INFORMATION SHARING AND RISK OVER INTERNATIONAL TRADE LANES
The Case of FloraHolland
S. Morales Velasquez
Information Sharing and Risk over International Trade Lines
The Case of FloraHolland - Public Version

by

S. Morales Valesquez

to obtain the degree of Master of Science
at Delft University of Technology,
to be defended publicly on Tuesday August 25, 2015 at 9:30 AM.

Information:
Author: Santiago Morales Velasquez – 4296419
         s.moralesvelasquez@student.tudelft.nl
Date: August 25, 2015

Academic Information:
University: Delft University of Technology
Faculty: Technology Policy & Management (TPM)
Master Programme: Management of Technology (MoT)
Graduation Section: Information & Communication Technology (ICT)

Graduation Committee:
Chairman: Prof.dr. Yao-Hua Tan
First Supervisor: Dr. Joris Hulstijn
Second Supervisor: Dr.ing. Bram Klievink
FloraHolland Supervisor: Roel Huiden

An electronic version of this thesis is available at http://repository.tudelft.nl/.
The research was performed from February to August 2015 and was a joint project between Delft University of Technology and FloraHolland. This Master Thesis corresponds to my last project before graduating from my master of programme in Management of Technology in the faculty of TPM (Technology, Policy and Management). The research was done at the ICT section.

This study lies within the fields of supply chain and risk management and aims to evaluate the applicability of a new chain assurance model that was developed as a way to improve the risk assessment in supply chain processes. In this case the study was going to be done in one of the main trade lanes to import flowers of FloraHolland. This objective of the research was reached based on a correlation between an extensive analysis of the extant literature and the analysis of the aforementioned case study.

This project would not have been possible to execute correctly without the good supervision and support from a great group of people whom I need to thank.

Firstly, many thanks go to my supervisor from from FloraHolland Roel Huiden, who welcomed me to the company and made it possible for me to graduate in this great company. Further, he was highly active in supporting my work and every activity performed.

During these seven to eight months of work, I referred to many people both within and outside FloraHolland who were kind enough to take the time to help my research with their input in the process for what I am really grateful.

Many thanks as well go to my all supervisors in TU Delft: Joris Hulstijn, Yao-Hua Tan and Bram Klievevink for taking the time and effort to guide me in the right direction every time I needed it and having the proper feedback for me to continue the research in the correct way.

Finally, but not less important, I also want to thank both my family in Colombia as well as the new Dutch family (a great group of friends), as they always gave me courage and support to continue the project no matter the problems or issues that showed in the process.

S. Morales Valesquez
Delft, August 2015
Multiple frameworks and procedures are used in organizations to analyse and assess risks in the most efficient way possible. COBIT, COSO or ISO as some of the most popular frameworks used to evaluate enterprise threats, but each of them offer an independent view on risks that are not the best solution for chains or well established organization networks that could benefit of a chain approach to assure the correct and efficient process in these integrated scenarios.

A stronger tie between actors in chain processes, increases the need to design and develop capable information platforms that support the regular and continual exchange of information in the supply chain and assess the risks associated with the development of this integrated network. This research aims to evaluate the applicability of an integrated assurance approach on a complex trade lane as a solution to manage and assess risks, where they aren't perceived as independent scenarios but dependent of the environment. The CANTOR approach refers to ‘Chain Assurance Network Transference of Obligations and Risk-Control’ and it is basically a model that aims to provide guidance on establishing assurance in chains by approaching the complete process and all the actors involved as one virtual organization.

This will be done by analyzing the Kenya trade lane by Air of FloraHolland and validating the current state of the chain and the possible risk scenarios in the process. To reach this objective, the following research question has been defined:

*Is the CANTOR approach a suitable solution to perform Risk Management for Information sharing that copes with international regulations and trade compliances within the trade lane for shipping flowers from Kenya to the Netherlands by air?*

By combining theoretical knowledge, the analysis of current status, processes and activities and main risk scenarios in the aforementioned trade lane, a first approach on the applicability of the integrated assurance approach and governance model will be verified, exposing the gap between theory and practice, clarifying how risk management can be implemented in the Kenya trade lane with the integral approach: CANTOR.

The first part of this research consists of the gap analysis. Theory from literature review on risk management, trust, risk assurance, information integration, among others, are compared with the reality of the process state acquired through interviews with actors from the Kenya Trade Lane. The results of these interviews define the main risk scenarios of the process regarding information sharing, that will provide insight in the main points to evaluate the suitability of the integrated assurance approach.

The second part consists of the design of the structural interviews that will provide the status of the chain regarding how aligned, equipped and organized are the actors in the trade lane in order to effectively apply the integrated assurance and governance control model.

