., 2004; Harland et al., 2003; Zsidisin, 2003a). The literature review conducted by the author identified a large variety of definitions for risk sources. According to Peck (2010, 2005), risk sources possibly operate at several different levels of the supply chain. These levels are related to: (1) products and processes, (2) asset and infrastructure dependencies, (3) organizations and inter-organizational networks, and (4) the environment. On the first level, risks stem from process engineering and inventory management. The second level considers risks to fixed and mobile assets used at level 1. On the third level, risks are associated to strategic decisions of single organizations and the entire chain. Finally, level four comprises risks from the environment in which the supply chain operates (Peck, 2010, 2005). In contrast, Wagner and Bode (2006) distinguish between demand-side risks, supply-side risks, and catastrophic risks. Spekman and Davis (2004) define six dimensions of risk sources: inbound supply, information flow, financial flow, security of a firm's internal information system (IS), relationship with partner, and corporate social responsibility. Cavinato (2004) relates his definition of supply chain risks to the different flows in supply chains. His risk sources are: physical, financial, informational, relational, or innovational. Kleindorfer and Saad (2005), however, categorize risk sources as operational contingencies, natural hazards, and terrorism and political instability. As a final example, Rao et al. (2009) define framework, problem specific, and decisions making risk sources.

In the selection of a definition of risk sources to be applied in this thesis, the author considered Cheng and Kam (2008) as well as Tang (2006). According to these authors, risk, in the context of SCRM, includes risks to operational aspects of the supply chain activities and disruptions to operations. Risks to operational aspects can be rooted within an organization but also in the relations between supply chain members (demand-side and supply-side risks). Natural disasters and terrorist attacks are examples of disruptions to operations (Cheng and Kam, 2008; Tang, 2006). In other words, risk sources can be internal to the firm, external to the firm but internal to the supply chain network, or external to the network, i.e. environmental. This represents the definition of risk sources by Jüttner et al. (2003). In order to clarify what is included in the first two categories, Christopher and Peck (2004) further subdivide these categories in process and control as well as demand and supply respectively. For the purpose of this thesis, the author follows Jüttner et al. (2003) as well as Christopher and Peck (2004) and applies the following definition of risk sources:

- Organizational risk sources (risks internal to the firm)
    - Processes
    - Control

- Network risk sources (risks external to the firm but internal to the supply chain)
    - Demand-side
    - Supply-side
- Environmental risks sources

“Processes” comprise the value-adding and managerial activities of firms as well as the internally owned or managed assets used to support these processes. In the area of “control”, risks stem from assumptions, rules, systems, and procedures applied to control processes. Demand-side and supply-side risk sources are external to the firm but internal to the supply chain. From a focus organization’s point of view, they relate to processes, control, and assets up and down the supply chain, respectively. The focal firm does not own the processes and thus has no direct control. Further, network risk sources stem from the linkages between firms in the supply chain. Finally, environmental risk sources may impact parts of the chain or the entire chain and comprise political, economical, social, or technological aspects (Peck, 2010; Christopher and Peck, 2004; Jüttner et al., 2003).

The applied definition of supply chain risk sources – especially on the first level – is comparable to that of other authors (Tang and Tomlin, 2008; Manuj and Mentzer, 2008; Bogataj and Bogataj, 2007; Waters, 2007).

The identified risk sources can have an effect on all three flows of supply chains – physical, information, and financial – as discussed in section 2.1.1. Furthermore, the identification of risk sources has to be conducted on an operational, tactical, and strategic level in order to elevate a risk management system from a statutory reporting to a planning function (Stemmler, 2010). At the operational level, risks affect day-to-day business and do not show a regular pattern. They demand a responsive disruption management. At the tactical level, risks relate to reoccurring issues in planning and execution. Structural changes through enhanced coordination and synchronization are common. Finally, the strategic level refers to the overall performance of the supply chain. Risks may impact the supply chain in general and demand changes in e.g. the design of the entire chain (Van Baalen et al., 2008; Christopher and Peck, 2004). These three levels of analysis have to be applied to the entire SCRM framework, i.e. to all subsequent steps as well.

The discussion of supply chain risk sources can be summarized in Figure 3.

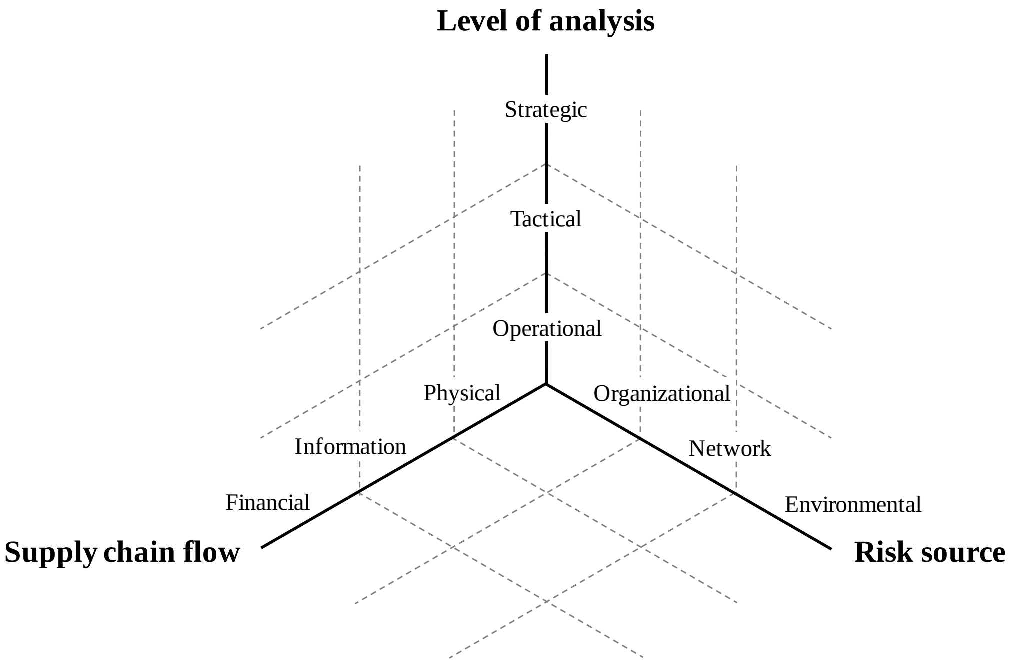

Figure 3, Levels of risk identification

Analyzing Risks

For the analysis of risk, the same applies as for its identification. Most of the papers covering the issue are conceptual or deal with SCRM as a whole. Tools for the analysis of risks are seldom provided (Sodhi et al., 2011).

A risk analysis can follow one of two approaches – a purely qualitative or a quantitative one (Waters, 2007). The qualitative approach solely focuses on describing the risk and its general features. It lays a good basis for discussion but is limited as it does not provide any numerical values. A qualitative risk analysis may raise a general sense of alarm in a single firm or in the entire supply chain, but responses will not necessarily be directed to the most relevant risks (Kleindorfer and Saad, 2005). Under the quantitative approach to risk analysis, in contrast, the relevance of each risk is numerically determined. Relevance depends on both the likelihood of a risk to occur and the significance of the risk's potential consequence. It is also referred to as the expected value of a risk (Knemeyer et al., 2009; Waters, 2007; Zsidisin et al., 2004; Kajüter, 2003; Harland et al., 2003):

$$Expected\ value\ of\ a\ risk = Likelihood * Potential\ damage$$

As discussed in the previous section, supply chain risk sources are multi-dimensional and dynamic. The estimation of the expected value is a complex task from a firm-specific point of view and becomes even more difficult for the entire supply chain (Waters, 2007; Jüttner, 2005; Harland et al., 2003). For that reason, similar to risk identification, the analysis of risks in a SCRM context is a two-step approach. Risks have to be analyzed by each firm individually and then reported to all members of the supply chain (Kajüter, 2003).

On a company-specific level, risks from all three sources, as presented in the previous section, have to be analyzed. The results of the risk analysis from a focal organization's point of view can be illustrated on a risk map (Figure 4), which is also referred to as a vulnerability matrix (Stemmler, 2010; Waters, 2007; Sheffi, 2005; Kajüter, 2003). Such a risk map facilitates the classification of risks into groups of priority. Most common is a differentiation of A-, B-, and C-risks with a decreasing priority (Stemmler, 2010; Waters, 2007; Kajüter, 2003). Due to the complexity of the risk analysis, likelihoods and potential damages are often expressed in ranges rather than exact values (Waters, 2007). Sometimes, risk consequences cannot be classified in a quantitative way with reasonable accuracy. This is especially true for off-balance sheet assets like credibility, reputation, status, authority, security, safety, or trust (Harland et al., 2003). However, consequences affecting these assets also have to be classified somehow in order to make them comparable and to direct responses to the most relevant risks (Kleindorfer and Saad, 2005). For these cases, a qualitative classification provides a fall-back approach (Waters, 2007; Kajüter, 2003). To determine the overall risk exposure of a focus company, one cannot just add the expected values of all risks. In fact, one has to follow a risk consolidation approach as risks are interrelated and thus compensate or cumulate each other (Kajüter, 2003).

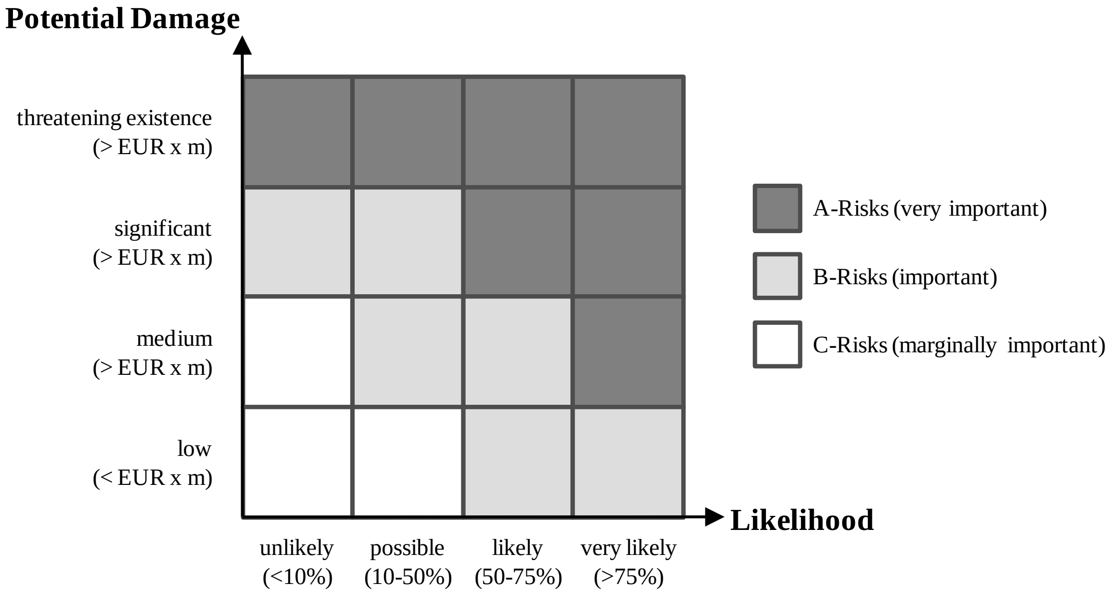

Figure 4, Company-specific risk map (Source: Kajüter, 2003)

The results of the company-specific analyses are reported to all members of the supply chain. Each risk's implication on the entire supply chain has to be evaluated. Again, risk consolidation has to be performed since risks reported by different members of the supply chain might be interrelated. The result at this stage of the risk analysis is a matrix (Figure 5) in which the risks analyzed on a firm-specific level are classified according to their company-specific risk category and their impact on the supply chain (Stemmler, 2010; Kajüter, 2003).

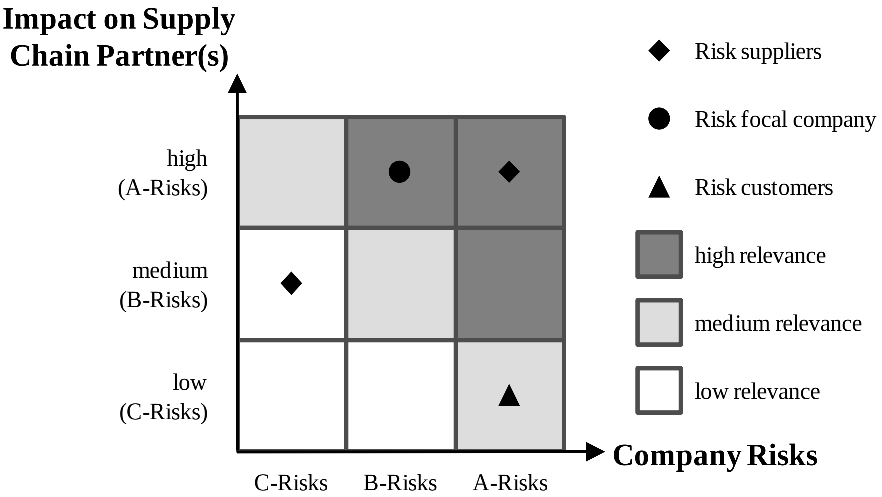

Figure 5, Supply chain risk matrix (Source: Kajüter, 2003)

The company-specific risk map and the supply chain risk matrix provide the basis for risk controlling, i.e. how to respond to risks (Stemmler, 2010). For an atomistic perspective of risk analysis, as applied in this thesis, the company-specific risk map is sufficient. It enables the author to analyze the supply chain risks of cross-border maritime container transport from the perspective of freight forwarders as a focus group.

Responding to Risks

After identifying and analyzing risks, decision makers have a prioritized list of risks. At this point, appropriate responses have to be selected and implemented (Mullai, 2009; Waters, 2007). Avoidance and reduction of risks are the two extremes of a range of possible responses. Within this range, different types exist (Stemmler, 2010; Kajüter, 2003; Miller 1992):

- Risk avoidance
- Risk reduction
- Risk transfer
- Risk acceptance

Risks can be so severe that an organization or supply chain decides not to engage in the particular activities that trigger the risk. Therefore, the likelihood of a particular risk is reduced to zero. In other words, risks are avoided by e.g. forfeiting investment opportunities, moving to a different business environment, or ceasing to exist. Since risk avoidance implies abandoning opportunities and in the worst case not continuing operations, it should only be considered under exceptional circumstances (Waters, 2007; Kajüter, 2003; Miller, 1992).

Risk reduction is a common and preferable response to risks (Stemmler, 2010; Kajüter, 2003). It is achieved either by decreasing the probability of a risk to occur or by reducing or limiting its potential damage. In integrated supply chains, higher degrees of standardization as well as intensified collaboration and information exchange reduce risks. These actions are more effective and usually less expensive than those that could be undertaken on a company-specific level – e.g. monitoring and personnel selection (Stemmler, 2010; Waters, 2007; Kajüter, 2003). The author further discusses benefits of collaboration and information exchange at a later point of this section.

Risk transfer moves some risks to an external entity. It can be achieved by insurance, hedging, or other contractual agreements (Waters, 2007; Kajüter, 2003). Risk transfer is comparatively easy to achieve in ERM, but is a difficult approach in SCRM (Stemmler, 2010). In SCRM, it is essential to transfer risks to entities outside the supply chain in order to reduce the overall risk exposure. If risks are simply transferred from one member of the supply chain to another, they still exist within the chain. In such a case, the chain's overall risk exposure only decreases if other members of the chain are more capable to handle the risk than the initial company that transferred it. However, as the opposite generally is the case, risk transfer within a supply chain tends to increase its overall risk exposure (Waters, 2007; Kajüter, 2003). Another issue with transferring risks is that not all risks are transferable. In general, only potential damages can be insured while speculative risks cannot. Further, even if companies are insured, they always face a certain residual. Insurances usually only reimburse for damages to tangible assets. Reputation losses due to supply problems after e.g. a destructive fire in a large distribution center are not covered (Stemmler, 2010; Waters, 2007; Kajüter, 2003).

If the costs of handling risks exceed their potential damage or if there are no other appropriate responses to risks, companies and supply chains have to accept them. This usually applies to low-scale or residual risks (Stemmler, 2010; Waters, 2007; Kajüter, 2003). Waters (2007) suggest adapting operations to accepted risks. However, this is only justifiable for risks of a certain magnitude. Risk ignorance is equivalent to risk acceptance (Waters, 2007).

Kajüter (2003) proposes another possibility for responding to risks which can be considered as an aggregate of risk acceptance and risk transfer. Supply chain members can share risks. By doing so, the supply chain’s overall risk exposure remains unchanged, yet potential consequences are distributed among all chain members involved rather than being born by a single company (Kajüter, 2003).

A final risk response refers to business continuity management (BCM). The author has not included it in the list of possible risk responses, as it mostly deals with unidentifiable risks (Waters, 2007). A structured management of such risks is not possible. Thus, they do not fit into the general SCRM framework presented in this chapter. However, the author briefly discusses a way of dealing with such risks. According to Peck (2006), BCM is comprised of risk management, security management, emergency management, and SCM. Briefly stated, BCM “looks for ways of dealing with actual disruptions to a supply chain, regardless of how these disruptions occurred” (Waters, 2007, p.215). It prepares and rehearses plans to restore supply chain flows after unpredictable disruptions (Waters, 2007; Kleindorfer and Saad, 2005).

Having outlined the spectrum of possible responses, it becomes apparent that different risk categories are best approached by different responses (Waters, 2007). In general, prevention is better than cure, i.e. SCRM should anticipate and respond to supply chain risks rather than simply reacting to their consequences (Stemmler, 2010; Waters, 2007). The choice of appropriate responses mostly depends on the trade-off between costs of mitigation and potential damage as well as on the risk strategy (Knemeyer et al., 2009; Waters, 2007; Kleindorfer and Saad, 2005; Jüttner et al., 2003). In general, type A risks need the most serious attention as they are potentially threatening the continuity of a company or the entire chain. Type B and C risks need subsequently less attention (Waters, 2007). However, risks with little impact or very low probabilities should never be completely ignored, but rather managed in a different manner (Kleindorfer and Saad, 2005). An integrated TQM approach helps in eliminating such risks without explicit SCRM. Applying TQM principles can eventually reduce risk exposure and drive down operating costs at the same time (Kleindorfer and Saad, 2005). Summing up, “deciding on suitable measures is a complex task in terms of decision making and implementation among the partners – even assuming that there is a consistent risk policy in place”

(Stemmler, 2010, p.187). Even within risk categories, responses might differ. Waters (2007) defines an appropriate response as one that maintains supply chain movements at low cost.

In general, the optimum is a robust supply chain that is not vulnerable to risks. This, however, is purely theoretical. In praxis, SCRM should focus on decreasing the frequency and severity of risks as much as possible (Kleindorfer and Saad, 2005; Christopher and Pack, 2004). Moreover, supply chains should be designed in a way that allows them to “bounce back from a disruption” (Sheffi, 2005, p.41). This is referred to as resilience (Waters, 2007; Van Oosterhout et al., 2007; Christopher and Peck, 2004; Sheffi, 2005). Christopher and Peck (2004) define resilience as “the ability of a system to return to its original state or move to a new more desirable state after being disturbed” (p.2). There are a number of basic principles involved with supply chain resilience. Most of these principles have already been discussed. They are consistent with SCRM in general and its prerequisites. Christopher and Peck (2004) summarize the principles in four main categories. These are namely: supply chain (re)engineering (design), supply chain collaboration, agility, and SCRM. The first category states that resilience has to be designed into the supply chain. The second category calls for collaboration because of the complexity of supply chains. Due to its analogy with the topic of this thesis, the author discusses that principle in more detail after briefly introducing the remaining two categories of principles. The third category refers to the fact that resilience implies quick responses to disruptions. Finally, the fourth category accentuates how SCRM enhances resilience (Christopher and Peck, 2004).

According to Waters (2007), the implementation of integrated SCRM and the creation of resilient supply chains are impossible without a basic level of collaboration. It can be achieved in a variety of ways ranging from informal discussions to strategic alliances. The bottom line of all forms of collaboration is information sharing. Christopher and Peck (2004) recognize this in their second category of principles for resilience, “supply chain collaboration”, and refer to information sharing as its underlying maxim. Information sharing among members of the supply chain increases visibility (Waters, 2007). Christopher and Lee (2004) define visibility by providing the right information “to the right member of the supply chain at the right time” (p.393). Visibility is essential for resilient supply chains as it allows for the early identification and analysis of as well as response to risks (Van Baalen et al., 2008). Further, only if risk information is shared among members of the supply chain, its potential is fully exploited (Christopher and Lee, 2004). Besides being a prerequisite for resilience, visibility has various collateral benefits, one of them being increased logistics efficiency (Rice and Spayd, 2005). Visibility, however, is not the only principle of supply chain collaboration and resilience. Supply chain members also need a certain degree of control (Jüttner et al., 2003). Control is needed over the information that is provided to the supply chain as well as over critical processes. In summary, conditions under which collaborative working, i.e. visibility and control, becomes possible have to be created (Christopher and Peck, 2004). Further, collaboration has to be achieved on an operational, tactical, and strategic level (Van Baalen et al., 2008; Christopher and Peck, 2004).

State-of-the-art information technologies facilitate the integration of information flows and assure supply chain visibility among all members of a supply chain (Kleindorfer and Saad, 2005). A PCS is an example for state-of the-art information technology. Given that, it can be assumed that PCSs have a role in assuring visibility and facilitating SCRM. PCSs are discussed in chapter 2.2.