The third and final part explains either the CANTOR approach is suitable for the trade lane or not, why and both the benefits or disadvantages of implementing such an approach. To answer this main question, a complete answer is also provided for each of the four sub-questions defined for the research project.

Besides contributing to the extant body of knowledge by providing a certain amount of empirical evidence, the study is rich in practical implications for the Kenya Air trade lane of FloraHolland and the information shared in the process. The conclusions could be used for further research, and the final recommendations could be used as additional findings to be considered by future projects that want to evaluate the suitability of the integrated assurance approach in other processes.
CONTENTS

Preface iii
Executive Summary v
List of Figures ix
List of Tables xi

1 Introduction 1
1.1 Problem Description ............................................. 1
1.2 Research Objective ............................................. 3
1.3 Research Question and Relevant Subquestions ..................... 4
1.4 Research Approach ............................................. 4
1.4.1 Problem .................................................. 5
1.4.2 Analysis .................................................. 5
1.4.3 Solution .................................................. 7
1.4.4 Conclusion ................................................ 7

2 Literature Review 9
2.1 Risk Management .............................................. 9
2.1.1 Risk Identification ......................................... 10
2.1.2 Risk Assessment .......................................... 11
2.1.3 Risk Mitigation .......................................... 12
2.1.4 Risk Evaluation .......................................... 12
2.1.5 Risk Monitoring .......................................... 13
2.2 Organizations and Risk ......................................... 13
2.2.1 Risk & Decision Making ................................... 14
2.3 Risk Management Frameworks .................................. 14
2.3.1 COSO Enterprise Risk Management - Integrated Framework .... 15
2.3.2 ISO 31000 ................................................. 16
2.3.3 COBIT ................................................... 17
2.4 Chains Dependencies .......................................... 18
2.4.1 Supply Chain Operations Reference (SCOR) .................... 19
2.5 Risk Organizational Trust ...................................... 20
2.6 Risk Assurance ............................................... 21
2.7 Supply Chain Information Integration ............................ 21
2.7.1 Document Sharing ....................................... 24
2.8 Towards Integrated Risk Management (CANTOR) .................. 24
2.9 Summary and Gap Analysis .................................... 27

3 Process Analysis 29
3.1 Stakeholders Analysis .......................................... 29
3.2 Process Description ........................................... 33
3.2.1 Process 1: Document Preparation .......................... 33
3.2.2 Process 2: Shipment Approval .............................. 34
3.2.3 Process 3: Carrier Arrangement ............................ 34
3.2.4 Process 4: Entry Process .................................. 34
3.2.5 Process 5: Import Process ................................ 35
3.2.6 Process 6: Customer Delivery ............................. 36
# List of Figures

1.1 Thesis division .......................................................... 5  
1.2 Research analysis goals ............................................ 6  
1.3 Research design .................................................... 7  

2.1 Overview of the rise management process ........................ 10  
2.2 Risk taxonomy group, [25] ........................................ 13  
2.3 General framework of risk management [26] ..................... 15  
2.4 IT Risk Categories [32] .............................................. 18  
2.5 SCOR Framework Levels [48] ..................................... 19  
2.6 Model of Trust [45] .................................................. 20  
2.7 Supply Chain Conceptual Model [41] ............................. 22  
2.8 Data Pipeline Conceptual Model [38] ............................ 23  
2.9 SCN SDN ........................................................... 25  
2.10 The chain atom approach [72] .................................... 25  
2.11 TORC [72] ........................................................... 26  
2.12 CICS [72] ........................................................... 26  

4.1 Kenya Air Trade Lane Risk Scenarios Matrix .................... 44  

5.1 CANTOR Components [73] ......................................... 47  
5.2 Chain Assessment and Hypothesis Structure [73] ................ 49  

A.1 Overview of FloraHolland's Kenya Air Trade Lane ............... 65
LIST OF TABLES

3.1 Overview of Information and Communication Systems in the Kenya Trade Lane ............ 37
Chapter 1 describes the research problem, which helps to frame the scope of the study and explains the goals to achieve. First we introduce the research subject followed by the description of the problem analysis, research objectives, methodology and the structure of the research. Additionally, the conceptual designs of the research are addressed, picturing the main aspects of the research and what is required to effectively find a sound answer to the set of research questions.

1.1. Problem Description

Information technologies (IT) have impacted and changed the way business is done around the world. With the capability to provide accurate and reliable information, companies rely on IT to improve their performance [41]. In the same grain, IT also has impact on the improvement of supply chain management (SCM) and the way information is shared among involved actors, when the supply chain integration is the main goal. “Information integration refers to the sharing of key information along the supply chain network which is enabled by information technology. One of the main purposes of information integration is to achieve real-time transmission and processing of information required for supply chain decision making” [56].

A stronger tie between actors in a supply chain increases the need to design and develop capable IT platforms that support the integration in the supply chain and assess the risks associated with the development of this integrated chain. By integrating the capabilities of the companies in the supply network, both data and information sharing become more immediately useful, that also allows the company to effectively create unique value, which is maximized when the supply network acts in unity, almost as if it was one organization in the marketplace [34].

As mentioned, in these integrated chains, companies deepen their relationship with partners and thus become more dependent on each other, and although there are many benefits and opportunities in integrated supply chains, there are also several risks that need to be addressed as well; information sharing is one of them. Non-disclosure of information, inappropriate disclosure, lack of information quality, lack of use of security, are some of the risks associated with chain integration that may impact upon the organisation.

Within these risks that emerge in integrated chains one concept becomes important to outline: trust, which can be defined as “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party” [45]. In cooperative supply chains it becomes important mainly due to the fact that it supports the level of formal norms and regulations that will backup the process and connections within organizations: if one party fails as a trusted actor, formal control mechanisms need to be implemented, therefore also affecting the risk levels on the chain.

To cope with the risks, different models, standards and frameworks have been established (i.e. ISO/IEC 27005, Cobit5 or COSO ERM) by diverse organizations that help enterprises in achieving their objectives for governance and management of the enterprise IT and guidance for risks management. As an example, Cobit5 for
Risk increases the enterprise risk-related capabilities and helps understanding how effective IT risk management optimises the business processes and value, improving the quality and reduced waste and costs [32].

Each of these mentioned models and frameworks are mostly focused in a single enterprise and the management of the risks over its processes, which can be hardly implementable to build the risk framework for an integrated chain. In this collaborative environments or scenarios is common to have several companies with their own objectives and goals, stating different risks that need to be handled and controlled, and where some of them are mutually dependent within the network of organizations; factors that are not considered in the above standards.

To analyse the processes and risks in an integrated supply chain and validate the dependencies inside the network the CANTOR approach was developed. CANTOR refers to ‘Chain Assurance Network Transference of Obligations and Risk-Control’ and is a model that basically aims to provide guidance on establishing and sustain assurance in chains [73]. The model works under four new concepts that help to implement the assurance evaluation [72]:

1. **Atomic approach of a service chain**: Validate the chain in its smallest possible way.

2. **Transference of Obligations of Risk and Control (TORC)**: Align and balance the different actors and frame the chain as a whole.

3. **Chain Internal Control System (CICS)**: Internal control based on the concept of “virtual” organization of the whole chain.

4. **Chain Governance**: Definition of Chain Policies, Chain Risk-Management and Chain audit and monitoring.

In chain integration processes, the bigger the number of actors the harder it can be to synchronize every stakeholder and direct them to a common goal. This situation will be further exposed and can be seen in the case study that will be portrayed in the report.

The selection of the case study was done with the guidance of the supervisors of the project, as they have been involved in different projects that encompass the optimization of supply chains by trying to reduce the amount of controls and checks in different processes. For this research it is required a trade lane process that have several actors involved, multiple points of information and documents exchanged, various control points and regulations to follow, so the chain assurance can be evaluated as a way to improve the process.

The air trade lane for the import of flowers from Kenya to the Netherlands is one example of a complex supply chain process in which multiple actors are involved and require the deep analysis to identify all the risks within the process. This is the case of FloraHolland in the Netherlands, which, through the CORE project, has been promoting the awareness of trade compliance, transparency and improvement of the levels of control over the supply chain.

FloraHolland is a Dutch cooperative founded in 1911 by several Dutch growers that decided to associate to be able to find better market possibilities. Nowadays, with more than 4500 members (of which 600 non-dutch), and 2400 customers, the company works as a facilitator and mediator in the distribution and trade process of flowers throughout the world. As part of its activities, besides the commercialization of flowers harvested in the Netherlands, FloraHolland also eases in the importation process of products from different parts of the world (i.e. South America and Africa), which also puts them in interaction with various actors in the supply chain (SC).

As a way to optimise the supply chain, improve the service levels with the customers and have a faster and more reliable process, both information transparency and risk management are important to consider and assess. For this, FloraHolland is in constant information exchange with several of these actors in the chain: suppliers, shipping agencies, logistic service providers (LSP), customs, plant health inspection agencies, and other protection organizations, etc.

2
By participating in the Core project \(^1\), both FloraHolland and some of the stakeholders involved in the trading process, are in constant analysis of improving supply chain transparency and efficiency and the role of IT to share and exchange its information; trust creates an environment that allows the firms to increase the likelihood of mutual benefits \([18]\). And with the idea to develop this type of platform, the company got involved in the CORE project (based on a previous EU project named CASSANDRA \(^2\)).