Monitoring and Control

As one of the two core concepts of SCRM, monitoring and control transforms the discussed framework from a one-time procedure into a continuing cycle (Waters, 2007). It is necessary for two reasons. First, the effectiveness of risk responses has to be controlled and if necessary adjusted (Kajüter, 2003). Second, companies and supply chains operate in a dynamic environment. Circumstances and risk exposure are constantly changing. New risks have to be identified and assessed in order to implement appropriate responses. Alternatively, established risk responses might become redundant as certain risks vanish (Waters, 2007).

According to van Baalen et al. (2008), a supply chain monitoring and control loop consists of six basic processes. As indicated in the discussion on risk identification, these processes need to be applied to the operational, tactical, and strategic level.

1. Collection and storage of actual data from the supply chain
2. Definition and storage of targets
3. Processing of data and comparison of actual and target data
4. Communicating a trigger if the deviation of actual and target data exceeds threshold
5. Definition and storage of response procedures
6. Processing trigger and inducing response procedure

All these processes can be related to the SCRM framework. Target setting (process two) corresponds to the definition of a supply chain risk strategy. The collection of actual data from the supply chain (process one) relates to risk identification. Risk analysis is reflected in the third general process. Comparing actual and target data translates to matching the actual risk exposure with the risk limits as defined in the risk strategy. Only if the expected value of the risks exceeds the cost of mitigation, a response is triggered (process four). Processes four to six are consistent with responding to risks in the SCRM framework. Responses are specifically designed and implemented to successfully mitigate the corresponding risk sources (processes five and six).

The monitoring and control loop can be performed periodically (e.g. annually) or ad-hoc whenever there are major changes to the business environment (Waters, 2007; Kajüter, 2003). It is not always necessary to go through all stages of the control loop, i.e. the entire SCRM framework. In order to not unnecessarily tie up financial or other resources, the framework can be suspended at any given stage if e.g. the risk analysis process does not reveal any changes to the risk exposure (Mullai, 2009). However, the process has to be re-started or re-entered regularly (Mullai, 2009; Waters, 2007; Kajüter, 2003).

The discussion of SCRM presented in this chapter leads to the first two research questions.

RQ 1: What are the main risks and their sources faced by freight forwarders in the cross-border maritime container transport?

RQ 2: What are the information needs of freight forwarders to manage the risks of cross-border maritime container transport?

2.2 Port Community Systems

In 2006, Rodon and Ramis-Pujol identified “only a handful” (p.2) of studies concerning PCSs. By 2011, research is still of exploratory nature. A Google scholar search of the exact phrase “port community system” returned 116 results only. Beyond that, most of these publications solely mention PCSs. Papers that study PCSs are descriptive by nature. The following discussion is, therefore, based on a developing body of literature regarding PCSs as well as on general literature regarding inter-organizational ISs and electronic data interchange.

Ports can be defined as “spatial, logistical, financial, and informational hubs that serve the interests of supply chains as well as geographical regions and nation states” (Van Baalen et al., 2008, p.8). However, they are no single entities, but rather composed of a number of public and private companies that make up a port community (Wrigley et al., 1994). Therefore, a port community can be defined as "an alliance of organizations which together perform logistical and related functions in a particular port, and thereby provide vital enabling services for economic activities within the local and nearby regions" (Wrigley et al., 1994, p.224). At the center of such an alliance stand the port authority (PA) and customs. Organizations operating around them depend on each other and vary in function. They include: shipping lines, terminal operators, forwarders, importers, exporters, and various others, all involved in conducting trade. Large logistics players usually have associations with multiple ports (Wrigley et al., 1994). For the purpose of this thesis, the term "port" implies the entire port community.

The complexity and dynamics of supply chains as well as their management have already been discussed in chapter 2.1. Trends in supply chain management in combination with world-wide economic growth lead to annually increasing trade volumes (Van Baalen et al, 2008; Teo et al., 1997). Simultaneously, safety and security, as subsets of risk management, have gained in importance (Van Baalen et al., 2008). Ports' operational and economic success is largely determined by these developments which go beyond the control of port management (Van Baalen et al., 2008). In today's highly integrated global supply networks, competition is not between ports, but rather between the supply and value chains they operate in (Vitsounis and Pallis, 2010). Moreover, ports' location characteristics have become less important. Instead, the value ports add and the services they offer to their supply and value chains form competitive advantages (Van Baalen et al., 2008). According to McMaser and Wastell (2005) and Wrigley et al. (1994), the standardization, automation, and rationalization of inter-firm information exchanges represent added value. Furthermore, port community members are reliant on each other's information to operate effectively (Long, 2009). Given that, "competition between ports depends progressively on the capability to foster information sharing between participants in port networks" (Van Baalen et al., 2008, p.18). Consequently, many ports are implementing PCSs or have already done so (Mila, 2009).

2.2.1 Definition

According to van Oosterhout et al. (2007), PCSs "act as an information broker between the different actors and fulfill the following functions: information aggregation, conversion and relay" (p.6). Rodon and Ramis-Pujol (2006) define a PCS as "an electronic platform that connects the multiple systems operated by a variety of organizations that make up a seaport community” (p.1). Van Baalen et al. (2008) also apply this definition and further accentuate that PCSs “are used to standardize message exchange among stakeholders and centralize all community information as much as possible” (p.102).

2.2.2 History

The need for central messaging infrastructures which support the translation of messages from one format to another was first recognized in the 1970s and ‘80s (Van Baalen et al. 2008; Brodmerkel, 1978). The development of PCSs shows different patterns across port communities. In some cases, public authorities tried to develop and implement PCSs following a top-down-approach, while in others private organizations cooperated to introduce such systems bottom-up. In all ports, however, customs as well as other port authorities supported the idea to centralize and standardize information exchange by becoming launching customers of the new systems. Since their first introduction, PCSs have continuously been adapted to the needs of increasingly complex supply chains as well as to changing national and international regulations (Van Baalen et al., 2008).

2.2.3 System Architecture

The architecture of an IS determines its capabilities to a large extent. For that reason, the author briefly touches upon the design of PCSs. System architecture can be described “as the set of relations between the components of a system” (Van Baalen et al., 2008, p.128). Following van Baalen et al. (2008), the discussion is organized along the processes of a monitor and control loop as discussed in section 2.1.4: data capture, data storage and transfer, and data processing.

Data can be captured in two ways. First, users can make data available through manual input or transfer from internal ISs. Second, data can be retrieved directly from supply chains. This refers to e.g. radio frequency technologies which track the position of a container and automatically feed the relevant data into ISs. Currently, PCSs depend mostly on the first option. Direct data capturing, however, is promising, especially regarding the physical flows in supply chains (Van Baalen et al., 2008).

Regarding data storage, PCSs function as hubs that connect different port community members. Hubs can be classified as private hubs and central orchestration hubs. Private hubs are usually implemented by dominant players of a supply chain and facilitate 1:n connections. In contrast, central orchestration hubs are processed focused and owned by independent operators. They facilitate n:1:m connections (Van Baalen et al., 2008). Given that, most PCSs can be classified as central orchestration hubs. They work as information brokers that provide the appropriate information to authorized users (Van Baalen et al., 2008; Van Oosterhout et al., 2007). Apart from the technical architecture, PCS operators also have to decide on a data exchange technology. Messages can be exchanged in different formats (e.g. EDIFACT, XML) by using numerous services (e.g. ftp, e-mail). Data exchange technology varies across PCSs (J. Weishaar, personal communication, February 3, 2011; Van Baalen et al, 2008; Rodon and Ramis-Pujol, 2006).

Regarding data processing, PCSs act and react based on the results of data processing. Examples are alert messages and status reports (J. Weishaar, personal communication, February 3, 2011). Van Baalen et al. (2008) take it one step further and include inter-organizational planning. Successful inter-organizational system support intra-enterprise as well as inter-enterprise planning. The first refers to organizations using processed data (external information) to adjust their own planning accordingly. In the latter case, information processed by an inter-organizational system facilitates arranged planning between two or more adjacent enterprises. Extending that idea to the entire supply chain is not easy for reasons discussed in chapter 2.1 (i.e. supply chain complexity). A future model, therefore, is IOS enabled chain synchronization and inter-enterprise planning. General planning autonomy is left with the individual enterprises while PCSs are used for information exchange and high-level synchronization and planning (Van Baalen et al., 2008).

Comparing PCSs among the discussed dimensions, two generations of systems can be distinguished. Generation I architectures are common for older systems and connect numerous bilateral information exchanges to a complex web of applications. In contrast, generation II systems comprise a central database and fitted port community platform. Instead of creating a complex web of bilateral information exchanges, processes are combined in modules. Organizations use the port community platform to subscribe for relevant modules. Both generations facilitate and centralize information exchange between port community members. The main advantage of generation II PCSs is their potential to provide additional application modules. They are most suitable for extensive data processing (Long, 2009; Van Baalen et al, 2008; Smit, 2004).

2.2.4 Characteristics

As indicated above, PCSs are multifunctional and virtually open-ended. Depending on their initiators, the characteristics of the port communities, and other factors, PCSs serve different needs and consequently offer a varying set of applications (Van Baalen et al., 2008). Van Baalen et al. (2008) characterize PCSs as "holistic, geographically bounded information hubs in the supply chain that primarily serve the interest of a heterogeneous collective of port-related companies" (p.171). In smaller port communities, PCSs tend to serve as extensions to the in-house systems of major players, offering company-specific applications. In large ports, however, they have a more neutral role as a true information broker. Company-specific functionalities are rare. The average number of companies using the system was found vary between 800 and 52,000 (Van Baalen et al., 2008). Mila (2009) summarizes a study undertaken by the International Association of Ports and Harbors in 2007. In order to characterize the average PCS, they questioned all member ports regarding their systems' main features. The resulting average PCS was implemented by the PA before 1995. The system is operated by a private company. Its use is charged and not mandatory. Further, the PCS is connected to its users' legacy systems and offers information services as well as documentary exchange services (Mila, 2009).

Long (2009) and Gustafsson (2007) emphasize fundamental prerequisites for the success of PCSs. First, members of the port community need to agree on the system's requirements. A true sense of community and a general feeling of involvement need to be established. Different prerequisites and interests of e.g. major multi-national companies and one-person service providers need to be overcome. The success of a PCS can only be maximized if all member groups of the port community realize benefits and thus share information. Second, a PCS should not duplicate functions that are already existent in other systems, but rather focus on general operational processes. Third, sensitive information needs to be safeguarded.

PCSs offer two main benefits. First, they facilitate the reporting to authorities (Gustafsson, 2007; Rodon et al., 2007). Information will be distributed to the respective authorities in compliance with effective directives. This is of particular importance since supply chain performance is increasingly driven by governmental regulations (Van Baalen et al., 2008). Second, PCSs enhance the coordination of operations at the physical, information, and financial layer (Van Baalen et al., 2008; Gustafsson, 2007). Supply chain flows are facilitated between both, parties that already have business relationships and parties that have never shared information before. In other words, cooperating and competing firms are bound together. (Van Baalen et al., 2008). In general, PCSs enhance the efficiency and effectiveness of interactions between port community members and thus help to reduce processing costs (Rodon and Ramis-Pujol, 2006). All this is achieved by providing a central information network which increases visibility and data quality (Mila, 2009; Gustafsson, 2007). Benefits regarding data quality are measured along four categories: intrinsic, accessibility, contextual, and representational (Van Baalen et al., 2008).

The intrinsic category of data quality is related to data accuracy, objectivity, and reputation (Van Baalen et al., 2008). PCSs enhance the accuracy of information by checking for input mistakes (J. Weishaar, personal communication, February 3, 2011; M. van der Velde, personal communication, March 9, 2011; Rodon and Ramis-Pujol, 2006).

Data accessibility is enhanced by centralizing community information as much as possible (Van der Velde, 2011; Van Baalen et al., 2008). Moreover, the structured approach of information exchange via PCSs supersedes existing informal information channels (Gustafsson, 2007). In general, information is detached from personal communication and thus made available on a 24/7 basis (J. Weishaar, personal communication, February 3, 2011; M. van der Velde, personal communication, March 9, 2011). Moreover, PCSs ensure data security by managing access rights and tracing unauthorized access attempts. Information is only made available to authorized members of the port community (M. van der Velde, personal communication, March 9, 2011; Long, 2009).

The contextual category of data quality comprises the dimensions of data relevancy, value-added, timeliness, completeness, and data complexity (Van Baalen et al., 2008). Besides assuring accuracy, input validations performed by PCSs also enhance data relevancy and completeness (J. Weishaar, personal communication, February 3, 2011; M. van der Velde, personal communication, March 9, 2011). Moreover, PCSs help to reduce data complexity by capturing information once and reusing it for different applications. The need to re-type data is avoided. This concept is referred to as “single submission” (Van der Velde, 2011; Long, 2009; Rodon and Ramis-Pujol, 2006). The application of ISs makes captured data instantly available (i.e. real-time information) to all authorized users (Rodon and Ramis-Pujol, 2006). Moreover, information becomes more transparent as changes can be traced back to individual organizations or users (Long, 2009; Rodon and Ramis-Pujol, 2006). The benefits of PCSs go beyond data capture, storage and transfer. Regarding data processing, PCSs enhance the automation of core workflows and processes based on captured information (Van der Velde, 2011; Mila, 2009). Two further value-adding features of PCSs have already been discussed regarding system architecture – alert messages/status reports and collaborative planning.

The final category of data quality is called representational. Its main dimensions are data interpretability, ease of understanding, concise presentation, and consistent representation (Van Baalen et al., 2008). In general, PCSs standardize the message exchange among port community members. All companies involved use the same language in terms of data formats and transmitting services (Van Baalen et al., 2008). Further, PCSs harmonize the representation of data by applying uniform system layouts (M. van der Velde, personal communication, March 9, 2011; A. Long, personal communication, March 14, 2011).

The above presented characteristics and benefits of PCSs could also be arranged along the basic process steps of the monitor and control loop. Therefore, PCSs support business requirements that arise from that loop. Examples are: data capture and analysis, communication of planning data and key performance indicators, creation of alert messages, and activation of response procedures (Van Baalen et al., 2008; M. van der Velde, personal communication, March 9, 2011).

2.2.5 Information Content

The information content, i.e. specific services and applications, of PCSs largely depends on local circumstances (Van Baalen et al., 2008). Among the few functionalities offered by virtually every PCS is the processing of customs declarations (Long, 2009). Besides that, limited information concerning the information content of PCSs is provided in the academic literature. According to Wrigley (1994), PCS services center around: obtaining the asset status, providing flexibility in supply chain flows, and facilitating the integration with other economic sectors. In order to gain a deeper understanding regarding the information content of PCSs, the author analyzed the services offered by six European PCSs. The results for the PCSs of the ports of Rotterdam, Bremen, Hamburg, Felixstowe, Le Havre, and Barcelona are summarized in Appendices 1-6. The author combined related services in broader service categories. Amongst these are: government declaration (including customs) and dangerous goods, import and export, vessel information services, rail and road related services, and miscellaneous services. For a detailed list of services, the author refers to Appendices 1-6. Applying the different services offered by the analyzed PCSs to the supply chain flows, allows the author to draw conclusions regarding the information content of PCSs. Table 1 provides an overview of the information content of PCSs from a port community perspective as well as from the perspective of the entire supply chain. This is also the order of discussion following Table 1.

		Perspective of analysis	
		Port community	**Entire supply chain**
Supply chain flow	**Physical**	◑	○
	Information	●	◔
	Financial	◔	○

○	none
◑	medium
●	high

Table 1, Information content PCSs

Port community perspective: Regarding the physical flow of goods, several PCSs offer features to organize the further transportation of imported goods via barge, road, and rail. As such services are not applicable to all physical flows in ports, the information content of PCSs regarding this supply chain flow is medium. In contrast, the information content regarding information flows is high. It is a PCS's core task to map the physical transport of goods in form of digital messages and to report status changes to relevant users (J. Weishaar, personal communication, February 3, 2011). This relates to all necessary information flows on a transaction (B2B) as well as a regulatory (B2G) level (Willis and Ortiz, 2004). The information content regarding financial flows is low. Some PCSs do provide information about payment status but do not allow the users to conduct payments.

Entire supply chain perspective: From this perspective, the information content of PCSs varies with the complexity of supply chains. However, general conclusions are possible. The information content is the highest regarding information flows. As PCSs enhance information flows on the import as well as the export side of the supply chain, the author classifies the information content as medium. In contrast, physical and financial flows are basically not supported from the perspective of the entire supply chain.

2.2.6 Strengths, Weaknesses, Opportunities, and Threats (SWOT)

Figure 6 summarizes a SWOT analysis of PCSs. As strengths have already been discussed in the section regarding characteristics of PCSs, the author only consolidates them at this point.

Strengths	Weaknesses
• Independent operator • Reporting to authorities • Coordination of operations • Reduced operating costs • Increased visibility • Input validation for accuracy, relevance, and completeness • Centralization of port community information • Elimination of informal information channels • Enhanced data security through access mgmt. • Reduced data complexity, “single submission” • Real-time information • Increased transparency • Automation of core work flows and processes • Standardization of data formats and transmitting services	• Localized solution • Indirect nature of most benefits • Use of system not mandatory • Uneven distribution of benefits • Fundamental differences in governance models across PCS operating companies • Unwillingness of port community members to share information
Opportunities	**Threats**
• Extension to the entire supply chain • Intensified cooperation among PCSs • Extension of service portfolio • Increased importance due to regulatory changes • Increased standardization of technologies in hinterland communication	• Possible shift from PCSs to supply chain-wide IOSs • Information theft and data manipulation

Figure 6, SWOT analysis PCSs

One of the main weaknesses of PCSs is that they only present localized solutions. This may reduce the willingness of some port community members to integrate as they might aim at a standardized world-wide logistics platform which facilitates information exchange along their entire supply chain (Rodon and Ramis-Pujol, 2006). Another possible weakness of PCSs is the indirect nature of their benefits. They can only be realized in the long run and depend on the achievement of a critical mass of system subscribers. Below such a critical mass, costs related to the centralization and standardization of information flows exceed the associated benefits (Van Baalen et al., 2008). Further, the use of PCSs is not mandatory by law. Only a few PAs encourage the use of PCSs through the application of different harbor dues for users and non-users. This might impede the achievement of a critical mass (A. Long, personal communication, March 14, 2011; Van Baalen et al., 2008). Moreover, the benefits associated with the use of PCSs might be distributed unevenly. Some companies provide a lot of information without receiving value-added. Given that, port community members might decide not to integrate with the system. This is especially relevant for small companies and may prevent the development of an advanced technological infrastructure. Further, the achievement of a critical mass in operations is hampered (Van Baalen et al., 2008; Rodon and Ramis-Pujol, 2006). Another possible weakness of PCSs is the fundamental difference in governance models across PCS operating companies. This may hinder the development of PCSs in global supply chains (Van Baalen et al., 2008). Finally, port community members might be unwilling to use the system because of skepticism regarding data security (Van Baalen et al., 2008).

The external environment provides numerous opportunities for PCSs to overcome their weaknesses and consequently strengthen their position in maritime transport. First, PCSs could expand to the entire supply chain. This would most probably be achieved through an integration of all information technology systems along the supply chain. Second, cooperation between PCSs might be enhanced. National, continental, or even world-wide PCSs might desirable. In both cases a further standardization of interfaces and processes would be required. Moreover, the requirements of and benefits for each company would have to be outlined and agreed on in advance (J. Weishaar, personal communication, February 3, 2011; Mila, 2009, Van Baalen et al., 2008). Third, PCSs could extend their service portfolio in order to further facilitate collaborative planning and inter-organizational data processing (Mila, 2009; Van Baalen et al., 2008). Fourth, regional or national governments might enhance the importance of PCSs by enforcing regulatory changes in the systems’ favor (Van Oosterhout et al., 2007). Finally, the market power of PCSs might be enhanced through the standardization of information technology in hinterland communication. Port community systems are very active in hinterland operations and would therefore be the right information platform for such standardization. Above that, many hinterland companies are strongly associated with port communities. Depending on the applied scope of the port community definition, most hinterland companies become a part of the port community (Van der Velde, 2011; Van Baalen et al., 2008).

The above presented opportunities relate to current debates among practitioners and academics. It is unclear whether PCSs, in order to become more competitive, should strengthen their territorial or rather their network embedding. Further, no consensus has been reached regarding the question whether PCSs are going to compete against each other or collaborate in order to create a bigger system (Van Baalen, 2011; Van der Velde, 2011)

The literature review has identified two major threats for PCSs. First, the market power of multi-national logistics providers might initiate a shift towards supply chain-wide inter-organizational systems. PCSs might be driven out of the market or taken over by more powerful IS providers (J. Weishaar, personal communication, February 3, 2011). Second, PCSs are always vulnerable to external threats to data security (Rodon et al., 2007).

The discussion of PCSs amounts in the final research questions of this thesis.

RQ 3: What information is provided by PCSs to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

RQ 4: What information is provided by alternative information systems to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

Research questions three and four are relevant for all SCRM processes: identifying risks, analyzing risks, and responding to risks.

The overall topic of this thesis will be presented as research question five. The answers to the four preceding research questions will determine the results of this thesis, i.e. the answer to the question:

RQ 5: What is the role and scope of PCSs in providing data that enhances SCRM of freight forwarders regarding the cross-border maritime container transport?