Both CORE and its predecessor (the CASSANDRA project finished in August 2014) were developed with the main purpose of improving the supply chain visibility, addressing the needs of both business and government in the international flow, by developing a data-sharing concept that allows an assessment of risks for every actor in the process. At the end, it brought key concepts like “trusted trade lane” or “data pipeline”, that allows to improve supply chain visibility, by providing one integrated access point to all the different sets of information that already exists in the supply chain, improving the efficiency of trade compliance and effectiveness of border control and supervision \([38]\).

The assessment of the information sharing risks over the chain to improve and standardize the whole process consists a complex problem. Its complexity lays mainly in the fact that a great number of stakeholders are involved in the flower importation process: from the growers to the LSPs and customs; and each of them use different approaches and practices to evaluate the several risks that can be presented over the chain. Without proper chain integration, the decisions made by one of the actors in order to assess a risk can have greater effect on the others.

Because of this complexity in the trade lane, is also important to identify the risk scenarios that makes the possible threats more understandable and shows the lack of alignment that can exist between the partners in the chain or the misuse and misplacement of key data that allows the risk to leads to operational or administrative loss. A total of three critical risk scenarios will be defined.

From the aforementioned scenario it becomes clear that the absence of an integrated risk assessment over the information shared in the trade lane makes it difficult for all the involved actors to have a well defined and clear process regarding information safety and visibility as well as standard communication channels; which is the problem that this research seeks to solve, by implementing and evaluating an integrated assurance approach on a complex trade lane to validate the applicability of integrated solutions to manage and assess risks, where they aren't perceived as independent scenarios but dependent of the environment. The CANTOR approach is presented as the solution to validate the integrated assurance position and to assess the different information sharing risks in the chain.

### 1.2. Research Objective

With the clear problem statement that there is no existing proved model that provides an integrated assurance approach for information shared in chains processes, the main objective of the thesis project is to evaluate the applicability and verify how suitable the CANTOR approach is in order to assess the information sharing risks that can emerge in the FloraHolland's trade lane for the importation of flowers from Kenya by air.

To achieve the main objective, some research activities will be held in eight main topics:

1. Illustrate and describe the current information sharing process through the trade lade and the norms it must comply with.

2. Identify all the stakeholders in the process in order to classify their interests in the risk assessment.

3. Conduct a literature study in the existing frameworks for risk management (business, supply chain and information), as a way to provide a theoretical background and requirements for the case study, as to evaluate these frameworks against the CANTOR approach on its suitability for the case and justify the selection of the new model as the one required for the solution.

---

\(^1\) http://www.coreproject.eu/

\(^2\) http://www.cassandra-project.eu/
4. Study the main points of the CANTOR approach to understand what are the benefits over the other existing risk management models, and how it can assess the process.

5. Perform interviews that supports the identification of the most critical information-sharing risks scenarios in the Kenya trusted trade lane; prioritizing the important elements that need to be assessed.

6. Design a structured questionnaire that acknowledges the current status of the trade lane as also the applicability of the model from the geographically dispersed actors, so the information can be obtained on the required substantial scale of detail.

7. Apply the CANTOR framework for the information sharing risks scenarios based on the current state of the supply chain.

8. Evaluate the new concepts required by the CANTOR approach (Atomic approach of a service chain, Transference of Obligations of Risk and Control (TORC), Chain Internal Control System (CICS) and Chain Governance) to assess the information sharing risks in the Kenya air trusted trade lane.

1.3. Research Question and Relevant Subquestions

Derived from the main objective of this master thesis and taking into consideration the mentioned concepts the following main research question is proposed:

- **RQ0:** Is the CANTOR approach a suitable solution to perform Risk Management for Information sharing that copes with international regulations and trade compliances within the trade lane for shipping flowers from Kenya to the Netherlands by air?

This main research question can be subdivided in four relevant subquestions:

- **RQ1:** What are the stakeholders and the current process related to information sharing and border control in the Kenya trade lane by air, and the information infrastructure, main norms and policy strategies that supports it (based on the CASSANDRA outcomes)?

- **RQ2:** What are the main characteristics of the CANTOR approach that differentiate it from existing risk management frameworks and allow it to be more suitable to evaluate the study case?

- **RQ3:** What are the main and more critical information-sharing risks scenarios in order to assess the way information is transferred in the Kenya trade lane by air?

- **RQ4:** How can the CANTOR approach assess the risk scenarios established in RQ3 in order to enhance the integrity levels of the information shared across the Kenya trade lane by air?

1.4. Research Approach

As expressed before, the main objective of the research is to analyse and evaluate how suitable is the CANTOR approach to assess the information sharing risks over FloraHolland’s air trade lane from Kenya. To do so, the key definitions about risk management and the main elements of the CANTOR approach need to be analysed, so is possible to evaluate the applicability for the case study.

First, is important to explain why we chose to perform in this project a case study research. This approach allows us to have better understanding of complex situations or topics (like chain assurance or risk management), and extend the knowledge of what is already known and do the inquiry within the real-life context and applicable scenarios. The case study approach allows the project to be defined in the required contextual conditions where the main topic wants to be proven [75], in our case, the applicability of the CANTOR approach.

The thesis is divided in four parts as indicated in Figure 1.1:
1.4.1. Problem
The first part is the theoretical background of the research that includes two of the chapters of the document. Chapter 1 consists of an introduction, with the definition of the problem, research objectives and methodology; as for Chapter 2 contains the literature review.

To conduct this study, it is important to first perform a desk research, where a literature review will be conducted on the background of the main topic in the project: risk management, highlighting the main definitions and different approaches businesses and organizations implement to manage risk.

Before describing the CANTOR concepts, and in order to have a sharper theoretical/background analysis and validate the assumptions about the existing risk management frameworks, it will also be performed a literature review on them for supply chains, ICT and information sharing, as well as on the different regulations and norms these frameworks must comply to, and present why they are not sufficient to cover the requirements in the case study. Questions like ‘What is Risk Management?’, ‘How do organizations approach Risk Management?’ and ‘What are the norms Risk Management frameworks must comply on?’ will be detailed in this section. This information is the foundation to validate and analyse the gaps in the existing frameworks for risk management on both ICT and supply chain, and on that account how the CANTOR approach aims to tackle these gaps.

Once the literature review on Risk Management is finished, a new chapter of the research will explore and go in detail to define the CANTOR concepts, analysing why this model fits best to the case study and how it should resolve the gaps found in the other risk management frameworks.

Different literature will mostly be found through the university library, several academic websites like Google Scholar or Scopus and referring to experts, following the snowball method, where from a base literature, new documentation will ramify in order to detail more the required information.

1.4.2. Analysis
The second part of the research document includes two chapters that concern the analysis. Chapter 3 refers to the process analysis and the current state of the trade lane, as for Chapter 4 contains the different risk scenarios that are initially analysed and evaluated.

As a starting point, is imperative to illustrate the current state of the selected case study: the process in the air Kenya trade lane of FloraHolland, and the risk levels on it: identification of the actors, documents, communication methods, norms and information security levels are some of factors to classify. This literature can be found by exploring the state of the company (FloraHolland) by conducting internal interviews and reviewing process documentation (desk research) like previous descriptions of the trade lane, internal policies and norms, certificates and other forms used to analyse chain. For the interview process, initially emails will be exchanged with the different players of the trade lane, as also later if further information is required, it will be selected by validating with FloraHolland's supervisor the relevant players that should provide extra information.

This case study was selected after several discussions and meetings with the first supervisor, the company’s supervisor, chairman, and the CANTOR approach expert, and consensus was reached that the most suitable case, for the project time period, was the mentioned FloraHolland's Kenya air trade lane.

The selected case study has all the potential variables to evaluate the applicability of the CANTOR approach, and evaluate the chain assurance methodology; it is a complex trade lane with multiple actors involved, and
because it involved trade of plants and perishable goods, any delay or inefficiency in the process can result in low quality of the product as higher cost, and it also has to comply with multiple regulations in both countries, like both phytosanitary as well as customs policies. Unlike the sea trade lane of FloraHolland, in the air trade lane process FloraHolland, besides acting as the orchestrator and head of the chain, highly depends on some of the other parties involved in the chain (i.e. Freight Forwarder), so needs to have assurance of the different measures taken and complete visibility of the whole trade lane to monitor and examine the process.

To achieve the main research objective, the analysis and evaluation is focused in three main subjects: the risks over the trade lane, information sharing and the governance model that exist (if any) in the supply chain, hence it is possible to evaluate the application of a chain assurance approach for the information managed in the trade lane, as intended by CANTOR. The intersection of those three topics bring the goals of the analysis section; data quality, process disconnections and insurance, as illustrated in Figure 1.2.

Within the analysis of the risks in the trade lane joint with the information sharing processes we will be able to validate the quality and integrity of the data exchanged between all the actors in the process; while combined with the analysis of the governance strategies within the chain will allow us to validate the assurance methodologies and strategies that are currently implemented as a way to evaluate the current status and viability of the chain assurance and control defined with the CANTOR approach, as the built-in controls in IT systems or the different governance mechanism to mitigate risks (i.e. data pipeline). The grouping of the information sharing analysis and the governance strategies in the chain will acknowledge the disconnections in the process and both the aligned and misaligned points in the trade lane where some of the risk strategies for the assessments can be focused to improve the process.