3 Research Methodology

The topics of SCRM and PCSs are comparatively new and, therefore, lack established theories and definitions. For that reason, the research conducted for this thesis is theory grounded and exploratory (Seuring, 2005; Norrman and Jansson, 2004). Different authors argue that field research in the form of case studies is an appropriate approach to conduct exploratory investigations (Sodhi et al., 2011; Seuring, 2005; Yin, 2003a). Case studies offer the ability to investigate real life contexts in which researchers have little control over events (Yin, 2003a, b). Moreover, they enable researchers to ask "'how' or 'why' questions" (Yin, 2003a, p.1).

For the purpose of this thesis, a case study of freight forwarders provides valuable insights on processes and the associated risks in the cross-border maritime container transport. Further, it enables the author to penetrate the issue of SCRM from the perspective of the focal group.

Empirical data is collected through semi-structured interviews undertaken by the author with representatives from freight forwarders, Portbase as a PCS operator, and Dutch customs. Copies of the questionnaires are sent out to the interviewees prior to the actual interview. After the interview, the author transliterates the answers and obtains the consent of the interviewees regarding the correctness of the protocol. The transliterations are provided in Appendices 11-18. The use of multiple interview partners from different supply chain members and trade facilitators enables the author to triangulate and thus verify the results and implications (Seuring, 2005). In other words, construct validity is improved (Yin, 2003a). Overall, the author conducts eight interviews with representatives from six companies and institutions. An overview of the interview partners is provided in Table 2.

In a first step, the author identifies processes of freight forwarders regarding the cross-border maritime container transport, i.e. an atomistic perspective of SCRM is applied (refer to sections 2.1.3 and 2.1.4). For the purpose of this thesis, "processes" comprise physical, information, and financial supply chain flows. Moreover, the author distinguishes between import and export processes.

In a second step, risks and their sources are derived from the identified processes. Of relevance are risks that affect the physical, information, and financial flows of the cross-border maritime container transport. Risk sources are organizational, network-related, or environmental and take effect on three levels: operational, tactical, or strategic (refer to section 2.1.4).

Company/institution	Interview partner(s)	Job position	Risk mgmt/ operations	Interview date
Kühne+Nagel	Roman Balog	Manager, Short Sea	Risk mgmt	July 21, 2011
Kühne+Nagel	Siegfried Forche	Senior Vice President, Seafreight	Operations	July 13, 2011
DHL Global Forwarding	Peter Sonnabend	Global Head of Ocean Secure, Ocean Freight	Risk mgmt	July 8, 2011
DHL Global Forwarding	Johan van Wensveen	Account and Development Manager, Global Operational OFR	Operations	July 14, 2011
Hellmann Worldwide Logistics	Robert Knief	Product Manager, Seafreight	Operations	July 19, 2011
Seacon Logistics	Johan Vosbeek	Sales Representative, Overseas	Operations	July 18, 2011
Portbase	Marten van der Velde Hans Rook	Strategy & Business Development Manager Product Manager	n/a	July 12, 2011
Customs Administration of the Netherlands	Frank Heijmann Pieter Verbakel	Head of Trade Relations Chief Inspector	n/a	July 12, 2011

Table 2, Overview interview partners

In a third step, the author describes the information needs of freight forwarders regarding SCRM in the cross-border maritime container transport.

In a fourth step, the information content of PCSs is analyzed. The author relates services offered by PCSs to the main steps of SCRM as discusses in section 2.1.4, i.e. identifying risks, analyzing risks, and responding to risks. A similar analysis is prepared for alternative IT systems. It is, however, not of the same scope as the one regarding PCSs, since other IT systems are not in the focus of this thesis.

In a final step, the author compares the information needs of freight forwarders with the information content of PCSs and other IT systems. It is determined to what extent PCSs can provide freight forwarders with relevant data concerning SCRM, i.e. identification, analysis, and response. For each process step of the SCRM framework, the author also investigates how other IT systems – alone or in combination with PCSs – can facilitate SCRM.

The following three sections discuss the relevance of the selected interview partners in detail.

3.1 Freight Forwarders

Freight forwarders represent this study’s focal group. Therefore, target interviewees within freight forwarders are of two types: a representative from the division in charge of risk management or compliance and a second company representative from an operational division. Interviewing two representatives per freight forwarder further improves the research design. Findings can be validated not only between but also within freight forwarders.

Interviews with representatives from risk management or compliance divisions are focused on the general risk management approach of freight forwarders. It is of main interest what ISs are used for SCRM and what purpose these systems serve. The questionnaire for risk management specialists of freight forwarders is provided in Appendix 7.

In contrast, operations specialists are questioned about the general processes freight forwarders are involved in concerning the cross-border maritime container transport. Further, they are asked to describe risks and the relevant risk sources associated with the identified processes. Given that, information needs for successful SCRM are derived together with the interviewee. Finally, it is of interest how the respective freight forwarder tackles SCRM from an operational perspective and what IT systems are used regarding the different process steps of the SCRM framework. The questionnaire for operations specialists of freight forwarders is provided in Appendix 8.

Data regarding freight forwarders comes from interviews with four companies. In total, the author interviewed six unique representatives (compare to Table 2).

The composition of the freight forwarder sample was mainly driven by the author’s ambition for the results to incorporate size effects. In other words, possible differences in the role and scope of PCSs in providing data for risk management between large and small forwarders are taken into consideration. Another selection criterion for freight forwarders was their involvement in the European research project CASSANDRA or in comparable projects. Thereby, their relevance for and interest in this case study is ensured. Based on these selection criteria, the author contacted selected companies from the body of freight forwarders operating in the port of Rotterdam.

The final sample of freight forwarders comprises Kühne+Nagel, DHL Global Forwarding, Hellmann Worldwide Logistics, and Seacon Logistics. In that, Kühne+Nagel and DHL Global Forwarding represent the world’s leading sea freight forwarders based on yearly volumes measured in TEU. Further, both companies are engaged in the CASSANDRA project. In contrast, Hellmann Worldwide Logistics and Seacon Logistics are of substantially smaller scale (compare to Table 3). While Seacon Logistics as a Dutch freight forwarder is an active participant of the CASSANDRA project, Hellmann Worldwide Logistics is engaged in a comparable project. Together with Eurogate and EADS Astrium, Hellmann Worldwide Logistics formed a workgroup to develop a safety and security system regarding the cross-border maritime container transport.

Table 3 presents selected financial and operational data of each sample freight forwarder.

	Kühne +Nagel		DHL Global Forwarding, Freight		Hellmann Worldwide Logistics		Seacon Logistics	
	2009	2010	2009	2010	2009	2010	2009	2010
Revenue [EUR m]	**11,700**	**16,251**	**11,234**	**14,341**	**2,470**	**2,650**	**85**	**103**
Thereof sea freight	5,090	7,216	2,450	3,446	776	n/a	17	27
EBIT [EUR m]	**399**	**614**	**174**	**383**	**n/a**	**n/a**	**4**	**3**
Thereof sea freight	228	334	n/a	n/a	n/a	n/a	1	1
Return on Sales	**3.4%**	**3.8%**	**1.5%**	**2.7%**	**n/a**	**n/a**	**4.1%**	**2.9%**
Return on Sales, sea freight	4.5%	4.6%	n/a	n/a	n/a	n/a	5.9%	3.7%
Sea freight [TEU '000]	**2,546**	**2,945**	**2,615**	**2,772**	**482**	**n/a**	**± 40**	**± 45**
Market position based on TEU	2	1	1	2	n/a	n/a	n/a	n/a
Employees [#, year-end]	**54,680**	**57,536**	**40,331**	**41,359**	**8,652**	**9,228**	**550**	**600**
Thereof sea freight	7,421	7,588	n/a	n/a	n/a	n/a	25	27

Table 3, Financial and operational indicators of freight forwarder sample

3.2 Portbase

Portbase, as the operator of the PCS in Rotterdam, is questioned about how the company estimates its role in providing relevant data for the different process steps of SCRM. Moreover, the interview is used to identify other IT systems which, from Portbase’s point of view, play a vital role in SCRM. The questionnaire for Portbase is provided in Appendix 9.

3.3 Dutch Customs

Dutch customs represent a third relevant participant in the cross-border maritime container transport. Main goal of the interview is an independent opinion on the SCRM approach of freight forwarders concerning the cross-border maritime container transport. Further, the interviewee is questioned about what ISs are used for the data transfer regarding IT-supported customs procedures between port companies and customs authorities. The questionnaire for the customs authority is provided in Appendix 10.

4 Results

4.1 Freight Forwarding Business

The results of this thesis are based on a merchant haulage scenario. This implies that the transport of goods is organized by forwarders rather than shipping lines or agents as it would be in a carrier haulage scenario (Van Baalen et al., 2008; Virtuele Haven, 2001).

The freight forwarding business can be traced back as far as the beginning of the last century. Its main service offering was the consolidation of less-than-carload freight into carloads in order to benefit from lower shipping rates (Barton and McGehee, 1942). Since then, the freight forwarding business has advanced substantially to "provide a variety of functions to facilitate the movement of cross-border shipments" (Murphy et al., 1992, p.2). In addition to the more traditional functions related to the transportation of goods, freight forwarders have diversified to also offer a large variety of logistical intermediary services – e.g. shared warehousing and distribution solutions, warehouse management systems, value-added services, and supply chain consulting (Brandenburg et al., 2010, Murphy and Daley, 2001). These services, however, lie outside the scope of this thesis. In fact, the author focuses on the traditional functions of seaport freight forwarders. Even though they are different for export and import activities, traditional functions of seaport forwarders include, but are not limited to, obtaining vessel space, arranging pre- and follow-up inland transportation services, paying freight charges, obtaining insurance, organizing customs declarations, preparing relevant documentation (Brandenburg et al., 2010; Murphy and Daley, 2001; Virtuele Haven, 2001).

General processes of seaport freight forwarders regarding the cross-border maritime container transport are described in section 4.1.1.

4.1.1 Processes

The first step in this study is to obtain an understanding of the processes of freight forwarders regarding the cross-border maritime container transport in order to map the main processes. The resulting process model serves as the basis for the subsequent risk analysis. For the purpose of this thesis, "processes" comprise physical, information, and financial supply chain flows. Information flows are further broken down into governance and transaction layers. Following Willis and Ortiz (2004), the governance layer summarizes all inspection and verification activities by governing bodies (e.g. customs) while the transaction layer depicts contractual relationships between all involved supply chain members. Moreover, the author distinguishes between import and export activities.

It is assumed that freight forwarders are involved in the container transport at origin as well as at destination. They take on the cargo responsibility – including the organization of pre- and follow-up transport – and organize customs clearance as well as vessel booking. For the purpose of this thesis, sea-to-sea as well as inland transshipment are not considered. Moreover, the process model assumes full container loads (FCL), which implies that the forwarder is not responsible for stuffing or stripping containers. The role of freight forwarders on import and export side depends on the shipment's Incoterms. However, for the purpose of this thesis, no specific Incoterm is assumed. In fact, the processes are outlined for a business case in which one (branches of the same) freight forwarder organizes export and import of the goods.

Export

In this section, the export processes of freight forwarders in the cross-border maritime container transport are described. The discussion is summarized in a process map (Figure 7). In that, supply chain flows regarding the export of containers are depicted by light grey rectangles while sea transport-related processes on the export side are shown in dark grey. Furthermore, white rectangles surrounded by dashed lines illustrate optional process steps. Concerning information and financial flows, the author distinguishes between incoming and outgoing information/payments. The information/payment provider or receiver is disclosed in parentheses following the process description.

The initial start of the export process is a customer's request to have a container transported from one country to another. In response to the request, freight forwarders make a quotation for the transport and possibly counsel the customer regarding general transport regulations. The official involvement of the freight forwarder in the export process, however, does not start until the customer issues a shipping instruction, including all relevant details concerning the goods and the desired transport schedule. In order to reduce the susceptibility to errors, freight forwarders provide their customers with special shipping instruction forms that have to be completed and transmitted via electronic data interchange (EDI) or e-mail. After checking the shipping instruction for completeness, the freight forwarder books vessel space for the deep-sea transport with a shipping line. The shipping line can either be pre-selected by the customer or chosen by the freight forwarder. In the latter case, freight forwarders select the best suited carrier from a pool of preferred shipping lines. Depending on the strategic relationship between freight forwarder and carrier, business-to-business (B2B) connections, third-party platforms like GT Nexus and INTTRA, or e-mail are used for vessel booking.

If the required vessel space is available, the shipping line provides the forwarder with a booking confirmation comprising all relevant information, like e.g. vessel name, when and where to pick up the empty container, when and where to deliver the full container for shipment, and reference numbers. Subsequently, the forwarder uses this information to book the pre-transport of the container from the exporter to the port of loading (POL). If needed, the forwarder insures container and goods for the transport at this point. However, the insurance is mostly done by the customer (exporter/importer) himself.

The physical movement of containers starts when the commissioned pre-transporter picks up a container at the empty container depot (ECD) of the shipping line and transfers it to the exporter. The shipping line informs the forwarder about the number/ID of the container picked up by the pre-transporter. This information is forwarded to the exporter in order to assure that the empty container is allocated to the corresponding shipping order and consequently stuffed with the correct goods.

The second physical process step is the stuffing of the empty container by the exporter. Even though the freight forwarder, in the case of FCL, is not responsible for and thus not present at the container stuffing, it is a crucial step in the export process and a possible risk source to the forwarder. Upon completion of container stuffing, the container is sealed and the exporter transmits container packing list as well as seal number to the forwarder.

Following the container stuffing, the pre-transporter conveys the container from the exporter to the POL. In parallel, the freight forwarder transmits all relevant container details (Bill of Lading data set) to the shipping line. Depending on the strategic relationship between freight forwarder and carrier, B2B connections, third-party platforms like GT Nexus and INTTRA, or e-mail are used for this. According to effective U.S. (AMS-filing – Automated Manifest System) and European regulations (ENS-filing), freight forwarder or shipping line need to pre-declare containers with customs at the port of destination (POD) at the latest 24 hours before the container is supposed to be loaded on the vessel. Moreover, the freight forwarder, at this point, prepares the export declaration with local customs (POL).

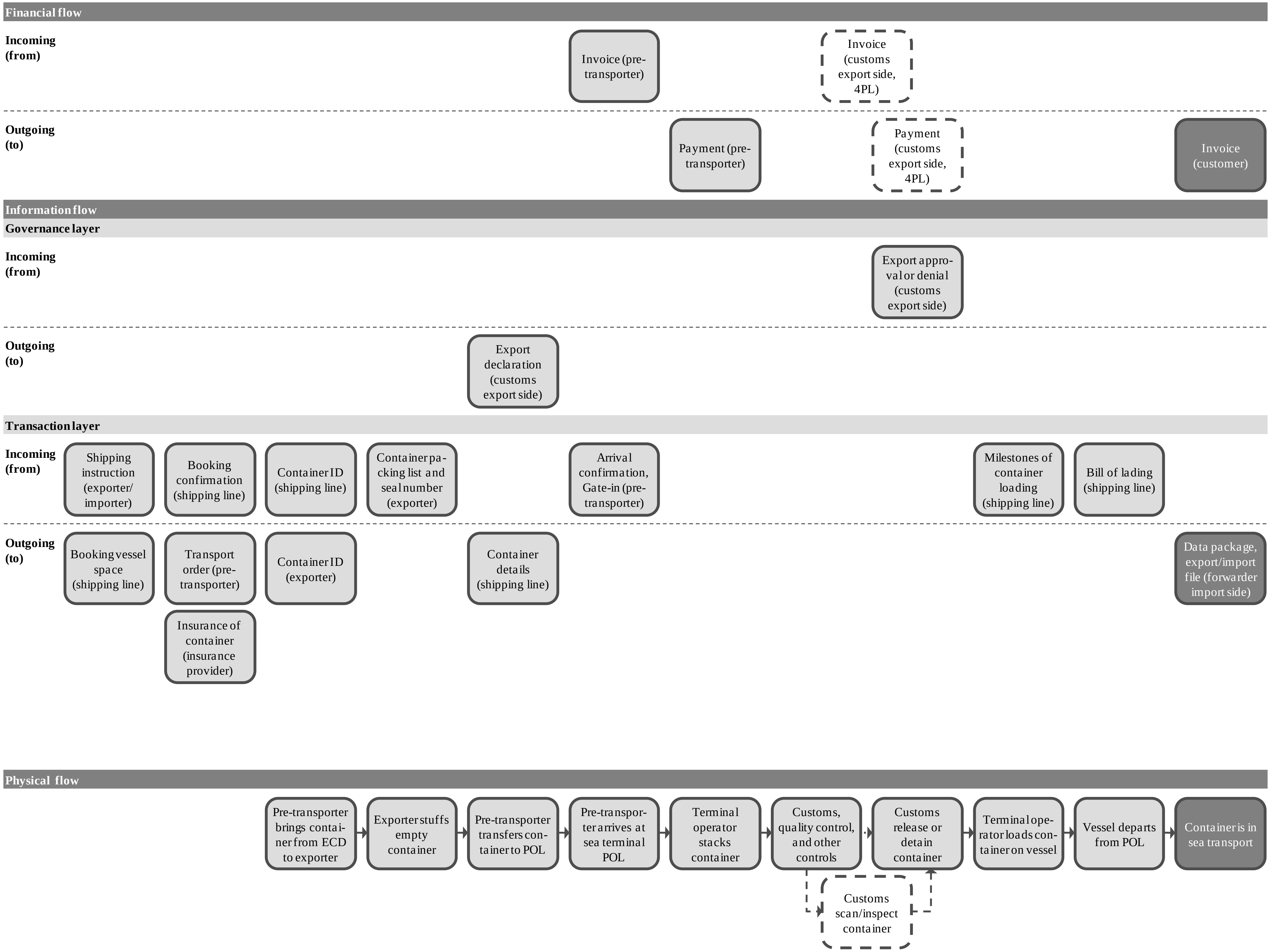
Financial flow
Incoming (from)
Invoice (pre-transporter)
Invoice (customs export side, 4PL)
Outgoing (to)
Payment (pre-transporter)
Payment (customs export side, 4PL)
Invoice (customer)
Information flow
Governance layer
Incoming (from)
Export approval or denial (customs export side)
Outgoing (to)
Export declaration (customs export side)
Transaction layer
Incoming (from)
Shipping instruction (exporter/ importer)
Booking confirmation (shipping line)
Container ID (shipping line)
Container packing list and seal number (exporter)
Arrival confirmation, Gate-in (pre-transporter)
Milestones of container loading (shipping line)
Bill of lading (shipping line)
Outgoing (to)
Booking vessel space (shipping line)
Transport order (pre-transporter)
Insurance of container (insurance provider)
Container ID (exporter)
Container details (shipping line)
Data package, export/import file (forwarder import side)
Physical flow
Pre-transporter brings container from ECD to exporter
Exporter stuffs empty container
Pre-transporter transfers container to POL
Pre-transporter arrives at sea terminal POL
Terminal operator stacks container
Customs, quality control, and other controls
Customs scan/inspect container
Customs release or detain container
Terminal operator loads container on vessel
Vessel departs from POL
Container is in sea transport

Figure 7, Supply chain flows of freight forwarders, export side

In a fourth physical process step, the pre-transporter arrives at the sea terminal in the POL, which has been booked by the shipping line. In other words, freight forwarder and terminal operator have no direct business relationship (contract). Upon arrival at the sea terminal, the pre-transporter notifies (gate-in notification) and invoices the freight forwarder. The invoice is settled based on the terms agreed on in the contract between freight forwarder and pre-transporter.

In a firth physical process step, the terminal operator stacks the container in the POL. It is now available for possible customs checks, other necessary controls, or a physical inspection by the freight forwarder. Subsequently, local customs, based on the export declaration prepared and submitted by the freight forwarder, release or detain the container, i.e. approve or deny export. Container scans or physical inspections (stripping of the container) by local customs are rather seldom regarding the export process. However, if local customs require scans or inspections, the freight forwarder is invoiced for related costs (e.g. transport to and from the scanning location). The freight forwarder settles the invoice and passes on the costs to his customer.

If local customs clear the container for export and customs at the POD do not announce any import restrictions based on the 24-hour pre-declaration, the terminal operator loads the container on the deep-sea vessel. The freight forwarder is provided with time stamps (milestones) regarding the container loading process by the shipping line via B2B connection, GT Nexus, or INTTRA. A direct B2B communication between freight forwarder and terminal operator is seldom as the two parties have no direct business relation.

As a final physical process step regarding the container export, the deep-sea vessel leaves the POL. After vessel departure, the shipping line provides the freight forwarder with the signed Bill of Lading.

While the container is in sea transport, numerous information and financial flows take place. Under the assumption that the freight forwarders on export and import side are represented by the same company, a data package (export/import file) is transmitted from the forwarder's local branch at POL to another one at POD. The data package includes master and house Bill of Lading, container packing list, commercial invoices regarding the sale of goods, and other necessary certificates. Data transmission between two branches of the same freight forwarder can be fully automated if the transport is organized for a definite seller and buyer. In that case an express Bill of Lading is issued. Such a Bill of Lading cannot be changed and is usually used for intra-company transports. Its final character makes a physical transmission of the Bill of Lading via mail unnecessary. Instead, the data is transmitted electronically and the Bill of Lading can be printed in the POD. If, however, no express Bill of Lading is issued, a physical transmission of the master Bill of Lading via mail is inevitable. This is also the case if goods are shipped to certain countries like e.g. Argentina or Brazil.