Through the analysis of the process of FloraHolland, the possible risk scenarios regarding the exchange and distribution of information will be explored, validating the vulnerability of the chain, their impact and possible frequency. The risk scenarios will allow us to have more detailed information on both the weak link of the trade lane as also the main actors involved in the key processes. With the information and detail of the process, the identification of the risk scenarios acknowledges the critical points that require or can be benefit from the implementation of a chain assurance.

The remaining part of the research will be conducted through an analysis of the main and key risk scenarios for sharing information in the study case trade lane, defined from the entire possible risks. First, and as a way to facilitate the research process and to identify the central ones, different interviews must be conducted with the key actors in the process to detect all the points that can be considered as a liability.
To evaluate the CANTOR approach's applicability for the chain assurance, the information is mainly obtained from three different sources: the process analysis (where all the information about the current process and activities on the trade lane is collected), a survey for the parties involved in the process to validate the existing state of the trade lane, and direct and indirect interviews (i.e. emails, virtual meetings) with experts and the actors in the chain. The three sets of information are sufficient to evaluate the solution in the next section.

1.4.3. Solution
The third part of the thesis includes two chapters that will present all the practical results of the analyses. Chapter 5 presents how the trade lane risk control and assurance levels are, as also results of the analysis of the current state of the organizations. Chapter 6 elaborates later on the verification and validity of the research and the implementation of the solutions in the chain.

With the risk points properly identified, by meetings and workshops with risk management and the CANTOR expert, and the trade lane and chain specialists, a questionnaire will be developed in order to evaluate, prioritize and measure the impact and criticality of each of the risk points in order to further evaluate the primary and most critical risk scenarios. The survey will be developed based on COBIT for risk approach, and as a way to make contact with all the actors, no matter the geographical location (i.e. Kenya or Netherlands).

With the expert in the CANTOR approach and specialists in the trade lane, an analysis and risk evaluation on the main scenarios will be conducted, to validate if all the concepts and variables required by the model: Atomic approach of a service chain, Transference of Obligations of Risk and Control (TORC), Chain Internal Control System (CICS) and Chain Governance can be designed and applied in the trade lane.

1.4.4. Conclusion
The fourth and last part of the report consists of Chapter 7, which after the analysis in the previous chapters, provides answers to the research questions and defines the overall theoretical contributions. The expected results from the aforementioned studies will be used to answer the main research question, since from these results the necessary information to analyse and evaluate the CANTOR approach in the trade lane are expected to arise.

The chapter also specifies short term and long-term recommendations and possible future researches, as also a personal reflection on this research.

This research process is summarized in Figure 1.3 below, where it is divided in three different parts: literature review, identification of the chain needs and the analysis and evaluation of the framework.

![Figure 1.3: Research design](image)
In this chapter, a broad presentation about Risk Management is given, specifically for Supply Chain and assurance. The definition of risk is introduced, as well as how it has evolved though time, the different phases to manage it and the potential benefits for organizations. We also discuss some of the implementing strategies and frameworks to assess risks in information technologies (IT) and supply chains, like COSO, ISO31000 or COBIT.

Additionally, we explore the concept of trust and how it impacts organizations and the risk scenarios that can emerge. Also, the gap between the current risk management approaches for both IT and supply chains and a new risk management approach for integrated chains is explored, presenting the main points to evaluate in the research as how the dependencies between the different actors in a network affect the existing frameworks.

This chapter gives a general overview of what the essence of this research is. Each sub section of the chapter will have a final observation that summarizes the main idea, which helps to build the conclusion with what is intended to be achieved.

2.1. Risk Management

Before describing more in detail the concept of risk management, it is important to define first the term risk by itself; in simple words, it can be said that risk is a situation where an individual is exposed to an event with negative consequences. But according to Ulrich Beck on his book Risk society: Towards a new modernity, "risk may be defined as a systematic way of dealing with hazards and insecurities induced and introduced by modernization itself. Risks, as opposed to other dangers, are consequences which relate to the threatening force of modernization and to its globalization of doubt." [9].

Changes in work, organizations or even routine activities and characteristics can be considered the modernization of the everyday life, and a society increasingly concerned and preoccupied with the future and safety of this modernization, is what generates the notion of risk. The risks of today world are different, in an essential way, from the similar ones in the Middle Ages mainly because the global nature of the possible threats at that time (i.e. people, animals and plants) and also because new modern causes: risks of modernization, being a product of industrialization [9]. Managing and dealing with these risks has become increasingly important in today's organizations, and consequently different risk management techniques have been developed, accordingly to different processes and areas. In general terms, firstly, it can be said that risk management is the process by which an individual (or organization) attempts to ensure the risk to which is exposed are those risks to which the individual thinks it will be exposed and is willing to be exposed in order to lead the process or activity they want [17].

All of the techniques, methodologies or processes for risk management have the basic idea of carrying out decisions and assessments to minimize negative effects or losses, due to the fact that "it is simply not possible to avoid taking risks. In every human decision or action the question is never one of whether or not to take a risk but rather which risk to choose. Individuals, organizations and governments confront essentially the same
Based on the fact that risk determinations are based on mathematical possibilities and social interests, especially, if they are presented with technical certainty, different organizations and sectors started to differentiate and separate risk analyses according to the type and area of impact [9]. Mainly, it can be differentiated between two types: the management of business risks—referred to the risks primarily in financial and insurance fields, with main focus on economic gains and losses—and management of operational risks, focused in the concerns with the uncertainties in the execution of the different activities the organization perform in order to fulfill their goals: like quality, security or safety [59]. But resulting from the growing interest on risk management of many other sectors, nowadays it can be seen different approaches to risk management which started to play a significant role behind the growth of an organization in the long term. Besides the already mentioned operational risk management (focused on quality and safety) and business and financial risk management (projects, portfolios, market and economy), it can now be also seen a more detailed risk management focused in engineering and technical processes (Software development, supply chain, construction, among others).

Risk management in organizations was first only related to the operational section, where it was mainly a discipline under the safety engineering practices and the technical certainty, mainly concerned with physical harm as result of the equipment and operators’ performance. But this view has evolved, and modern risk management has now a bigger scope, mainly due to factors like the increase in the degree of complexity in the different business processes, the transition towards knowledge-intense type of work and the central role of technology [59]. Making these assessments requires all the activities commonly seen in process and project management: identification, analysis, implementation, evaluation and monitoring, with regard to risks.

Before explaining further on risk identification, assessment, evaluation and ultimately management, it is important to recognize the fact that risk is a perceived issue that sometimes doesn’t necessary means actual risk: “individuals, organizations and governments make decisions based on perceptions about the likely consequences may not be recognized, there may be a gross misconceptions about the likelihood or magnitude of those that are recognized, and yet other perceived consequences may be more imagined than real” [3]. Missed and misconstrued perceptions of the consequences of different decisions are of themselves a major (and possible the main) source of risk in decision making, situation which makes management of risk central to the livelihood and success of all organizations, where any responsible decision maker will work to obtain a complete accurate perception of the diverse set of risks faced before attempting to undertake a full analysis and assessment [3].

Most of the risk management standards and framework can be explained in three different phases [24] [68] [63], as shown in Figure 2.1.

![Figure 2.1: Overview of the risk management process](image)

### 2.1.1. Risk Identification

Inside the risk management process, the identification of the possible outcomes of the different decisions is known as the risk identification phase, where the examination of the complete system or process is done (verifying the elements and their relationship); which involves also outlining together several disciplines, depending on the issue addressed, such as engineering methodologies, statistics, sociology, economics, etc. [60].

According to O. Renn (1985) [60], there are four distinctive approaches to risk identification:

- **The engineering approach** is basically orientated towards the quantification of risk, based on techno-
logical considerations.

- **Decision-analysis** techniques take into account several risk dimensions: economic and environmental losses, as well as technical factors.

- **Risk-perception** is oriented to understand the social side of risk, and recognize why people often have singular priorities to risks that differ from those that can be justified by theoretical and statistical analyses.

- **Policy-analysis** methods try to describe how social and political influences affect the design and implementation of risk policies.

According to the same author, for a good risk management there are five general main steps to follow, from where the first two steps fit the risk identification activity:

1. **Defining which outcomes or events can be labelled as risk:** Although this involves some degree of subjective and social judgment in evaluating several of the scenarios and consequences, it is important as a starting point to verify and have a complete list of possible risks.

2. **Choosing which factors are to be given priority:** There are many possible dimensions to a particular risk, and it must be chosen which are to be considered.

### 2.1.2. Risk Assessment

The risk assessment is the second part of risk management activity, where the estimation of the probabilities, the size of the outcomes and evaluation of the different alternative courses of action are the main points to discuss.

Risk is a concept mostly associated with the failure of a system, where the likelihood of a system failure is usually being understood in terms of probability [3]. The risk assessment is mainly done with the analysis of likelihood for some events to happen and the scientific methods for identifying causal links between events [15]. This has something to do with the anticipation of the unknown and the "destruction" that has not yet happened, but threatens the way organizations and society behaves [9], resulting in the combination of the probability of the stated threat or hazard and the level of magnitude of the consequences of the occurrence [24].