If the freight forwarders on export and import side are represented by different companies, the data package has to be transmitted via exporter (seller) and importer (buyer). It is transferred from the freight forwarder on the export side to the exporter, who forwards it to the importer before it is finally made available to the freight forwarder on the import side. Usually, banks are involved in that process to ensure payment for the goods sold from the exporter to the importer.

Besides the exchange of relevant data between the exporting and importing side, the vessel travel time is also used by the freight forwarder to prepare the invoice for his customer.

Import

In this section, the import processes of freight forwarders in the cross-border maritime container transport are described. The discussion is summarized in a process map (Figure 8). In that, supply chain flows regarding the import of containers are depicted by light grey rectangles while sea transport-related processes on the import side are shown in dark grey. Furthermore, white rectangles surrounded by dashed lines illustrate optional process steps. Concerning information and financial flows, the author distinguishes between incoming and outgoing information/payments. The information/payment provider or receiver is disclosed in parentheses following the process description.

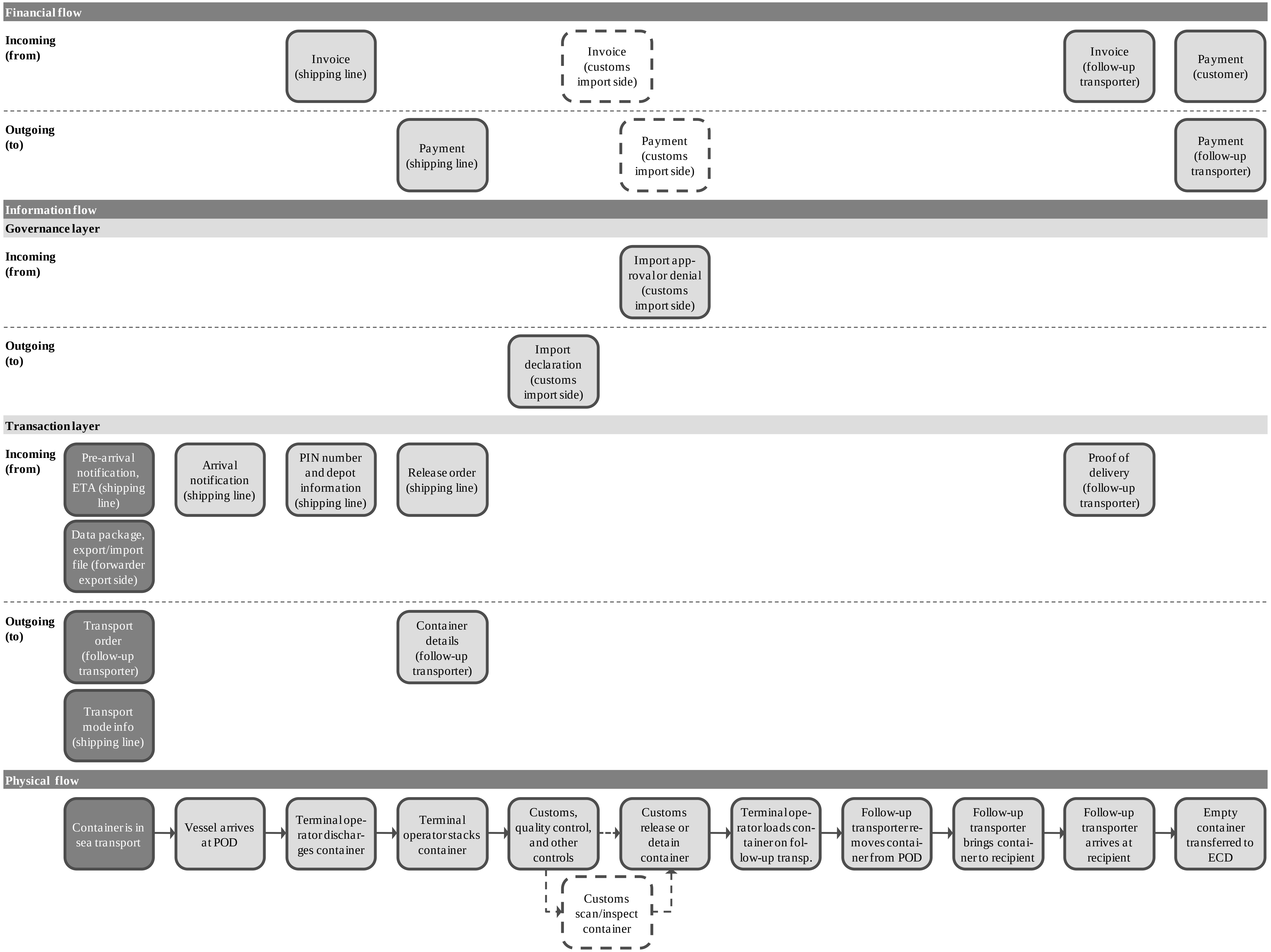
Financial flow
Incoming (from)
Invoice (shipping line)
Invoice (customs import side)
Invoice (follow-up transporter)
Payment (customer)
Outgoing (to)
Payment (shipping line)
Payment (customs import side)
Payment (follow-up transporter)
Information flow
Governance layer
Incoming (from)
Import approval or denial (customs import side)
Outgoing (to)
Import declaration (customs import side)
Transaction layer
Incoming (from)
Pre-arrival notification, ETA (shipping line)
Data package, export/import file (forwarder export side)
Arrival notification (shipping line)
PIN number and depot information (shipping line)
Release order (shipping line)
Proof of delivery (follow-up transporter)
Outgoing (to)
Transport order (follow-up transporter)
Transport mode info (shipping line)
Container details (follow-up transporter)
Physical flow
Container is in sea transport
Vessel arrives at POD
Terminal operator discharges container
Terminal operator stacks container
Customs, quality control, and other controls
Customs release or detain container
Terminal operator loads container on follow-up transp.
Follow-up transporter removes container from POD
Follow-up transporter brings container to recipient
Follow-up transporter arrives at recipient
Empty container transferred to ECD
Customs scan/inspect container

Figure 8, Supply chain flows of freight forwarders, import side

The vessel voyage is the kickoff for forwarder operations on the import side. Most importantly, the freight forwarder receives all necessary information and documentation regarding the shipment (data package) either directly from the forwarder on the export side or from the importer (buyer) of the transported goods. Moreover, the follow-up transport of the container to the importer (buyer) needs to be prearranged while the container is in sea transport. The freight forwarder is continuously updated about the expected time of arrival (ETA) by the shipping line. At some cut-off point, the most recent ETA is used by the forwarder to schedule and organize the follow-up transport. A transport order with all relevant information is sent to the follow-up transporter and the shipping line is informed about the follow-up transport mode. This information is then forwarded by the shipping line to the terminal operator at the POD. Again, there is no direct business relationship between forwarder (import side) and terminal operator at POD.

Upon arrival of the vessel at the POD, the terminal operator discharges the container from the deep-sea vessel and stacks it. Subsequently, the shipping line informs the forwarder about the arrival of the vessel, transmits PIN number and depot information for container pickup and invoices the freight forwarder for the container transport. As soon as the forwarder settles the carriers invoice, he is provided with a release order by the shipping line, without which he cannot receive the container at the terminal. PIN number, depot information, and release order are forwarded to the follow-up transporter who will pick up the container at the sea terminal.

Once the container is stacked at the POD, it is available for possible customs checks, other necessary controls (e.g. veterinary), or a physical inspection by the freight forwarder. The freight forwarder needs to prepare the import declaration with local customs by submitting all relevant data. The import declaration is of much greater interest to customs than the export declaration. At the port of Rotterdam, Dutch customs follow a layered approach and check containers on four layers. On the first and second layer, the involved actors as well as goods and movements are analyzed, respectively. However, it is only on layers three and four that physical checks in the form of scanning and container inspection (stripping) are undertaken. If the customs clearance process is associated with additional costs (e.g. transport to and from the scanning location, import duties), the freight forwarder is initially invoiced, but passes on the expenses to his customer. Based on the results of risk analysis and physical checks, customs release or detain the container, i.e. approve or deny import.

Once the container is cleared for import, the follow-up transporter, upon presentation of all relevant documents, can pick it up at the terminal. Subsequently, the container is dispatched from the POD and transported to the importer (buyer). Upon delivery, the follow-up transporter notifies and invoices the freight forwarder.

As a final physical process step regarding the cross-border maritime container transport, the empty container needs to be returned to an ECD of the shipping line. This transport can be assumed by the follow-up transporter, the importer (buyer) of the goods, or another third- or fourth-party logistics provider. In a final step and depending on the terms of payment, the freight forwarder settles the invoice with the follow-up transporter and collects the money for his services.

4.1.2 Risks

The answers to the question, how exposed forwarders consider their company to risks in the cross-border maritime container transport, average at a score of 1.8 (min=1, max=3), with 1 being a very low and 5 being a very high exposure. This suggests that the freight forwarding business in the cross-border maritime container transport is a rather safe bet. From this perspective, it appears comprehensible that “an active management of risks in the freight forwarding business is not as common as one would think” (R. Balog, personal communication, July 21, 2011). However, in-depth discussions concerning risks and their sources suggest that an average score of 1.8 underestimates the risk exposure of forwarders. Risks are not always denoted as such. Rather, different terms are used (e.g. weaknesses in operations).

Generally speaking, the overall forwarding business is a risk. Even though forwarders themselves are mostly not responsible or legally liable for supply chain disruptions, they are the first point of reference for customs and other regulatory authorities, third-party supply chain members, and, of course, shippers. This is partly because forwarders as business intermediaries represent the only known party to most stakeholders involved in the container transport. Thus, they are always involved in the aftermath of incidents. Even though such involvement might be limited to e.g. insurance claims or investigations, this alone is already associated with certain transaction costs, which forwarders mostly cannot claim. Beyond that, forwarders have to bear other financial and business consequences of supply chain disruptions. The former is related to e.g. possible penalty payments to regulatory authorities, fairness settlements, and costs for dry runs[1]. Examples for the latter are negative impacts on brand image or reputation and lower container volumes. Consequently, everything that could possibly go wrong in the cross-border maritime container transport should be considered a risk to forwarders.

In the following, the author discusses the main risks to forwarders in the cross-border maritime container transport as presented in the interviews. The section is sub-divided to represent the different views on risks from the perspective of all three interest groups: freight forwarders themselves, Portbase as a PCSs operator, and Dutch customs. Thereby, the results' validity can be cross-checked. The author presents all risks along the three supply chain flows: physical, information, and financial. Furthermore, risk sources as well as level of analysis (refer to Figure 3) are also discussed.

Freight Forwarders

Regarding physical supply chain flows, it all comes down to whether transport services are rendered in due time. Unscheduled delays represent deviations from originally planned transport times and affect transported goods as well as containers themselves. Concerning transported goods, forwarders, in case of delays, face demands for compensation by their customers (shippers). Examples range from one-time fairness settlements and alternative transportation to permanently lowered transport rates. In the worst case, shippers lower future contract volumes with the respective forwarders. In addition, forwarders are liable for prearranged transportation and have to pay for dry runs. These business and financial risks cannot be insured. Moreover, other supply chain members are usually not liable for physical delays, even if they have caused them. In other words, forwarders usually do not receive any compensation payments from third parties. Concerning containers, delays in the physical transport possibly result in detention charges. As indicated in section 4.1.1, forwarders rent containers for the maritime transport from shipping lines. If empty containers are not returned within a specified time period, including overdraft, freight forwarders face penalty payments – detention charges from shipping lines. Just as with financial risks related to late delivery of transported goods, detention charges cannot be passed on to third-party supply chain members or customers.

Unscheduled delays and the above discussed associated risks to forwarders have numerous sources. From a network perspective, containers might be misrouted or left behind within the

[1] For the purpose of this thesis, dry runs refer to situations in which unscheduled delays in container transport result in costly chain breaks, i.e. prearranged transport modes are missed but have to be paid for by forwarders.

cross-border supply chain. For example, terminal operators might load or unload wrong containers and shipping lines might discharge containers because of capacity problems even though vessel space has been prearranged by the forwarder. Another network-related source for delayed physical delivery is an unscheduled route change by the carrier due to economic interest on his behalf. Finally and probably most importantly from a network perspective, late delivery of goods and containers can be rooted in customs checks and other necessary inspections. Even if forwarders are accredited by customs as authorized economic operators (AEO), they are never certain whether or not specific containers will be inspected and thus held up. This uncertainty is aggravated by the fragmentation of customs regimes. Repeated inspections can occur if one customs regime does not trust the results of another. Risks regarding additional inspections of containers (e.g. veterinary) are rooted in the fact that they are not necessarily aligned with customs and thus might add on delays.

From an environmental perspective, containers might be delayed because of e.g. weather changes, theft and damage as well as piracy and possible terrorist attacks. Unpredictable weather conditions affect transport times through adaption of vessel speed or shipping routes. Theft, damage, and piracy might result in lengthy investigations or negotiations while in the case of terrorist attacks, goods or entire containers can be confiscated by authorities.

Beyond network-related and environmental risk sources, unscheduled delays are also rooted in risks to information flows which will be discussed below. However, before turning to information flows, the author wants to address two more risks to physical supply chain flows which are not directly related to delays. First, capacity forecasts performed by forwarders in order to reserve container contingents with shipping lines might under- or overestimate future demand. In case of underestimation, forwarders might not be able to handle demanded volumes because of lacking vessel contingents. In contrast, overestimation and thus overbooking of contingents might result in cancellation fees. At this point, the author wants to emphasize that the example of wrong capacity estimations is the first risk factor to the physical flow of goods that lies in the forwarders’ responsibility. In other words, it is the only organizational risk source. Second, smuggling of any kind poses a society risk to forwarders. Even if rooted in the environment, it can negatively affect brand image with clients in particular and society in general. Lower order volumes and tighter transport regulations are possible consequences.

Information flows support the physical transport of containers. According to some interviewees, they have become more important than physical flows themselves. Consequently, risks to information flows indirectly also affect the physical flow of containers. With six major categories, the author identified the most risks for this specific supply chain flow. First, forwarders face the risk of not knowing the actual content of containers. Within Kühne+Nagel, for example, container contents are always only “said to be” (R. Balog, personal communication, July 21, 2011). This is because forwarders in the FCL business organize the container transport but do not supervise stuffing and stripping activities. Instead, they rely on third-party information concerning container contents. Therefore, the risk is clearly network-related, i.e. it stems from the linkages between firms in the supply chain. Information regarding container contents provided to forwarders might either intentionally be wrong in the first place or could be corrupted when transferred from one supply chain member to another. Consequently, forwarders, even if accredited AEO, might not be a trustworthy source of information for customs, making physical scans and inspections of containers inevitable. Such interventions in the physical container flow result in delays. Moreover, not knowing the actual container contents makes forwarders prone to brand and image risks. Once again, incidents might result in lower order volumes or tighter restrictions (e.g. loss of AEO accreditation) for specific forwarders or the entire forwarding business.

A second risk to information flows is the uncertainty regarding ETA of containers at POD. From the moment of vessel departure to the actual arrival at POD, ETAs available to forwarders can only be considered “guestimates” (J. van Wensveen, personal communication, July 14, 2011). Vessel travel times are subject to change due to reasons discussed above. Furthermore and more related to information flows, forwarders do not necessarily receive updates regarding changes of ETA. Moreover, a proactive validation of ETA by the forwarders themselves is complicated by the fact that numerous supply chain members (e.g. carriers, terminal operators, PCSs) provide possible ETAs. Forwarders can never be sure about the validity of the information. Therefore, the organization of follow-up transportation always involves the risk of having to pay for dry runs.

A third risk to information flows is very similar to the one discussed above. Yet, instead of being related to ETAs, it concerns the uncertainty about actual handling times of containers at terminals. As forwarders have no direct business connection with terminal operators, direct B2B connections between the two supply chain members are seldom. Rather, milestones regarding container handling at terminals (e.g. gate-in and gate-out information) are provided by shipping lines. However, crucial status updates might either be made available to forwarders too late or not at all. In general, there is a considerable time slack between the event and the point of time when the corresponding information is provided to the forwarder. Once more, this gives rise to financial as well as business risks. From a financial perspective, forwarders might have to pay for possible dry runs resulting from delayed information and involuntary interruptions in the logistical chain of transportation. A relevant business risk or rather burden is related to labor intensive manual checks of container status. Currently, most forwarders manually trace every container in order to verify ETA and container handling times as provided by third-party supply chain members. This is labor intensive and error-prone. Both risks, uncertainty concerning ETA and container handling times at terminals, are network-related, i.e. the risk source is external to forwarder but internal to the supply chain.

A fourth risk to information flows is the flow of documents. If original documents are needed for e.g. container pick-up at POD, the forwarder at destination faces the risk of not receiving the necessary documents (e.g. Bill of Lading, commercial invoice, certificates of origin, etc.) in time. As a consequence, the transport chain is at risk to be disrupted. However, freight forwarders themselves are only seldom responsible for breaks in the flow of documents. According to Robert Knief of Hellmann Logistics, the probability amounts to less than 1% (Robert Knief, personal communication, July 19, 2011). This is because information channels within forwarders are automated and standardized to a large extent. In contrast, the timely and accurate supply of relevant documentation is a much larger risk factor if third-party supply chain members are responsible for it.

A fifth risk regarding information flows relates to the whereabouts of empty containers. As indicated above, empty containers need to be returned to the shipping line after a specific time period. If empty containers are returned late, freight forwarders face detention charges. Considering an annual container volume of 2.5 million TEU for the leading forwarders, such detention charges could easily sum up to considerable cost factors. However, empty container management including information exchange regarding the whereabouts of the containers shows room for improvement. Interviewees pointed out cases in which shippers have suggested to return containers but did so only with a large delay. On the forwarder side, however, a follow up of empty containers is not possible as they do not receive gate-in information from empty container depots or proof of return from shippers.

A final risk to information flows, as presented in interviews with forwarders, relates to the cumulative effect of years of tightened security requirements in response to numerous severe terrorist attacks in the last decade. AMS- and ENS-clauses have already been discussed. Further examples are the ISPS-Code, TAPA, C-TPAT, and CSI. Additionally, more security regulations are looming on the horizon – e.g. China is currently preparing its own pre-declaration process comparable to AMS and ENS. Therefore, freight forwarders have to stay sharp and continuously adapt to changing legal environments. That alone is already costly and labor intensive. Furthermore, the task is aggravated by varying regulations across jurisdictions as well as uncertain validity periods of new regulations. Arguably, this risk factor could also be related to physical supply chain flows as containers will not pass through the supply chain if certain regulatory requirements have not been fulfilled. However, the aspect of information exchange is more relevant at this point.

Financial supply chain flows represent commercial relationships between the stakeholders involved in the cross-border maritime container transport. Therefore, they are not necessarily in line with physical and information flows. From all interview partners, only Peter Sonnabend of DHL addressed risk factors related to financial flows. Thus, they appear to be of comparatively little importance. First, forwarders face variable costs of shipping due to volatile surcharges (e.g. bunker fuel) imposed by the shipping lines. However, these surcharges cannot easily be passed on to shippers as these usually purchase certain freight volumes (TEU) from forwarders for a fixed price. Consequently, forwarders bear the risk of variable costs of shipping alone. Second, forwarders are exposed to possible payment defaults of customers. The risk is further exacerbated by the fact that containers are not easily distrainable as they, depending on payment terms, might have already moved on in the supply chain before payment defaults can be detected. In general, this risk to forwarders increases with customers' container volumes.

Portbase

The interview with Portbase confirmed the main risk factors to physical supply chain flows as discussed above. Safety- and security-related customs procedures are considered the main sources for unscheduled delays inside the port. However, the interviewees accentuated that delays due to customs checks have become less severe over the last years.

Risks related to information and financial flows were not identified in the interview.

Customs

According to Dutch customs, the main risk factor for freight forwarders is fraud concerning information related to the actual container contents. Freight forwarders receive relevant information from third parties and are not in the position to verify the data or the commodities to be shipped. Even though, buyers and sellers are not necessarily genuine about what they claim to import or export, forwarders do not have a risk management in place regarding safety and security issues. Customs claim that forwarders are not even interested in verifying the data and, therefore, willingly accept risks related to fraud concerning the actual container contents. One reason might be that knowledge about the actual content might oblige forwarders to follow different, possibly more expensive transport regulations. This would automatically lower their profit margins as price alterations towards the customer are impossible due to fixed transport rates. Moreover, the more forwarders know about what is being shipped, the higher their liabilities will become due to civil contracts as well as international treaties (e.g. CMR treaty).

However, a possible paradigm shift is illustrated by the CASSANDRA project. Forwarders begin to show an increasing interest in safety and security issues, including possible fraud concerning the actual container contents. Nevertheless, according to Dutch customs, this is only due to the commercial benefits related to the management of these risks. Forwarders fear that if they are involved in incidents concerning security and safety threats to the society, their reputation might suffer, resulting in lower transport volumes. Moreover, changing safety and security requirements by the government force freight forwarders to get more involved in what they actually forward in containers.

Contrary to safety and security issues, business risks are already being managed actively by forwarders. Customs see the main reason for this in the related commercial benefits. As an example for a business risk, customs refer to unscheduled delays in the physical flow of containers. More risks to physical, information, or financial flows are not pointed out explicitly.

Classification

Concluding and with reference to Figure 3, the author classifies the above discussed risks to freight forwarders along three dimensions: supply chain flows, risk sources, and levels of analysis.

Regarding the first dimension (supply chain flows), the vast majority of identified risks are directly or indirectly related to physical and information flows. Concerning financial flows, however, interviews have only revealed two risk factors which have no connection with PCSs or other visibility platforms. Consequently, the author disregards them in further discussions.

With reference to the second dimension (risk sources), most risk factors are network- or environment-related, i.e. stem from linkages between firms in the supply chain and political, economical, or social aspects, respectively. Only one of the identified risks is internal to forwarders. Therefore, it could be argued that they did not want to admit organizational weaknesses. However, interviews with Portbase as a PCS operator and Dutch customs have not revealed additional risk factors internal to forwarders either.

Finally, regarding level of analysis, most risks affect forwarders at the operational level. In other words, they affect day-to-day business without showing regular patterns. Unscheduled delays are an exemplary risk factor to which forwarders have to react case-specific, i.e. on an operational level. However, if delays or other disruptions occur frequently, they represent reoccurring issues in planning and execution. In such cases, forwarders have to analyze the incidents for patterns and make structural changes. For example, the decision about how much slack to build in forwarding activities in order to avoid repeated payments for dry runs can be considered tactical. Therefore, it can be concluded that most risks have both, an operational as well as a tactical component. However, security requirement-related risks take a special role. They may impact the overall performance of the supply chain by drastically changing the regulatory environment. Consequently, these risks also have a strategic component. Nevertheless, once effective and implemented by supply chain members, the operational component of security requirement-related risks predominates in the long run.

A detailed risk analysis in order to rank the identified risk factors on a risk map (refer to Figure 4) is not possible based on the interview results. The interviewees did not provide the author with sufficient information regarding the relevance of different risks to forwarders.

4.1.3 Information needs

In theory, information needs of forwarders to actively manage supply chain risks are twofold: They require target data as well as real-time performance information. For the purpose of this thesis, target data refers to aspired performance targets of freight forwarders. It is mainly produced by internal planning systems in coordination with customers and third-party supply chain members. Consequently, relevant information is available to forwarders, minimizing their actual information need regarding target data. In contrast, real-time performance information has to be captured from the supply chain, i.e. retrieved from running processes. Most information sources are external to forwarders and thus not under their control. Therefore, the actual information need regarding real-time performance data is rather high. Supply chain risks to forwarders as discussed in the previous section corroborate this fact.

Generally, the need for real-time performance data by forwarders can be satisfied by increasing the visibility in the supply chain, i.e. by providing more accurate real-time data in a timely manner. The higher the supply chain visibility, the more actively forwarders can manage or even prevent relevant risks. In order to be more specific, the author discusses the actual information needs of forwarders with reference to the different physical and information flow-related risk factors as presented in the previous section.

Physical flows

As discussed above, unscheduled delays represent the main risk factor regarding the physical flow of goods. The author identified different possible sources for delays which are related to specific information needs. First, misrouting could be detected and actively managed if the forwarder had available real-time information about the whereabouts of each container. In other words, a reliable real-time track and trace system on container level is required to react to incidents. Second, unscheduled route changes by shipping lines are associated with ETAs of deep sea vessels which will be discussed in the next sub-section. Third, in order to minimize delays related to customs and other inspections, forwarders require timely information regarding which containers need to undergo certain checks. This way, forwarders can coordinate or possibly align inspections and further organize follow-up transport accordingly, i.e. with certain buffers in order to avoid costs related to dry runs. Moreover, inspection delays might be minimized if forwarders were provided with genuine and verifiable data regarding all supply chain members involved in the container transport, the actual commodities transported, and the actual movement of containers. This information could be made available to customs and other authorities, possible reducing the number of physical interruptions in the supply chain. Fourth, delays due to changing weather conditions are associated with ETAs of deep-sea vessels which will be discussed in the next sub-section. Firth, theft and damage are hardly avoidable. Nevertheless, regarding theft, information about when and where containers are opened while in transport are beneficial in managing incidents. Sixth, piracy and terrorist attacks are neither avoidable nor better manageable by improved transparency regarding real-time performance data. Thus, they are not related to additional information needs.

The issue of preparing correct capacity forecasts is a managerial task mainly based on historic data and market knowledge. Even though the preparation of rolling forecasts is dependent on actual performance data, all necessary information regarding the preparation of capacity forecasts should be provided by internal management systems. In other words, this risk factor is not related to additional information needs.

Finally, in order to manage the risk of smuggling, forwarders need two kinds of information. First, verifiable data regarding all supply chain members involved in the container transport can be used to assess the risk of smuggling a priori in order to possibly back out of dubious deals. Second, information about when and where containers are opened while in transport is beneficial in reconstructing incidents.

Information flows

Regarding the risk factor of not knowing the actual content of containers, forwarders need the same kind of information as discussed with reference to possible delays in the physical flow due to customs inspections. In other words, forwarders need clarity regarding all supply chain members involved in the container transport, the actual commodities transported, and the actual movement of containers. Even though the information is already provided to them, it is important for forwarders to identify genuine sources. Currently, they are not in the position to verify data regarding importer and exporter or actual commodities to be transported.

With reference to ETAs of deep-sea vessels, forwarders need a reliable information source that automatically provides them with relevant updates in a timely manner. Currently, ETAs are provided by different stakeholders: shipping lines, terminal operators, and PCSs. However, forwarders have no certainty about the validity of the provided ETAs.

Concerning container handling times at terminals, forwarders need a reliable source that provides them with relevant milestones in a timely manner. Currently, direct B2B connections with terminal operators are the exception and shipping lines do not necessarily make relevant information available to forwarders as soon as they receive it. Moreover, third-party information providers do not guarantee the validity of data provided to them by terminal operators or shipping lines.

Risks related to the flow of documents are not related to additional information needs by forwarders.

The management of empty containers could be enhanced with gate-in information upon arrival of empty containers at the ECD. Moreover, an active track and trace of empty containers could be beneficial. In general, the internal awareness regarding the importance of empty container management needs to be increased by forwarders.

Finally, in order to adapt to constantly changing security requirements in a timely manner, forwarders depend on information regarding pending regulations.

4.2 Information Offerings

This chapter provides an overview of the different categories of IT systems which can possibly provide freight forwarders with risk-relevant information. The author discusses Portbase as an example of PCSs in detail and briefly addresses four additional system types: business systems, community systems besides PCSs, authority systems, and container movement and control systems.

4.2.1 Portbase

Information content as well as strengths and weaknesses of PCSs in general have already been outlined in sections 2.2.5 and 2.2.6. Therefore, this section focuses on Portbase specifically.

In conformity with PCSs in general, Portbase's information content varies considerably across the three supply chain flows: physical, information, and financial. First, regarding the physical flow of goods, Portbase provides selected information in the form of status updates regarding the whereabouts of containers. This information, however, is only available for port-side activities, i.e. from the moment of vessel arrival until the container is dispatched from the port, and vice versa. Second, most information provided by Portbase covers information flows, i.e. the governance and transaction layers (refer to Figures 7 and 8). For example, selected services inform users about scheduled Customs inspections and the release of containers afterwards. As a second example, Portbase provides information about the terminal at which a container is planned to arrive and the point at which it is supposed to be unloaded. Third, regarding financial flows, Portbase offers no information concerning payment status.

The only service related to financial flows supports the PA in the calculation of harbor dues by providing it with relevant cargo information.

As to freight forwarders in the cross-border container transport, Portbase provides only one relevant service – “Cargo Information”. It facilitates handling the administration associated with container shipments and arranging follow-up transport. Thus, it is mostly related to information flows. There is a general demand for more forwarding-specific services which has not yet been satisfied. Furthermore, especially large forwarders ask for direct interfaces between Portbase and their internal information systems. Currently, the “Cargo Information” service is solely web-based which requires forwarders to visit Portbase’s web page in order to retrieve relevant information.

With reference to risk management, Portbase does not offer any services or systems specifically designed for risk identification, analysis, or response. However, by providing stakeholders in and around the ports of Rotterdam and Amsterdam with relevant information, most of Portbase’s services support the identification of risks to a certain extent. Status updates regarding the whereabouts of containers which could theoretically be related to risk analysis, represent readiness instead of exception alerts. In other words, Portbase does not compare as-is data with performance plans in order to alert customers in case of deviations. The reason for this lies in Portbase’s credo that PCSs can only be successful if they remain neutral. In other words, they cannot strive for control in the supply chain or be decisive. This implies leaving risk analysis and response to the ports’ stakeholders.

With reference to the general weaknesses of PCSs as outlined in section 2.2.6, the author wants to emphasize three main aspects which restrain the role and scope of Portbase in the risk management of forwarders. First, Portbase is a local area solution for the ports of Rotterdam and Amsterdam as well as the associated hinterlands. Therefore, the information provided to customers covers only parts of the cross-border maritime container transport chains. Second, the use of Portbase is not mandatory. Consequently, system users cannot be sure to be provided with the required information by all relevant stakeholders. Single companies or even entire stakeholder groups might not be represented. For example, major freight forwarders are not using Portbase as actively as desired due to reasons discussed above. Third and probably most important, Portbase collects data, bundles or transforms it, and distributes it to relevant information users. However, the system does not perform data quality checks. Thus, genuineness and timeliness of the provided information cannot be guaranteed to users.

4.2.2 Alternative Information Systems

Business systems, community systems, authority systems, and container movement and control systems have been identified as four alternative system categories which can facilitate the risk management of freight forwarders.

First, business systems are defined as information systems of individual supply chain members. These systems facilitate the planning and management of internal operations and can possibly be interlinked with each other in order to exchange relevant information on a bilateral level. Depending on the operations of the respective company, business systems have a local or global scope. Of particular importance for forwarders are shipping line and terminal systems. Shipping line systems hold necessary information regarding vessel travel times, shipping routes, and ETAs. Terminal systems facilitate the container handling in sea terminals. Consequently, they represent direct information sources for container handling times and updates concerning the loading of containers on deep-sea vessels as well as pre- and follow-up transport modes.

Second, community systems feature broad information content. Examples are GT Nexus and INTTRA, which have been identified as the two most important platforms in the maritime container business. Both systems represent collaboration platforms used by different supply chain members to exchange relevant information. Just as with PCSs, the idea is to connect to only one information platform rather than each business partner individually. In more detail, GT Nexus is a cloud solution used by importers, exporters, logistics providers as well as banks to optimize the flows of goods as well as trade information from order to final payment. INTTRA is specialized on managing ocean shipments, i.e. scheduling and booking of vessel voyages, document transfer, and electronic invoicing. The scope of these systems is much wider than the one of PCSs. Instead of facilitating the flows of goods and documents in ports as microcosms, they operate on a global scale. However, as community systems, GT Nexus and INTTRA face more or less the same general weaknesses and threats as PCSs. System use is not mandatory, benefits might be distributed unevenly, information theft can be an issue, and neither genuineness nor timeliness of the information provided to users can be guaranteed.

Third, authority systems, such as e.g. customs systems, mainly hold safety and security relevant information. Examples are cargo information, information regarding the involved supply chain members, and, in case of scans or physical inspections, information about the actual content of containers. Moreover, customs systems give AEO-certified supply chain members advance warnings about which container will be scanned or physically checked. Authority systems are mostly provided with relevant information by third-party supply chain members active in container transport. In the case of customs, information is drawn from export and import declarations. Authority systems operate on a local (national) level but, to some extent, share information among each other.

Container movement and control systems can supply information concerning the position and integrity of containers. Smart container seals can be tracked via GPS and therefore allow real-time monitoring on a container- rather than just a vessel-level. Moreover, these seals measure if containers have been opened during transport. Vessel and container tracking platforms bundle the information, which can be accessed upon request (payment of user fees).

4.3 Supply Chain Risk Management of Freight Forwarders

This chapter brings together findings from chapters 4.1 and 4.2 in order to conclude on the role and scope of PCSs in the SCRM of freight forwarders regarding the cross-border maritime container transport. The author discusses risk management as practiced by the interviewed companies following Waters' (2007) structured approach: (1) identifying risks, (2) analyzing risks, and (3) responding to risks (refer to section 2.4.1). In that discussion, a special focus lies on risk identification and a comparison of information needs by forwarders and offerings by Portbase or alternative information systems.

However, before turning to the three steps of SCRM, the author refers to the concept of SCRM prerequisites. As outlined in detail in section 2.4.1, SCRM prerequisites are factors that enhance the successful implementation of a SCRM philosophy. If these are not given, SCRM is severely hampered (Pfohl et al., 2010). Of particular importance are the aspects risk perception, top management support, risk strategy, and cooperation and mutual trust.

Regarding risk perception, organizations need to have an understanding of risk in general and a willingness to manage identified risks and their sources. The interviews have shown that risk perception and attitude towards risk management need to improve among forwarders. Even though the answers to the question, how active forwarders consider their company in managing relevant risks, average at a score of 3.9 (min=3, max=5), with 1 being very inactive and 5 being very active, these results have to be scrutinized. To the author, they do not reflect common business. The interviews have revealed numerous risk factors, which are not necessarily regarded as such by forwarders and therefore not actively managed. Further, according to Roman Balog (personal communication, July 21, 2011), "an active management of risks in the freight forwarding business is not as common as one would think". This is confirmed by Peter Sonnabend's statement that "DHL more actively manages risks in other divisions such as 'Global express' or 'Air freight'" (personal communication, July 8, 2011). Moreover, Johan Vosbeek stated that Seacon is AEO accredited, which, according to him, is basically everything they can do regarding risk management (Johan Vosbeek, personal communication, July 18, 2011). In general, the interviews left the author with the impression that forwarders, at least to a certain extent, hide behind AEO accreditation and their participation in risk-related research projects. They do not always take on the responsibility of risk management and instead refer to responsibilities of other supply chain members.

Despite a rather critical evaluation of risk perception, the conducted interviews have proven that risk management is an aspect on managers' agendas. In other words, top management support is given. All interviewed forwarders have successfully worked towards fulfilling the requirements for AEO accreditation. Moreover, several in-house initiates aiming at improved risk management as well as cross-company research projects have been described. INTEGRITY and CASSANDRA are well-known examples for that. However, the author was also introduced to alternative approaches like e.g. an initiative by Eurogate, EADS Astrium, and Hellmann Worldwide Logistics. Nevertheless, it remains questionable to what extent top management support and risk-related initiatives are affecting general risk perception and attitude, i.e. whether they will have significant impacts on the operational level.

Regarding risk strategy, forwarders claim to follow both: proactive and reactive approaches to risk management. Even though a proactive (preventive) management of risks is necessary and desirable, it will never be bullet proof, making corrective measures inevitable. Peter Sonnabend refers to these two strategies as "two sides of the same coin" (personal communication, July 8, 2011).

Concerning cooperation and mutual trust, forwarders show a general willingness to share information with third-party supply chain members. Information sharing is very well developed towards customers, i.e. importers and exporters. Beyond that forwarders make important information available to other relevant business partners. Regarding the means of data transfer, B2B connections are preferred for data security reasons but forwarders also show a general willingness to provide community platforms with necessary information. It all comes down to whether information sharing through such platforms is safe and generates associated benefits. In general, forwarders do not want to over share information as it represents an essential part of their competitiveness.

Contrary to information sharing behaviors with customers and business partners, the author could not identify cooperation among forwarders in terms of data exchange in order to enhance SCRM of the entire business.

4.3.1 Identifying Risks

This section first outlines the status quo of risk identification. Subsequently, information needs of forwarders are compared to offerings of information systems in order to identify the theoretically best suited information sources as well as Portbase’s capacity.

Regarding the status quo of risk identification, interview results show similar patterns across all four freight forwarders. In other words, company size only has a marginal effect concerning how forwarders approach the identification of risks.

First and most importantly, risk identification is performed by the forwarders themselves. No external services or systems are applied. The only role of external information providers of any kind is to make available the necessary information to identify risks and their sources. In that process, forwarders prefer information directly from the source, i.e. from shipping lines, terminal operators, etc. It is only at this point that size matters. Large forwarders like Kühne+Nagel and DHL establish B2B connections to automate the information exchange with third-party supply chain members. In contrast, smaller forwarders like Hellmann Worldwide Logistics and Seacon Logistics mostly rely on first-hand information provided through the web pages of e.g. shipping lines and terminal operators. They prefer to access or acquire first-hand information in a manual manner instead of relying on third-party information providers. Similar patterns show regarding information exchange with customers. Large forwarders either establish B2B connections or offer web-services for their customers, while small forwarders have to rely on less automation.

If information is not obtainable via B2B connections and through web-pages of the information providers or if forwarders want to automate information exchange in a different way than B2B connections, they rely on platforms like GT Nexus, INTTRA, and CargoSmart. The former two have been introduced in section 4.2.2 while the latter is comparable in information content and scope. However, especially for large forwarders and from a managerial or risk management perspective, third-party information providers are not beneficial as reliability and data security cannot be guaranteed. Thus, if first-hand information sources are available, these will be used preferably. This is also relevant for Portbase and PCSs in general. Portbase, across all interviews, was only mentioned as some kind of fall-back or backup information provider. It falls behind other third-party information providers because of its local focus. Forwarders prefer to connect to globally operating information providers. Moreover, Portbase's cargo information service does not add benefit. Forwarders can acquire most of the provided information through preferred sources as outlined above.

Portbase is mainly used for three information blocks. First and probably most important, it represents the preferred source for information and status updates regarding the Customs clearance process. Second and also Customs related, Portbase provides proof for the final departure of containers from Europe. This information cannot be acquired directly from Dutch Customs. Finally, Portbase represents a backup information source regarding the loading process of containers as well as for vessel information (e.g. ETA). Forwarders use Portbase to verify the information they receive from shipping lines or other information platforms.

In the following, the author compares forwarders' information needs for risk identification with offerings of information systems. In doing so, only risk factors which entail additional information needs as defined in section 4.1.3 are discussed. Moreover, the results of section 4.1.3 have been slightly modified in order to avoid covering the same information need twice, regarding physical and financial supply chain flows. Changes in vessel routes and weather conditions represent reasons for delays in the physical container flow, but also impact ETAs of deep-see vessels (information flows). For the purpose of this section, these two aspects are attributed to the information flow-related risk factor "ETA" only.

Table 4 presents physical and information flow-related risk factors, associated information needs as well as information offerings. The latter is subdivided into "Best source" and "Capacity of Portbase".

		Information offerings	
Risk factor	**Information need**	**Best source**	**Capacity of Portbase (PCSs)**
Physical flows			
Misrouting (delays)	Real-time information about the whereabouts of containers	Container movement and control systems	Limited
Customs and other inspections (delays)	Timely information about which containers will be checked	Customs, Portbase	High
	Genuine and verifiable data regarding involved supply chain members, transported commodities, and actual movement of containers	Customs export side, Container movement and control systems	Limited
Theft and damage	Information about when and where containers are opened	Container movement and control systems	Limited
Information flows			
Uncertain container contents	Genuine and verifiable data regarding involved supply chain members, transported commodities, and actual movement of containers	Customs export side, Container movement and control systems	Limited
ETA	Reliable and automated updates in a timely manner	Shipping lines	Medium
Container handling time at terminal	Reliable and automated Milestones (updates) in a timely manner	Terminal operators	Medium
Empty container management	Gate-in information upon arrival of empty containers at the ECD	ECD (shipping line)	Limited
	Track and trace of empty containers	Container movement and control systems	Limited
Regulations	Timely information regarding pending regulations	Customs, Portbase	High

Table 4, Comparison of information needs and offerings

Table 4 covers three risk factors related to physical supply chain flows. First, the risk of delays due to misrouting cannot be eliminated. However, container movement and control systems can provide forwarders with the necessary information to locate containers in real-time and thus mitigate delays. Portbase's capacity regarding the location of containers is very limited. The system currently only covers the whereabouts within the ports of Rotterdam and Amsterdam. Moreover, the information is neither real-time nor first-hand. According to Marten van der Velde, Portbase is considering to offer track and trace information in the future. However, even if the service spectrum is widened to include such information, it is just second-hand. Therefore, validity issues would remain.

Second, delays associated with customs and other inspections are related to two different information needs. First, forwarders value timely notifications about which containers will be inspected. Such information can either be directly provided by Dutch Customs or via Portbase. The system has a history in supporting Customs declarations. Beyond that, interviews have not revealed any trust issues regarding data validity or timeliness. Moreover, Portbase is currently used by most forwarders to file necessary declarations and receive status updates. Thus, the system's capacity regarding this special information need is high. Second, forwarders depend on genuine and verifiable data regarding involved supply chain members, transported commodities, and actual movement of containers. The main source for the first two information blocks is the exporter or importer. None of the discussed information systems mitigate the forwarders' risk of receiving false data from their customers. However, if a forwarder is only responsible for the import side of a container transport chain, the Customs system on the export side might represent a genuine and thus valuable information source. Forwarders could obtain relevant information from export declarations and therefore mitigate the risk of container inspections in the Netherlands. Moreover, container movement and control systems can provide forwarders with data regarding actual container movements. As this represents a risk measure for Dutch Customs, it might further mitigate the probability of physical inspections, i.e. delays in the container transport. Portbase's capacity in providing any of the three discussed information blocks is limited. The system cannot be classified as a genuine data source as it is only a third-party information provider that does not perform data quality checks. Furthermore, Portbase suffers from the same weaknesses as discussed regarding its capacity in mitigating the risk of misrouting.

Finally, risks of theft and damage can, at most, be mitigated. Container movement and control systems represent appropriate sources of information about when and where containers have been opened during transport. In contrast, Portbase's capacity in providing relevant information is limited due to the same reasons as discussed regarding the risk of misrouting.

Table 4 also depicts five risk factors concerning information flows. First, risks related to uncertainty about the actual container content are again associated with the need for genuine and verifiable data regarding involved supply chain members, transported commodities, and actual movement of containers. Thus, best-suited information source and Portbase's capacity coincide with the above discussed information offerings regarding Customs and other inspections.

Second, the most reliable source regarding ETA updates is the shipping line. However, in order to enhance forwarders' risk management, ETA updates need to be pushed to them automatically and in a timely manner. Portbase's capacity in supplying the relevant information can only be considered medium. Even though the system provides forwarders with ETAs, data quality is questionable. Portbase, as a third-party information source, is fed with data by shipping lines. In many cases this is either done with considerable time slack or not at all.

Third, the issue regarding uncertainty about container handling times at sea terminals is similar to that of ETA. Terminal operators represent the best first-hand information source, while Portbase's capacity is medium. Reasons coincide with the ones discussed regarding ETAs.

Fourth, concerning empty container management the information need of forwarders is again twofold. First, gate-in information upon arrival of the empty container at the ECD is best provided by the ECD operator, i.e. the shipping line. Portbase's capacity as an information source for the necessary data is limited. Currently, the system's service spectrum does not comprise the relevant information. Even if Portbase widened its spectrum to offer gat-in information at ECD, data quality issues as described above remain. Second, empty containers could be traced by container movement and control systems, while Portbase capacity regarding container tracing is limited, as discussed concerning e.g. the risk of misrouting.

Finally, forwarders need timely information about pending security regulations. Dutch Customs represents the most direct source for that. However, Portbase also has a high capacity in providing forwarders with relevant information in due time. Even though Portbase is a neutral third-party information platform, it has strong ties to the PAs of Rotterdam and Amsterdam as well as to Dutch Customs. All three can be considered as genuine data sources. Thus, data quality issues do not apply regarding this information block.

4.3.2 Analyzing risks

The interviewees consider risk analysis as too critical and important to be outsourced to external service providers. Thus, forwarders use their internal information systems to compare target and actual data. Reoccurring issues in planning and execution as well as other potential risk factors are classified into priority groups according to likelihoods and potential damages.

All interviewed forwarders rely on internal as well as external data sources as a basis for risk analysis (refer to section 4.3.1). Nevertheless, large forwarders seem to put more emphasis on risk analysis than small niche players. Johan Vosbeek of Seacon Logistics, as an example for a small forwarder, used the terminology “if performed” and “might” when talking about the subject (personal communication, July 18, 2011). Thus, the author was left with the impression that risk analysis is not considered a main issue.

More details regarding how risks are analyzed have not been disclosed to the author.

4.3.3 Responding to Risks

Comparable to risk analysis, risk responses are handled internally without direct support of third-party service providers. Furthermore, risk mitigation is considered as too specific and vital to be highly automated. Even though certain mitigation processes (e.g. the location of misrouted containers) are pre-defined and standardized to a certain extent, risk managers as well as operational specialists evaluate risks individually and act accordingly.

Interviewees provided the author with some generic examples of how risks to forwarders are being managed. First, forwarders work with preferred carriers and actively select them for certain shipments based on past experience. This way, possible delays can be curtailed by selecting the most reliable shipping line. Second, the risk of not knowing the actual content of containers is managed in a similar way. Forwarders might work only with a certain group of trusted customers, not engage in contracts with private persons, or not transport certain types of goods (e.g. removable) in order to reduce the risks associated with container contents.

Risk responses, or in different terms, incident management towards customers is somewhat automated. Customers, if interested in such services, are provided with automatic alert messages or e-mails informing them about delays in the transport of containers.

More details regarding risk responses have not been disclosed to the author.

4.3.4 Role and Scope of PCSs

The prevailing research goal of this thesis is to identify the role and scope of PCSs in providing data that enhances SCRM of freight forwarders regarding the cross-border maritime container transport. Role and scope have already been defined following the Oxford Dictionaries in the introduction to this thesis. Nevertheless, the author wants to refresh the definitions at this point: A role is “the function assumed or part played by a person or thing in a particular situation” (Oxford Dictionaries, 2011a) and scope is defined as “the extent of the area or subject matter that something deals with or to which it is relevant” (Oxford Dictionaries, 2011b).

Hypothetically, the role of PCSs in general and Portbase specifically regarding the risk management of forwarders seems to be easily definable. Considering Portbase's role as a central and neutral information broker on an operational level, one could expect the system to fulfill a similar purpose regarding the risk management of a specific user group.

Prima facie, Portbase assumes the function of a source for risk-relevant information without being involved in the actual risk management process of forwarders. In other words, Portbase provides the necessary data for forwarders to identify, analyze, and respond to risks associated with the cross-border maritime container transport. However, analyzing the results presented up to this point in detail, Portbase's role must be defined more restricted. To forwarders, the system does not represent a primary source for risk-relevant information but is rather mainly used for verification of data obtained from other supply chain members. For example, Kühne+Nagel employs PCSs to validate milestones regarding container loading processes as provided by shipping lines. Moreover, Portbase's importance in providing status updates concerning the Customs clearing process constitutes a rare exception. Consequently, the author defines Portbase's role in providing data that enhances forwarders' risk management regarding cross-border maritime container transport as follows:

Portbase serves as a source for information used to prove the validity and accuracy of risk-relevant data provided by other supply chain members.

This definition holds for large as well as small forwarders, which stands in contrast to what was generally expected. Representatives of Kühne+Nagel and DHL presumed that the role of PCSs might be a different one for small forwarders, i.e. PCSs are more important for the risk management of small freight forwarders. However, interviews with Hellmann Worldwide Logistics and Seacon Logistics have rebutted this assumption. Presumably, PCSs play a slightly less important role for small forwarders, as they attach less importance to risk management in general. This, however, could not be generally validated by the presented results.

Defining the scope of PCSs is more complicated as the "subject matter" is rather complex. In other words, "scope" relates to different contexts. Bottom line:

The scope of Portbase is limited. This limitation can be demonstrated with respect to four different subject matters – risk management process, offered services, supply chain, and geographical focus.

First, regarding the process of SCRM as outlined in section 2.1.4, Portbase's scope is limited to risk identification. As the results have shown, forwarders rely on internal information systems when managing risks associated with the cross-border maritime container transport. In other words, no external systems are applied. Therefore, Portbase's scope is restricted to providing information which can be used for risk identification.

Second, concerning the number of services offered to forwarders, Portbase's scope is limited to only one relevant service – "Cargo Information". Moreover, the information content of that service is rather low as forwarders can acquire most of it through preferred sources, e.g. B2B connections.

Third, regarding the entire container transport (supply) chain, Portbase only covers a certain part. The system's informational scope is limited to port-side activities, leaving out pre- and follow-up transport as well as most of the deep-sea voyage.

Fourth, concerning the geographical focus, Portbase is limited to the ports of Rotterdam and Amsterdam. In a broader sense, the system's scope is limited to the Netherlands.

The limitations in scope concerning supply chain and geographical focus reinforce each other. Portbase's scope comprises only parts of the entire container transport chain and above that does so for only a very small geographically region, i.e. one country. Therefore, Portbase's overall information content from globally operating freight forwarders' points of view is very limited.

5 Summary and Conclusions

Given the increasing importance of SCRM for operational success in global trade, efficient exchange of risk-relevant information among supply chain members has become a competitive advantage. PCSs facilitate the information exchange in and around port communities and, therefore, might contribute to risk management of port community members.

Despite their practical importance, the topics of SCRM and PCSs are rather new and comparatively under-researched. For that reason, the author summarized the existing bodies of literature and interviewed selected supply chain members in order to investigate to what extent risk managers of forwarders can rely on PCSs to provide them with risk-relevant information.

This chapter summarizes, discusses and concludes on the results of this thesis. Further, limitations and recommendations for future research are outlined.

5.1 Summary

The prevailing objective of this thesis was to define the role and scope of PCSs in providing data that enhances the SCRM of freight forwarders. In order to arrive at the aspired definition, the author addressed four sub-questions presented as research questions one to four in the main text. The results of these sub-questions as well as the definitions concerning role and scope of PCSs in forwarders' risk management are briefly summarized one by one in the remainder of this section.

What are the main risks and their sources faced by freight forwarders in the cross-border maritime container transport?

The author addressed this research question in section 4.1.2 after outlining the main processes of forwarders concerning export and import of containers in section 4.1.1. The main risk factors were discussed along the three supply chain flows: physical, information, and financial. However, risks to financial flows were dropped from further discussions as they showed no clear connection to PCSs.

- Physical flows
    - Unscheduled delays
    - Wrong capacity forecast
    - Smuggling

- Information flows
    - Uncertainty regarding container contents
    - Uncertainty regarding ETA
    - Uncertainty regarding container handling times at sea terminals
    - Flow of documents
    - Whereabouts of empty containers
    - Changing security requirements
- Financial flows
    - Variable costs of shipping
    - Payments defaults of customers

Moreover, section 4.1.2 outlined sources to each risk factor and classified the discussed risks concerning levels of analysis – operational, tactical, and strategic. Most risk factors are found to have an operational as well as a tactical component.

What are the information needs of freight forwarders to manage the risks of cross-border maritime container transport?

Forwarders' information needs for an active risk management are twofold: They require target data as well as real-time performance information. In section 4.1.3 the author identified that forwarders' need for target data is met by internal planning systems while the need for real-time performance data can only be satisfied by increasing the visibility in the supply chain, i.e. by receiving more accurate real-time data from external information providers in a timely manner. Further, section 4.1.3 outlined in detail the actual information needs of forwarders with reference to physical and information flow-related risk factors.

What information is provided by PCSs to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

With reference to risk management, Portbase does not offer any services or systems specifically designed for risk identification, analysis, or response. However, the "Cargo Information" service provides forwarders with operational data, which can support the identification of risks to a certain extent.

Moreover, section 4.2.1 discussed general weaknesses of Portbase in supplying forwarders with risk-relevant information. Most importantly, Portbase does not quality check data received from third-party supply chain members and consequently cannot guarantee its genuineness and timeliness.

What information is provided by alternative information systems to support the SCRM of freight forwarders regarding the cross-border maritime container transport?

Section 4.2.2 discussed four alternative system categories which can facilitate the risk management of freight forwarders by providing forwarders with relevant information. Internal business systems of individual supply chain members, authority systems, and container movement and control systems have been identified as first-hand information providers. Depending on the systems' focus, forwarders can acquire associated risk-relevant information directly from the source.

In contrast, community systems like GT Nexus or INTTRA represent collaboration platforms used by different supply chain members to exchange information on a global scale. Therefore, they hold a large variety of potentially risk-relevant information. However, these systems face more or less the same general weaknesses and threats as PCSs. System use is not mandatory, benefits might be distributed unevenly, information theft can be an issue, and neither genuineness nor timeliness of the information provided to users can be guaranteed.

What is the role and scope of PCSs in providing data that enhances SCRM of freight forwarders regarding the cross-border maritime container transport?

Sections 4.3.1-4.3.3 discussed the status quo of risk identification as practiced by the interviewed freight forwarders. The author revealed that risk analysis, and response are neither outsourced to nor directly supported by external service providers. However, forwarders are in need of certain information in order to identify possible risk factors. Consequently, the author compared forwarders' information needs to offerings of information systems in order to identify the theoretically best suited information sources as well as Portbase's role and scope in providing risk-relevant data.

Portbase's role was defined as to serve as a source for information used to prove the validity and accuracy of risk-relevant data provided by other supply chain members.

The system' scope is limited with respect to risk management processes, offered services, supply chain, and geographical focus.

5.2 Discussion and Conclusions

Portbase's restricted role in forwarders' risk management as some kind of backup information source is mainly rooted in three matters – the first two being related to the system's scope and the third representing Portbase major structural weakness.

First, Portbase's supply chain and geographical foci are too narrow for freight forwarders. Portbase only covers port-side supply chain activities for sea ports in the Netherlands. The same holds for PCSs in general. Therefore, if forwarders were to use PCSs as a primary data source, they would have to connect to a large number of PCSs all over the world in order to cover their information needs related to global business operations. In parallel, alternative information sources would have to be established in order to obtain necessary data regarding the cross-border maritime container transport which is not covered by PCSs. In praxis however, forwarders aim at minimizing the number of information sources and data connections. Consequently, B2B communication with relevant supply chain members represents the most efficient information source. Data interfaces have to be established only with a small number of e.g. preferred shipping lines instead of a large variety of locally-focused PCSs. As soon as the number of involved stakeholders makes B2B communication inefficient, forwarders rely on globally oriented community systems like GT Nexus and INTTRA (refer to section 4.2.2).

Second, Portbase's service offering for forwarders is too limited and not demand-oriented. The only forwarding business-specific service "Cargo Information" primarily offers information concerning the whereabouts of containers within the port as well as announcements and status updates of Customs inspections. Consequently and for similar reasons as outlined above, forwarders acquire most of the provided data through preferred information sources (e.g. B2B connections with shipping lines).

Portbase's limited service offering for freight forwarders allows two conclusions. First, from a general perspective, Portbase seems to not perceive freight forwarders as an important stakeholder group in the port communities of Rotterdam and Amsterdam. Instead, they focus on satisfying other supply chain members' demands. Reasons for that have not been investigated in this thesis. Second, from a risk management perspective, Portbase's risk perception seems to be limited to possible delays in Customs processes. Safety and security related Customs procedures are considered the main risks (sources) inside the port. A broader consideration of possible risks in the maritime container transport, however, could result in a more demand-oriented service offering.

Finally, the interviews have revealed one major structural weakness of Portbase. The company's business model is based on collecting, bundling, transforming, and distributing data to relevant stakeholders. In doing so, however, the system does not check data quality, i.e. the actual content. Therefore genuineness and timeliness of the provided information cannot be guaranteed to Portbase's users. This reliability issue would impede a change in Portbase's role even if the system widened its supply chain or geographical scope.

A discussion of Portbase's role in enhancing the SCRM of forwarders would be incomplete without specifying the highest feasible role of external information providers in general. The results presented in chapter 4.3 make clear that forwarders consider risk management as too critical to be outsourced to or substantially supported by external service providers. Moreover, forwarders risk perception was proven to be limited. For that reason, the author does not expect any major changes in forwarders' general approach to risk management. In other words, there will be no demand for fundamentally different services in the near future. Consequently, the highest feasible role for external information providers like Portbase is that of a primary source for risk-relevant information.

With regard to scope, the subject matters of supply chain and geographical focus are worth discussing in more detail. Even though Marten van der Velde of Portbase indicated that the platform has no intention to grow and widen the scope of business to become a supply chain-wide operating system, selective coverage extensions are planned. Portbase considers hinterland activities in the form of pre- and follow-up transport to be closely related to and thus crucial for deep-sea port activities. Consequently, they want to develop several hinterland-related services. Such services would not be limited to the Netherlands. In other words, Portbase is willing to accept overlaps and therefore competition with other PCSs as long as there is some relation to Rotterdam or Amsterdam as Dutch main ports. However, in order to share costs and risks associated with extensions to the supply chain scope, Portbase is planning to realize them in close collaboration with existing service providers (e.g. movement and control systems) instead of developing the services single-handed. For example, Portbase plans to offer a service which allows users to optimally plan and select hinterland transport routes through Portbase. In the context of this service, the system would send pre-notifications to inland terminals in order to inform them about the ETA of containers. As a second example, Portbase plans to make general hinterland activities visible through track and trace services. This coincides with forwarders’ need for a more sophisticated empty container management.

From a strategic perspective, Portbase’s plans to extend its supply chain scope seem reasonable. Currently, pre- and follow-up transporters do not provide forwarders with automated status updates regarding their transport services. Collecting the relevant information is time-consuming and burdensome for forwarders. Moreover, other community systems’ market position (e.g. GT Nexus and INTTRA) concerning hinterland activities is not as strong as in the maritime part of the container transport chain. However, despite a weaker market position, these systems might still be preferred over Portbase as possible information sources regarding hinterland activities. Thus, the market entry must be well prepared. One possible option for Portbase is to develop new hinterland services with a special focus on smaller or more locally-focused forwarders which are not highly integrated in global networks like e.g. GT Nexus.

Concerning its geographical scope, Portbase does not strive for becoming a globally operating system. The only geographical extensions would take place in line with the development of new hinterland-oriented services. Nevertheless, PCSs in general could widen their geographical scope by interconnecting among each other. In June 2011, six European PCSs, with Portbase being one of them, took a first major step towards more cooperation and interconnection by forming the European Port Community Systems Association (EPCSA). The association’s mission is to “influence public policy in the European Union level in order to achieve e-logistics throughout all European ports, operating as a key element of the EU maritime, shipping and logistics industry” (EPCSA, 2011). Nevertheless, for PCSs to become more relevant concerning the risk management of forwarders and to possibly complement B2B information exchanges in the cross-border maritime container transport, true interconnection and data exchange are necessary. This requires the standardization of communication standards among all PCSs. Moreover, data ownership issues represent possible obstacles to establishing data exchange between PCSs. It is mostly not the PCS but rather the legal owner of the information who decides what to share and who to share it with. Furthermore, despite the potential benefits associated with interconnected PCSs, the author wants to emphasize that such would only replicate information exchanges which are already present on a B2B level or in other community systems. Beyond that, data reliability issues remain.

In general, the interviews left the author with the impression that Portbase in particular but also PCSs in general need to redefine their role – not only regarding the risk management of container supply chain members, but rather concerning their overall business model. As discussed in chapter 2.2, PCSs were first established to facilitate and improve the enormous load of communication between port community members. They were designed to collect, bundle, and distribute data within the port community – a task which represented a burden for the individual stakeholder. Over the last decade, PCSs developed into the systems they are today. At the same time, however, information technology has improved dramatically. Data collection and bundling do not represent as much of a burden as they did a decade ago. New technologies enable information sources to push necessary information to relevant stakeholders all over the world in a timely and cost-efficient manner. Local information brokers like PCSs might not be needed anymore. Consequently, PCSs need to find new niches and develop alternative business models in order to survive in the long-run. Currently, PCSs in general but also Portbase in particular do not seem to have a preferred position.

Furthermore, this thesis clearly shows the need for an improved coordination of the overall information demand and supply in the cross-border maritime container transport. On the demand-side, a large variety of stakeholders of different sizes, interests, and capabilities require more and more specific information. This information demand translates into promising business opportunities for community and visibility platforms. They try to satisfy the different demands by offering tailor-made solutions. Information is collected, transformed, and distributed to whoever might need it. However, the information brokers do not perform data quality checks. This creates validity issues and mistrust instead of increasing supply chain visibility. As a consequence, supply chain members with numerous B2B connections and community platform subscriptions still manually collect data in order to verify the information they were automatically provided with. A possible solution for that dilemma remains to be discovered. However, consensus-building on demand- and supply-side represents a first step into the right direction. Thus, European research projects like CASSANDRA, even if not specifically investigating this issue, are of major importance.

Finally, a global standardization of security and safety management might be beneficial. Currently, different countries use their own systems to manage and audit the safety and security of supply chains. However, most systems rely on more or less the same information. A standardized platform to provide the authority systems of countries all over the world with the required information would be beneficial. Such a global single-window towards authority systems might only be hypothetical, but PCSs can possibly provide relevant services. PCSs are companies that are either owned by or operate in close cooperation with regulatory bodies (e.g. PAs and Customs authorities). Thus, they could either influence public policy in order to achieve a larger degree of standardization or collaborate among each other and exchange information to be fed into the local authority systems without any intervention of third-party supply chain members. The former coincides with the mission of the newly formed European Port Community Systems Association. Thus, it will be very interesting to monitor activities and initiatives of the EPCSA and whether the association can help to solve any of the above described general challenges faced by PCSs.

5.3 Limitations

In interpreting the results of this thesis, the reader should take notice of its limitations. First, this thesis is build upon two evolving bodies of literature. New insights or developments could contradict the theoretical frameworks as applied in thesis. Second and due to the nature of the exploratory research approach, external validity and generalizability of the findings are debatable. The results are based on interviews with only one PCS, four selected forwarders, and Dutch Customs. Other PCSs might offer a larger variety of services for forwarders or are possibly currently working towards a new business model. Even though the interviews left the author with the impression that Portbase’s role and scope in enhancing forwarders’ risk management is representative for other PCSs, an increasing number of similar case studies would contribute to increased validity and generalizability. Third, for Hellmann Worldwide Logistics and Seacon Logistics, the author could only schedule interviews with operational representatives. Consequently, a general risk management perspective is missing for these two forwarders. However, due to the rather small scale of the two companies, the author does not expect the answers of operational and risk management specialists to differ significantly.

5.4 Recommendations

The most obvious opportunity for further research is a replication of the presented case study. This could be undertaken in one of two ways. First, forthcoming case studies could lay their focus on different port communities in order to investigate the role and scope of alternative PCSs regarding the risk management of forwarders. Second, case studies could be reproduced for Portbase and the port of Rotterdam, but with regard to the risk management of different focus groups – e.g. shipping lines or terminal operators. Doing so would enhance the understanding of the overall information needs of all involved stakeholders in the cross-border maritime container transport.

Further, it would be interesting to analyze PCSs in detail. Several aspects represent promising leads. First, feasible future roles and scopes of PCSs regarding the risk management of stakeholder in the cross-border maritime container transport need to be identified and worked towards. Second, the preparation of a cost/benefit analysis for Portbase's planned hinterland services in combination with a competitor analysis enable an improved judgment of the extension plans. Further, the generated results could provide valuable insights regarding possible service extension of PCSs beyond the ports' boundaries in general. Third, it is crucial to solve PCSs' data reliability issues. Therefore, it is of importance to develop a feasible and cost-efficient method of performing more advanced quality checks regarding genuineness and timeliness of the information that is made available to PCSs. Fourth and most importantly, the role of PCSs as local information brokers in global supply chains needs to be scrutinized. If advancements of information technologies have eroded PCSs' business models, new possible niches and preferred positions need to be investigated.

Finally, researchers should support the global standardization of safety and security management as well as the coordination of information supply and demand in the cross-border maritime container transport. The author sees the researchers' role as an external mediator in the process of consensus-building among the different supply chain members. The interviews have clearly shown that the different stakeholders are pursuing their own economic interests, which leads to more variety and diversity instead of standardization. Consequently, comprehensive research projects which initiate and stimulate standardization across different stakeholder groups are of major importance.

References

Baird, I. S. and Thomas, H. (1990). What is risk anyway. In R. A. Bettis and H. Thomas (Eds.), *Risk, Strategy, and Management* (pp. 21-52). London: JAI Press.

Barnes, P. and Oloruntoba, R. (2005). Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. *Journal of International Management*, *11*(4), 519-540.

Barton, F. L. and McGehee, R. B. (1942). Freight Forwarders. *Harvard Business Review, Spring,* 336-347.

Bogataj, D. and Bogataj, M. (2007). Measuring the supply chain risk and vulnerability in frequency space. *International Journal of Production Economics*, *108*(1-2), 291-301.

Borge, D. (2001). *The Book of Risk*. New York: John Wiley & Sons.

Brandenburg, H., Gutermuth, J., Oelfke, D. Oelfke, W., and Waschkau, S. (2010). *Güterverkehr-Spedition-Logistik: Leistungserstellung in Spedition und Logistik*. Troisdorf: Bildungsverlag EINS.

Brodmerkel, E. (1978). *Premiere für Datenbank-Informationssystem: Compass beschleunigt Bremische Häfen*. Retrieved May 21, 2011 from http://www.computerwoche.de/heftarchiv/1978/13/1195329/

Burgess, K., Singh, P. J., and Koroglu, R. (2006). Supply chain management: a structured literature review and implications for future research. *International Journal of Operations & Production Management*, *26*(7), 703-729.

Cavinato, J. L. (2004). Supply chain logistics risks: From the back room to the board room. *International Journal of Physical Distribution & Logistics Management, 34*(5), 383-387.

Cheng, S. K. and Kam, B. H. (2008). A conceptual framework for analysing risk in supply networks. *Journal of Enterprise Information Management*, *22*(4), 345-360.

Chopra, S. and Sodhi, M. S. (2004). Managing Risk to Avoid Supply-Chain Breakdown. *MIT Sloan Management Review, Fall,* 53-61.

Christopher, M. and Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 388-396.

Christopher, M. and Peck, H. (2004). Building the Resilient Supply Chain. *International Journal of Logistics Management*, *15*(2), 1-13.

Christopher, M. and Rutherford, C. (2004). Creating supply chain resilience through agile six sigma. *Critical Eye*, *June-August*, 24-28.

Christopher, M. (1998). *Logistics and Supply Chain Management: Strategies for Reducing Cost and Improving Service*. Harlow: Financial Times Prentice Hall.

Closs, D. J. and McGarrell, E. F. (2004). Enhancing Security Throughout the Supply Chain. *Special Report Series, IBM Center for the Business of Government*. Retrieved May 13, 2011 from http://www-03.ibm.com/procurement/proweb.nsf/objectdocswebview/filesupply+chain+security+white+paper+and+assessment+guide+april+2004/$file/supply+chain+security+white+paper+and+assessment+guide+april+2004.pdf

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

Cranfield School of Management (2003). Creating Resilient Supply Chains: A Practical Guide. Retrieved May 21, 2011 from https://dspace.lib.cranfield.ac.uk/bitstream/1826/4374/1/Creating_resilient_supply_chains.pdf

Dakosy (2011). *EDI Services via DAKOSY*. Retrieved May 19, 2011 from http://www.dakosy.de/en/solutions/port-community-system/edi-in-the-port

dbh Logistics (2011). *Products of dbh Logistics IT AG*. Retrieved May 19, 2011 from http://www.dbh.de/en/navigation/products.html

David, P. A. and Stewart, R. D. (2008). *International Logistics: The Management of International Trade Operations*. Mason: CENGAGE Learning.

EPCSA (2011). *Mission and Objectives*. Retrieved August 8, 2011 from http://www.epcsa.eu/about-epcsa/mission-and-objectives

Fiegenbaum, A. and Thomas, H. (1988). Attitudes toward Risk and the Risk-Return Paradox: Prospect Theory Explanations. *The Academy of Management Journal, 31*(1), 85-106.

Fishburn, P. C. (1970). *Utility Theory for Decision Making*, New York: Wiley.

Forrester, J. W. (1968). *Industrial Dynamics*. New York: Wiley.

Gaonkar, R. and Viswanadham, N. (2007). *A Conceptual and Analytical Framework for the Management of Risk in Supply Chains*. Indian School of Business. Retrieved May 10, 2011, from http://www.isb.edu/WorkingPapers/AConceptual_AnalyticalFramework.pdf

Gerber, M. and von Solms, R. (2005). Management of risk in the information age. *Computers & Security*, *24*(1), 16-30.

Guinipero, L. C., Hooker, R. E., Joseph-Matthews, S., Yoon, T. E., and Brudvig, S. (2008). A Decade of SCM Literature: Past, Present and Future Implications. *Journal of Supply Chain Management*, *44*(4), 66-86.

Gustafsson, I. (2007). Interaction between Transport, Infrastructure, and Institutional Management: Case Study of a Port Community System. *Transportation Research Record: Journal of the Transportation Research Board*, *2033*, 14-20.

Harland, C., Brenchley, R., and Walker, H. (2003). Risk in supply networks. *Journal of Purchasing & Supply Management*, *9*(2), 51-62.

Haywood, M. and Peck, H. (2003). *An investigation into the management of supply chain vulnerability in UK aerospace manufacturing*. Paper presented at the 8th International Symposium on Logistics, July 6-8, Seville.

Hendricks, K. B. and Singhal, V. R. (2005). An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm. *Production and Operations Management*, *14*(1), 35-52.

Hendricks, K. B. and Singhal, V. R. (2003). The effect of supply chain glitches on shareholder wealth. *Journal of Operations Management*, *21*(5), 501-522.

IBM (2008). *Supply Chain Risk Management: A Delicate Balancing Act*. Retrieved June 12, 2011 from ftp://ftp.software.ibm.com/common/ssi/sa/wh/n/gbw03015usen/GBW03015USEN.PDF

Integrity (2011). *Integrity project*. Retrieved June 12, 2011 from http://www.isl.org/projects/integrity/index.php?module=Downloads&func=sublevel&cid=13&start=0

Jüttner, U. (2005). Supply chain risk management. *International Journal of Logistics Management*, *16*(1), 120-141.

Jüttner, U., Peck, H., and Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics: Research & Applications, 6*(4), 197-210.

Kahneman, D. and Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. *Econometrica*, *47*(2), 263-292.

Kajüter, P. (2003). Risk Management in Supply Chains. In S. Seuring, M. Müller, M. Goldbach, and U. Schneidewind (Eds.), *Strategy and Organization in Supply Chains* (pp. 321-336). Heidelberg: Physica-Verlag.

Kleindorfer, P. R. and Saad, G. H. (2005). Managing Disruption Risks in Supply Chains. *Production and Operations Management*, *14*(1), 53-68.

Knemeyer, A. M., Zinn, W., and Eroglu, C. (2009). Proactive planning for catastrophic events in supply chains. *Journal of Operations Management*, *27*(2), 141-153.

Knight, F. H. (1937). *Risk, Uncertainty and Profit*. Boston: Houghton Mifflin.

Lambert, D. M. and Cooper, M. C. (2000). Issues in Supply Chain Management. *Industrial Marketing Management*, *29*, 65-83.

Lambert, D. M., Cooper, M. C., and Pagh, J. D. (1998). Supply Chain Management: Implementation Issues and Research Opportunities. *The International Journal of Logistics Management*, *9*(2), 1-19.

Lee, H. L. and Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics*, *96*(3), 289-300.

Long, A. (2009). Port Community Systems. *World Customs Journal*, *3*(1), 63-68.

Manuj, I. and Mentzer, J. T. (2008). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192-223.

March, J. G. and Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, *33*(11), 1404-1418.

Martin, J. and Thomas, B. J. (2001). The container terminal community. *Maritime Policy & Management*, *28*(3), 279-292.

McKinsey (2008). *Managing global supply chains: McKinsey Global Survey Results*. Retrieved June 12, 2011 from https://www.mckinseyquarterly.com/PDFDownload.aspx?ar=2179

McMaster, T., and Wastell, D. (2005). Diffusion - or delusion? Challenging an IS research tradition. *Information Technology & People*, *18*(4), 383-404.

MCP (2011). *Destin8 Functionality*. Retrieved May 19, 2011 from http://www.mcpplc.com/Destin8/Functionality.aspx

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., Smith, C. D., and Zacharia, Z. G. (2001). Defining Supply Chain Management. *Journal of Business Logistics*, *22*(3), 1-25.

Mila, S. G. (2009). Port Community System (PCS), its present & future. *Sail to the Future*, *2*(1), 1.

Miller, K. D. (1992). A Framework for Integrated Risk Management in International Business. *Journal of International Business Studies*, *23*(2), 311-331.

Mitchell, V.-W. (1995). Organizational Risk Perception and Reduction: A Literature Review. *British Journal of Management*, *6*(2), 115-133.

Morgan, R. M. and Hunt, S. D. (1994). The Commitment-Trust Theory of Relationship Marketing. *The Journal of Marketing*, *58*(3), 20-38.

Mullai, A. (2009). Risk Management System – A Conceptual Model. *International Series in Operations Research & Management Science*, *124*(1), 83-101.

Murphy, P. R. and Daley, J. M. (2001). Profiling International Freight Forwarders: An Update. *International Journal of Physical Distribution & Logistics Management*, *31*(3), 152-168.

Murphy, P. R. and Daley, J. M. (1999). EDI benefits and barriers: Comparing international freight forwarders and their customers. *International Journal of Physical Distribution & Logistics Management,* 29(3), 207-216.

Murphy, P. R., Daley, J. M., and Dalenberg, D. R. (1992). Profiling International Freight Forwarders: A Benchmark. *International Journal of Physical Distribution & Logistics Management*, *22*(1), 35-41.

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

Norrman, A. and Lindroth, R. (2002). *Supply chain risk management: purchasers' vs. planners' views on sharing capacity investment risks in the telecom industry*. Paper presented at the 11th International Annual IPSERA Conference, March 25-27, Enschede.

Oliver, R. K. and Webber, M. D. (1982). Supply Chain Management: Logistics Catches Up with Strategy. In M. Christopher (Ed.), *Logistics: The Strategic Issues* (pp. 63-75). London: Chapman & Hall, 1992.

Oxford Dictionaries (2011a). *Definition of "role".* Retrieved June 30, 2011 from http://oxforddictionaries.com/definition/role

Oxford Dictionaries (2011b). *Definition of "scope".* Retrieved June 30, 2011 from http://oxforddictionaries.com/definition/scope

Oxford Dictionaries (2011c). *Definition of "risk"*. Retrieved May 10, 2011 from http://oxforddictionaries.com/definition/risk

Peck, H. (2010). Supply chain vulnerability, risk and resilience. In D. Waters (Ed.), *Global logistics: new directions in supply chain management* (pp.192-207). London: Kogan Page.

Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics: Research and Applications*, *9*(2), 127-142.

Peck, H. (2005). Driver of supply chain vulnerability: an integrated framework. *International Journal of Physical Distribution & Logistics Management*, *35*(3/4), 210-232.

Pfohl, H.-C., Köhler, H., and Thomas, D. (2010). State of the art in supply chain risk management research: empirical and conceptual findings and a roadmap for the implementation in practice. *Logistics Research, (2)*1, 33-44.

Portbase (2011). *Portbase services*. Retrieved May 19, 2011 from http://www.portbase.com/en/Portbase/Service-selector.aspx

Portic (2011). Portic's Solutions. Retrieved May 19, 2011 from http://www.portic.net/ENG/soluciones.shtml

Rao, S., Goldsby, T. J., and Iyengar, D. (2009). The marketing and logistics efficacy of online sales channels. *International Journal of Physical Distribution & Logistics Management*, *39*(2), 106-130.

Rice, J. B. and Spayd, P. W. (2005). Investing in Supply Chain Security: Collateral Benefits. *Special Report Series, IBM Center for the Business of Government*. Retrieved May 16, 2011 from http://www-03.ibm.com/procurement/proweb.nsf/objectdocswebview/fileinvesting+in+supply+chain+security+-+collateral+benefits+may+2005/$file/investing+in+supply+chain+security+-+collateral+benefits+may2005.pdf

Rice, J. B., Caniato, Fleck, J., Disraelly, D., Lowtan, D., Lensing, R., and Pickett, C. (2003). Supply Chain Response to Terrorism: Creating Resilient and Secure Supply Chains. *Interim report, MIT Center for Transportation and Logistics*. Retrieved May 11, 2011 from http://web.mit.edu/scresponse/repository/SC_Resp_Report_Interim_Final_8803.pdf

Rodon, J., Pastor, J. A., and Sesé, F. (2007). The Dynamics of an IOIS in the Seaport of Barcelona: An ANT Perspective. In T. McMaster, D. Wastell, E. Ferneley, and J. DeGross (Eds.). *Organizational Dynamics of Technology-Based Innovation: Diversifying the Research Agenda* (pp. 297-314). New York: Springer.

Rodon, J and Ramis-Pujol, J (2006). *Exploring the Intricacies of Integrating with a Port Community System*. Paper presented at the 19th Bled eConference, June 5-7, Bled.

RSM (2008). *INTEGRITY*. Retrieved June 12, 2011, from http://www.rsm.nl/home/faculty/academic_departments/decision_and_information_sciences/research/smart_port_networks/integrity

Seuring, S. (2005). Case study research in supply chains – An outline and three examples. In H. Kotzab, S. Seuring, M. Müller, and G. Reiner (Eds.), *Research Methodologies in Supply Chain Management* (pp. 235-250). Heidelberg: Physica-Verlag.

Sheffi, Y. (2005). A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Review*, *Fall*, 41-48.

Smit, S (2004). *A Comparison of Port Community Systems* (Master's thesis, Erasmus University Rotterdam). Retrieved May 16, 2011 from http://www.maritimeeconomics.com/system/files/downloads/Thesis%20SmitS.pdf

Sodhi, M. S., Son, B.-G., and Tang, C. S. (2011). Researchers' Perspective on Supply Chain Risk Management. *Production and Operations Management*, *Forthcoming*. Retrieved May 10, 2011 from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1639435

Sodhi, M. S., Son, B.-G., and Tang, C. S. (2010). *What is Supply Chain Risk Management in the perception of researchers*. Presentation at the 10th International Research Seminar on Supply Chain Risk Management, September 6-7, Loughborough.

SOGET (2011). *SOGET*. Retrieved May 19, 2011 from http://sogetccs.com/

Spekman, R. E. and Davis, E. W. (2004). Risky business: expanding the discussion on risk and the extended enterprise. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 414-433.

Stemmler, L. (2010). Risk in the supply chain. In D. Waters (Ed.), *Global logistics: new directions in supply chain management* (pp. 178-191). London: Kogan Page.

Stock, J. R., Boyer, S. L., and Harmon, S. (2009). Research opportunities in supply chain management. *Journal of the Academy of Marketing Science*, *38*(1), 32-41.

Svensson, G. (2002). A conceptual framework of vulnerability in firms' inbound and outbound logistics flows. *International Journal of Physical Distribution & Logistics Management*, *32*(2), 110-134.

Svensson, G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. *International Journal of Physical Distribution & Logistics Management*, *30*(9), 731-749.

Tang, C. S. and Tomlin, B. (2008). The power of flexibility for mitigating supply chain risks. *International Journal of Production Economics*, *116*(1), 12-27.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*(2), 451-488.

Teo, H.-H., Tan, B. C. Y., and Wei, K. K. (1997). Organizational transformation using electronic data interchange: The case of TradeNet in Singapore. *Journal of Management Information Systems*, *13*(4), 139-165.

TNO (2011). *Ambitious CASSANDRA aims to make container security more efficient and effective*. Retrieved June 12, 2011 from http://www.tno.nl/werkenbij/content.cfm?context=overtno&content=nieuwsbericht&laag1=37&laag2=69&item_id=2011-06-06%2017:59:04.0&item_id=2011-06-06%2017:59:04.0&Taal=2

Van Baalen, P. (2011). *BKMME165, lecture 6: Ports in Global Networks, Port Community Dynamics* [PowerPoint slides]. Rotterdam: Rotterdam School of Management.

Van Baalen, P., Zuidwijk, R., and van Nunen, J. (2008). Port Inter-Organizational Information Systems: Capabilities to Service Global Supply Chains. *Foundations and Trends in Technology, Information and Operations Management*, *2*(2-3), 81-241.

Van der Velde, M. (2011). *BKMME165, lecture 1: The role and function of Port Community Systems* [PowerPoint slides]. Rotterdam: Rotterdam School of Management.

Van Oosterhout, M. P. A., Veenstra, A. W., Meijer, M. A. G., Popal, N., and Van den Berg, J. (2007). *Visibility Platforms for Enhancing Supply Chain Security: a Case Study in the Port of Rotterdam*. Paper presented at the International Symposium on Maritime Safety, Security and Environmental Protection, September 20-21, Athens.

Virtuele Haven (2001). Risk Analysis of Container Import Processes. Retrieved June 30, 2011 from https://doc.novay.nl/dsweb/Get/Document-19007

Vitsounis T. K. and Pallis A. A. (2010). *Creating Value for Port Users: Port value chains and the role of interdependencies*. Paper presented at the International Association of Maritime Economists Conference, July 7-9, Lisbon.

Wagner, S. M. and Bode, C. (2006). An empirical investigation into supply chain vulnerability. *Journal of Purchasing & Supply Management*, *12*(6), 301-312.

Waters, D. (2007). *Supply Chain Risk Management: Vulnerability and Resilience in Logistics*. London: Kogan Page.

Willis, H. H. and Ortiz, D. S. (2004). Evaluating the Security of the Global Containerized Supply Chain. *Technical Report 214 (TR-214)*. Retrieved May 23, 2011 from http://www.rand.org/content/dam/rand/pubs/technical_reports/2004/RAND_TR214.pdf

Wrigley, C. D., Wagenaar, R. W., and Clarke, R. A. (1994). Electronic data interchange in international trade: frameworks for the strategic analysis of ocean port communities. *Journal of Strategic Information Systems*, *3*(3), 211-234.

Wu, T. and Blackhurst, J. V. (2009). *Managing Supply Chain Risk and Vulnerability: Tools and Methods for Supply Chain Decision Makers*. London: Springer.

Yin, R. K. (2003a). *Case Study Research – Design and Methods*. Thousand Oaks: Sage Publications.

Yin, R. K. (2003b). *Applications of Case Study Research*. Thousand Oaks: Sage Publications.

Zsidisin, G. A., Ragatz, G. L., and Melnyk, S. A. (2005). The Dark Side of Supply Chain Management. *Supply Chain Management Review*, *9*(2), 46-52.

Zsidisin, G. A., Ellram, L. M., Carter, J. R., and Cavinato, J. L. (2004). An analysis of supply risk assessment techniques. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 397-413.

Zsidisin, G. A: (2003a). A grounded definition of supply risk. *Journal of Purchasing & Supply Management*, *9*(5/6), 217-224.

Zsidisin, G. A: (2003b). Managerial Perceptions of Supply Risk. *Journal of Supply Chain Management*, *39*(1), 14-26.

Appendices

Appendix 1 Portbase – PCS services for the ports of Rotterdam and Amsterdam

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods			
Cargo declaration export EDI/Internet	B2G	Administrative tasks; Status report within ports	All port sectors
Cargo declaration import EDI/Internet	B2G	As indicated by service labeling	All port sectors
Cargo declaration status report	B2G	As indicated by service labeling	All port sectors
Customs scan process	B2G, B2B	Transport between terminal and scanner; Status report	Container
Declaration Food and Consumer products EDI/Internet	B2G	As indicated by service labeling	Every kind of veterinary cargo
Discrepancy list	B2G	Analysis whether vessel shortlanded or overlanded	Container
ECS notification	B2G	As indicated by service labeling	Container
Notification bonded warehouse	B2G	As indicated by service labeling	All port sectors
Notification dangerous goods	B2G	As indicated by service labeling	All port sectors
Notification local clearance	B2G	As indicated by service labeling	Container
Notification of arrival ECS cargo	B2G	As indicated by service labeling	Liquid and dry bulk; General cargo
Notification of arrival ECS containers	B2G	As indicated by service labeling	Container
Notification waste disposal	B2G	As indicated by service labeling	All port sectors
Pre-arrival cargo declaration import (24h)	B2G	As indicated by service labeling	Container
Pre-arrival cargo declaration import (4h)	B2G	As indicated by service labeling	Liquid and dry bulk; General cargo; Shortsea sector
Statement harbor dues	B2G	As indicated by service labeling	All port sectors
Track and trace ECS	B2G	As indicated by service labeling	Container
Transit declaration	B2G	As indicated by service labeling	All port sectors
Vessel notification	B2G	As indicated by service labeling	All port sectors
Veterinary inspection process	B2G	As indicated by service labeling	Every kind of veterinary cargo
Import and Export			
Cargo information	B2B	Travel information for container ships; Bill of Lading	Container
Discharge confirmation report	B2B	Status report on discharged vs. announced containers	Container
Discharge information	B2B	B/L and stowage information; Actual weight discharged	Liquid bulk
Discharge list	B2B	As indicated by service labeling	Container
IMA notification EDI	B2B	Forward "permission to remove"	Container
Loading list	B2B	Loading list from shipping company to terminal	Container
MRN notification EDI/Internet	B2B	Forward "Movement Reference Number"	Container
Transport order	B2B	A single standardized procedure for transport orders	Container

Service	Relation	Content	Main target sector
Rail and Road Related			
Rail planning	B2B	Information exchange (trains and their cargo in port)	Dry bulk and intermodal transport
Road planning EDI/Internet	B2B	Information exchange; Pre-plan port visits	Container
Miscellaneous			
Barge planning	B2B	Operational report	Container
User management	n/a	Companies can manage user rights for PCS	n/a

Source: Portbase (2011)

Appendix 2 Bremer Hafentelematik – PCS services for the port of Bremen

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods			
Advantage Customs (ATL@S)	B2G	Clearance, Status report, Administrative tasks	All port sectors
Advantage Local Port Order (ALPO)	B2G	Connection to port communication systems; Administrative tasks	All port sectors
Notification dangerous goods (DaCOM)	B2G	As indicated by service labeling	All port sectors
SIS (Ship Information System)	B2G, B2B	Journey data (Departure, cargo type, etc.)	All port sectors
Import and Export			
Names of services not specified	B2B	Mapping of physical flow in messages to relevant users	All port sectors
Rail and Road Related			
CODIS	B2B	Communication platform rail transport (within port)	All port sectors
Miscellaneous			
Pro Alert	B2B	Add-on for ATL@S and other services; Automatic status reports (alerts)	All port sectors

Source: dbh Logistics (2011), J. Weishaar (personal communication, February 3, 2011)

Appendix 3 DAKOSY – PCS services for the port of Hamburg

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods (ZODIAK, Import Message Platform, and Export Message Platform)			
NCTS Declaration (ZODIAK)	B2G	As indicated by service labeling	All port sectors
Summary Declaration (IMP, ZODIAK)	B2G	As indicated by service labeling	All port sectors
Import Declaration (ZODIAK)	B2G	As indicated by service labeling	All port sectors
Import Announcement (IMP, ZODIAK)	B2G	As indicated by service labeling	All port sectors
Export Declaration	B2G	As indicated by service labeling	All port sectors
Manifest Data (EMP)	B2G	As indicated by service labeling	All port sectors
Dangerous Goods Declaration	B2G	As indicated by service labeling	All port sectors
Wagon Sequence Rail (HABIS)	B2G	As indicated by service labeling	Rail
Import and Export (IMP and EMP)			
Gatepass/Release Order	B2B	As indicated by service labeling	All port sectors
Port Order Export Hamburg	B2B	As indicated by service labeling	All port sectors
Port Order Export Bremen	B2B	As indicated by service labeling	All port sectors
Export Decs Rotterdam	B2B	As indicated by service labeling	All port sectors
Bill of Lading	B2B	As indicated by service labeling	All port sectors
Consignment Data	B2B	As indicated by service labeling	All port sectors
Booking/Booking Confirmation	B2B	As indicated by service labeling	All port sectors
Manifest Data	B2B	Carrier to port and customs authorities	All port sectors
Gate-in and gate-out reports	B2B	Terminal assigns and reports gates	Containers
Load-/Discharge Report	B2B	Terminal informs other participants	Containers
Vessel Information Platform			
Ship Departures	B2B	Status information	All port sectors
Ship Arrivals	B2G	Arrival notification, Status information	All port sectors
HABIS (connection of German railway with shipping industry)			
Load Order Rail	B2B	As indicated by service labeling	Rail
Status Order Rail	B2B	As indicated by service labeling	Rail
Miscellaneous			
Pre Announcement Truck	B2B	As indicated by service labeling	All port sectors
Damage/Repair Report	B2B	Between terminal and carrier	All port sectors
Status Messages	B2G, B2B	Status reports on all services	All port sectors
Invoicing	B2B	Terminal to forwarder	Container

Source: Dakosy (2011)

Appendix 4 Destin8 – PCS services for the port of Felixstowe

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods			
Names of services not specified	B2G	Gateway for all communication with port and customs authorities (incoming and outgoing); Status reports	All port sectors
Import and Export			
Import (names of services not specified)	B2B	Receipt of manifest data and distribution of information to relevant stakeholders; Issuance of delivery instructions and physical delivery from port; Nomination of clearing agents and road haulers	All port sectors
Export (names of services not specified)	B2B	Pre-notifications; Reports for changes in status and operational activities; Loading completed; Info on consignment loaded	All port sectors
Consolidations			
Names of services not specified	B2B	Organization and control of unstuffing and re-stuffing of containers	Container
Transshipments			
Names of services not specified	B2G, B2B	Bridging of import and export procedures to control transshipments	All port sectors
Warehousing			
Names of services not specified	B2G, B2B	Information regarding containers moved from port to warehouses (whereabouts of container for companies and customs)	Container
E-commerce			
Names of services not specified	B2B	Added value to information in system in order to allow users to reap full benefits of e-commerce	All port sectors

Source: MCP (2011)

Appendix 5 SOGET – PCS services for the port of Le Havre

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods			
Vessel Traffic & Harbor Master Mgmt System (VTM)	B2G	Content of services not specified	All port sectors
Import Control System (ICS)	B2G	ENS creation and amendment; ENS diversion message notification; Arrival notification; Receipt, translation, and transmission of customs responses	All port sectors
Cargo Community System (CCS)			
Names of services not specified	B2G	Identification of overlanded/shortlanded goods; Writing-off manifests; Tracing goods; Transmission of voyage data; Berth request handling; Authorization	All port sectors
Names of services not specified	B2B	Submission of manifest; Information on shipments, gate-in, gate-out, discharge, loading, release, stuffing, stripping, etc.; Send and receive transport orders	All port sectors
Intermodal Management System (IMS)			
Names of services not specified	n/a	Content of services not specified	n/a

Source: SOGET (2011)

Appendix 6 PortIC – PCS services for the port of Barcelona

Service	Relation	Content	Main target sector
Government Declaration and Dangerous Goods			
Names of services not specified	B2G	Vessel notification; Transit declaration; Pre-arrival notification; Waste notification; SAD information; Customs clearance and notification	All port sectors
Import and Export			
Import (names of services not specified)	B2B	Transport order; Notification of cargo collection; Notification of empty-container collection; Shipment confirmation request; Request for dockers; Summary declaration; Shipment confirmation and pro forma invoice; Telematic invoice; Electronic payment	All port sectors
Export (names of services not specified)	B2B	Transport order; Container collection note; Container delivery note; Notification of cargo delivery; Notification of empty-container collection; Request for dockers; Manifest	All port sectors

Source: Portic (2011)

Appendix 7 Questionnaire for freight forwarder (risk management)

For this questionnaire, cross-border maritime container transport refers to both, import and export activities. Further, it comprises pre-transport to the port of loading and follow-up transport from the port of destination. Sea-to-sea as well as inland transshipment are not considered.

General questions

1. On a scale from 1 to 5, how exposed do you consider your company to risks in the cross-border maritime container transport? (1 being the lowest and 5 the highest)
2. On a scale from 1 to 5, how active do you consider your company in managing risks in the cross-border maritime container transport? (1 being the lowest and 5 the highest)
3. To what extent is top management supporting and encouraging SCRM in your company? Can you give examples or indicators for that?
4. Does your company have a reactive or a proactive approach to managing risks concerning the cross-border maritime container transport?
5. Besides the criteria in question 4, how would you describe your company's risk strategy regarding e.g. risk attitude, goals in risk management, methods, and procedures?
6. Regarding the cross-border maritime container transport, how much cooperation and mutual trust, especially concerning the sharing of (risk-relevant) information, does your company experience in relationships with other supply chain members? Both ways are relevant, from your company as well as from other supply chain members.
7. How comfortable is your company regarding the sharing of risk-relevant information on supply chain visibility platforms (e.g. port community systems)?

Academia breaks supply chain risk management down into three processes: *identifying risks* (capturing actual data from supply chain), *analyzing risks* (comparison of actual and target data), and *responding to risks* (communication of trigger when induced; definition and execution of responses)

Identifying risks

8. What supply chain risk sources are relevant for your company concerning the maritime container transport and how common are these risk sources? (General categories of supply chain risk sources: organizational, network, environmental)
9. What risks to physical, information, or financial flows are associated with these risk sources?
10. At what level do these risks affect your company: operational (day-to-day business), tactical (reoccurring issues in planning and execution), or strategic (refers to the overall performance of the supply chain)?
11. Of the supply chain risks (sources) that are relevant for your organization, which ones are the (five) most important? Why?
12. What information is needed to identify the risks (sources) discussed in the previous question?
13. Is your company using port community systems (PCSs) to identify risks (sources)?
    - If so, what information is provided by PCSs?
    - If so, are PCSs effective in identifying risks (sources)? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?
14. Is your company using any other information systems to identify risks (sources)?
    - If so, what information is provided by these systems?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?

15. How far in the supply chain can you see with the information systems you use? Please differentiate between the information systems.
    - Is it sufficient?
    - If not, what would you consider to improve the range of the tools?
16. Any follow-up comments regarding risk identification?

Analyzing risks

17. How are risks analyzed in your company? What are the results of risk analysis?
18. Is your company using PCSs to analyze risks?
    - If so, what is the role of PCSs in that process?
    - If so, are PCSs effective in that process? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?
19. Is your company using any other information systems to analyze risks?
    - If so, what is the role of these systems in that process?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?
20. Any follow-up comments regarding risk analysis?

Responding to risks

21. To what extent are risk responses automated in your company (e.g. trigger communication, alert messages to other member of the supply chain, standardized responses which are executed automatically)?
22. Is your company using PCSs to respond to risks?
    - If so, what is the role of PCSs in that process?
    - If so, are PCSs effective in that process? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?

23. Is your company using any other information systems to respond to risks?
    - If so, what is the role of these systems in that process?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?
24. Any follow-up comments regarding risk response?

Port Community Systems

25. In general, what role (function) and scope (extent of services) do port community systems currently play in supply chain risk management regarding maritime container transport?
26. What role and scope can port community systems play in supply chain risk management in the future? Why?

Appendix 8 Questionnaire for freight forwarder (operational level)

For this questionnaire, cross-border maritime container transport refers to both, import and export activities. Further, it comprises pre-transport to the port of loading and follow-up transport from the port of destination. Sea-to-sea as well as inland transshipment are not considered.

General questions

1. Please provide a brief overview and description of the processes your company is involved in concerning the cross-border maritime container transport (refer to overview provided by interviewer).
2. What main information flows are associated with the described processes in question 1 (refer to overview provided by interviewer)?
3. Questions regarding information flows as provided by interviewer:
    - Do freight forwarders receive a gate-out notification from terminal operators POL (loaded on ship) and POD (loaded on follow-up transporter)? In POD, does Gate-out information possibly come from follow-up transporter?
    - Who “books” terminal operator, freight forwarder or shipping line?
    - Who registers container in harbor/with port community system (possibly called “harbor data set” used by terminal operator, shipping line, and customs)?
    - Who sends customs clearance notification (import release) to shipping line and terminal, customs or freight forwarder import side?
    - Who gets invoiced for export and import approval by customs? Who has initial outlay and who pays finally?
    - Payments in general: what is in responsibility of freight forwarder? (insurance, shipping line, pre- and follow-up transporter, customs)
    - Who insures freight (container) in transit? If freight forwarder, at what point does it insure container?
4. Is the information/document transfer fully automated/electronically (information systems) or are certain parts still done “by hand”?

5. If so, what EDI systems are used to send documents to
    - Affiliates
    - External supply chain members?
6. Regarding B/L in detail, do you use the BOLERO system or any other system to send it to other supply chain members?
7. On a scale from 1 to 5, how exposed do you consider your company to risks in the cross-border maritime container transport? (1 being the lowest and 5 the highest)
8. On a scale from 1 to 5, how active do you consider your company in managing risks in the cross-border maritime container transport? (1 being the lowest and 5 the highest)
9. To what extent is top management supporting and encouraging SCRM in your company? Can you give examples or indicators for that?
10. Does your company have a reactive or a proactive approach to managing risks concerning the cross-border maritime container transport?
11. Regarding the cross-border maritime container transport, how much cooperation and mutual trust, especially concerning the sharing of (risk-relevant) information, does your company experience in relationships with other supply chain members? Both ways are relevant, from your company as well as from other supply chain members.

Academia breaks supply chain risk management down into three processes: *identifying risks* (capturing actual data from supply chain), *analyzing risks* (comparison of actual and target data), and *responding to risks* (communication of trigger when induced; definition and execution of responses)

Identifying risks

12. What supply chain risk sources are relevant for your company concerning the maritime container transport and how common are these risk sources? (General categories of supply chain risk sources: organizational, network, environmental)
13. What risks to physical, information, or financial flows are associated with these risk sources?

14. At what level do these risks affect your company: operational (day-to-day business), tactical (reoccurring issues in planning and execution), or strategic (refers to the overall performance of the supply chain)?
15. Of the supply chain risks (sources) that are relevant for your organization, which ones are the (five) most important? Why?
16. What information is needed to identify the risks (sources) discussed in the previous question?
17. Is your company using port community systems (PCSs) to identify risks (sources)?
    - If so, what information is provided by PCSs?
    - If so, are PCSs effective in identifying risks (sources)? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?
18. Is your company using any other information systems to identify risks (sources)?
    - If so, which systems and what information is provided by these systems?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?
19. How far in the supply chain can you see with the information systems you use? Please differentiate between the information systems.
    - Is it sufficient?
    - If not, what would you consider to improve the range of the tools?
20. Any follow-up comments regarding risk identification?

Analyzing risks

21. How are risks analyzed in your company? What are the results of risk analysis?

22. Is your company using PCSs to analyze risks?
    - If so, what is the role of PCSs in that process?
    - If so, are PCSs effective in that process? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?
23. Is your company using any other information systems to analyze risks?
    - If so, what is the role of these systems in that process?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?
24. Any follow-up comments regarding risk analysis?

Responding to risks

25. To what extent are risk responses automated in your company (e.g. trigger communication, alert messages to other member of the supply chain, standardized responses which are executed automatically)?
26. Is your company using PCSs to respond to risks?
    - If so, what is the role of PCSs in that process?
    - If so, are PCSs effective in that process? What would increase the systems' effectiveness?
    - If not, why not and what else is needed?

27. Is your company using any other information systems to respond to risks?
    - If so, what is the role of these systems in that process?
    - If so, which ones are effective? What would increase the systems' effectiveness?
    - If so, are any of these systems used in combination with PCSs?
        - If so, is that combination effective? What would increase the effectiveness?
    - If not, why not and what else is needed (applies to both, whether other systems are used and whether they are used in combination with PCSs)?
28. Any follow-up comments regarding risk response?

Port Community Systems

29. In general, what role (function) and scope (extent of services) do port community systems currently play in supply chain risk management regarding maritime container transport?
30. What role and scope can port community systems play in supply chain risk management in the future? Why?

Appendix 9 Questionnaire for Portbase

For this questionnaire, cross-border maritime container transport refers to both, import and export activities. Further, it comprises pre-transport to the port of loading and follow-up transport from the port of destination. Sea-to-sea as well as inland transshipment are not considered.

General questions (1/2)

1. Where do you see the main risks and their sources in the cross-border maritime container transport?
2. Supply chains comprise three types of flows: physical (goods), information, and financial flow. How do you consider the information content of port community systems (PCSs) regarding these flows?
3. In general, is the average user of a PCS rather small and regionally focused or a big multinational with world-wide operations?
4. Are multinational companies the main target group for PCSs or do such systems rather focus on mid-sized and small companies as such do not have capabilities of internal visibility systems/connections to other systems (e.g. customs)?

Academia breaks supply chain risk management down into three processes: *identifying risks* (capturing actual data from supply chain), *analyzing risks* (comparison of actual and target data), and *responding to risks* (communication of trigger when induced; definition and execution of responses)

Identifying risks

5. How does a PCS support the identification of risks (sources) in the cross-border maritime container transport? What services relate to that?
6. Is Portbase aiming at providing services that support risk identification? What services can be related to that stage of the management and control loop?
7. Have system users required special system features to use in risk identification?
8. Has Portbase received any user feedback regarding the applicability of provided data for risk analysis?
9. Is Portbase currently developing or implementing new services that further support risk identification?

10. Does Portbase incorporate any data from third party information systems/visibility platforms (not only clients' in-house systems) to facilitate risk identification regarding the maritime container transport?
11. Does Portbase provide any data to third party information systems/visibility platforms (not only clients' in-house systems) to facilitate risk identification in detail and supply chain visibility in general?
12. Any follow-up comments regarding port community systems and risk identification?

Analyzing risks

The same questions as for "Identifying risks" also apply here and the two following are added:

13. Do companies provide target data (KPIs) to Portbase (PCSs in general) for the system to compare it to as-is data (actual) and warn about deviations?
14. With reference to the previous question, do companies show a general reluctance to supply Portbase (PCSs in general) with sensitive
    - operational data
    - management data (targets)

Responding to risks

The same questions as for "Identifying risks" also apply here and the following is added:

15. Are alert messages (text messages and mails) representing readiness or exception alerts?

General questions (2/2)

16. To which stages of the monitor and control loop would you allocate the existing services Portbase offers?
    - Identifying risks: Capture and storage of actual data (and target data)
    - Analyzing risks: Comparison of actual data and targets
    - Responding to risks: Communicate trigger, induce response procedure
17. From your perspective, what other IT systems facilitate the risk management of supply chain members in the cross-border maritime container transport?

18. With reference to the previous question, to which stages of the monitor and control loop would you allocate their services/information offerings?
19. In general, what role (function) and scope (extent of services) do port community systems currently play in supply chain risk management regarding maritime container transport?
20. Do you see differences in the role and scope of PCSs regarding supply chain risk management related to
    - Size (multinational vs. small local company)
    - Territorial focus (doo-to-door activities vs. local port operations)?
21. What role and scope can port community system play in supply chain risk management in the future? Why?
    - Is it preferable to become a (maritime) supply-chain wide visibility platform or rather to be feeding such platforms with relevant data?
    - Is there a general ambition to share data among PCSs in order to increase supply chain visibility? Is that even feasible in the light of competition, data ownership, etc.?
22. Is Portbase (PCSs in general) widening its scope to include hinterland activities – e.g. inland terminals, pre-transport, follow-up transport?

Appendix 10 Questionnaire for customs authority

For this questionnaire, cross-border maritime container transport refers to both, import and export activities. Further, it comprises pre-transport to the port of loading and follow-up transport from the port of destination. Sea-to-sea as well as inland transshipment are not considered.

1. From a customs' perspective, what general risks to the physical, financial, and information flow are affiliated with the cross-border maritime container transport?
2. From the perspective of freight forwarders, what general risks to the physical, financial, and information flow are affiliated with the cross-border maritime container transport?
3. What risks do freight forwarders face when dealing with customs regarding the cross-border maritime container transport?
4. How do you evaluate the supply chain risk management approach of freight forwarders?
5. In what aspects does the supply chain risk management of freight forwarders in the cross-border maritime transport of containers need to improve?
6. What third party information systems are connected with the customs' internal systems?
7. What kind of information (blocks) is (are) exchanged?
8. Are port community systems the preferred information system for data transfer regarding IT-supported customs procedures between port companies and customs authorities? What other systems are possibly accredited?
9. What criteria does a system have to fulfill in order to be accredited for data transmission regarding customs clearance processes?
10. What other systems (besides Portbase) are accredited for data transmission regarding customs clearance processes?
11. From the customs' (government's) perspective, do you have a preference for community solutions or single entity solutions regarding supply chain visibility platforms? Also regarding customs clearance and data feed into customs portal.
12. With reference to the previous question, is one of the solutions easier to control/supervise?

13. What kind of information from authority systems (e.g. customs) could be relevant for the risk management of freight forwarders regarding the cross-border maritime container transport?
14. With reference to the previous question, what kind of risks (sources) does the information address: operational (day-to-day business), tactical (reoccurring issues in planning and execution), or strategic (refers to the overall performance of the supply chain)?
15. In general, what role (function) and scope (extent of services) do port community systems currently play in supply chain risk management regarding cross-border maritime container transport?
16. What role and scope can port community systems play in supply chain risk management in the future? Why?
17. With reference to the previous two questions, are PCSs the appropriate information system/information broker to connect government requirements regarding SCRM with supply chain requirements? If so, why? If not, why not and what other system is more suitable?