Mathematically speaking, the probabilities for the risk assessment can be indicated by differentiating the diverse risk scenarios (Si), the likelihood for them to happen (Li) and the consequences of each of them (Ci), where none of these mathematical concepts (by themselves) is enough to capture the general idea of risk; but the set of triplets can be set as sufficient to analyse risk, defining it with a formula that relates the three concepts as \( R = <S_i, L_i, C_i> \) [35].

As mentioned in the previous section, according to Renn (1985) [60], there are five general main steps within all the different risk management approaches and to define the probabilities of likelihood and consequences, from these steps, the last three are valid for the assessment of the risk:

1. **Evaluate the magnitude of the risks:** Once identified the events to consider, the development of the risks needs to be traced and further quantified.

2. **Calculating probabilities of the various outcomes:** This can be accomplished using several statistical methodologies. Is important to remark, that somehow they are limited by the fact they are largely based on past and known performance of the same or similar risk sources.

3. **Determining which are the actors affected by the risk:** An event can affect different people and organizations in different ways, which has led to equity issues in the distribution of risks and benefits becoming key factors in regulation.
2.1.3. Risk Mitigation

Based on the results or evaluation completed with the risk assessment, it is then required to develop the strategies to manage them and decide how the different risk scenarios can be controlled and which mitigation measures are possible. Education and attentiveness to information over the different scenarios open up new possibilities of dealing with and avoiding risks, reducing the impact and probability of it [9]. For each possible outcome or measure for the risk events there should be a cost/benefit analyses so it is possible to assess the best possible mitigation strategies.

At the end of the risk analysis and assessment processes organizations are in a better position to build a good risk register, that will indicate for each risk identified [2]

- The causes and impacts
- The likelihood of this risk event.
- The existing controls to deal with this risk.
- An assessment of the consequences.

Risk mitigation and control can be achieved through several ways [63], where some of them are listed up next:

- Risk avoidance by simply stopping the different activities which generate risk.
- Reduce as much as possible the probability of the occurrence of the risk events (prevent).
- Diminish the impact the defined risk event can have (detect and correct).
- Transfer the risk to other parties.
- Retain the residual risks by financing and accepting the possible consequences.

Based on these risk events, organizations establish and translate them into internal control activities, which nowadays are necessary conditions of a risk-based regulation and a successful operation of the risk management state [54].

2.1.4. Risk Evaluation

After the assessment and mitigation phases have been performed, risk managers measure and evaluate them periodically against the agreed risk tolerance levels of the organisation itself. If the risk, (and the potential impact), is not acceptable to the organisation, then the risk manager sets out to bring these aspects within that agreed tolerance level.

According to the book Business Risk Management Handbook: A sustainable approach by Spedding, L. S. and A. Rose (2007) [64], a solid risk management evaluation and communication plan enables the organization to:

- Improve safety
- Minimize lawsuits
- Achieve best practice
- Make better business decisions
- Enhance asset management
- Meet regulatory compliance standards; that in turn:
  - Protects reputation
  - Improves the bottom line
  - Leads to a more attractive insurance proposition
2.1.5. Risk Monitoring

Once risks have been identified, analysed and evaluated all techniques to manage the risk fall into monitoring, avoidance, reduction and transfer of it [26]. It is basically the process of keeping track of the identified risks, monitoring possible residuals that can transform into new risks, and evaluating the effectiveness of the executed plans to reducing it. Risk monitoring is an ongoing process in the organization as a way to constant improvement.

Good risk control provides information that assists with making effective decisions in advance of the risk appearing, helping to determine if:

- Risk responses have been implemented as planned.
- Risk responses are as effective as expected.
- A risk trigger has occurred.

Risk management experts advise that it is helpful to keep a register and categorization of the different assessed risks to monitor and control them. And although there are several methods to classify them, the actual method used is less important than the existence and monitoring of systems to control the risks involved and the consistency with which they are appraised [64].

Observation 1: In order for companies to stay and be competitive, they must consider risks and constantly review their processes and models and validate that they are operating without risk. In addition, they must examine new areas of emerging risk and develop systems to control it.

2.2. Organizations and Risk

The term risk in the business environment is mainly used with an undesirable connotation, referencing to unanticipated or negative variations in the organization outcomes, such as revenues, costs, profit, or market share [46]. In order to avoid these negative variations and stay competitive, organizations must constantly review their activities and validate that everything is operating correctly; in addition to a constant study of possible new areas and scenarios of risk [64].

Organizations are not passive entities when it comes to risks, most of the time they take preventive steps in trying to predict and reduce them. With the main goal of containing risk, organizations create risk communication strategies that go above all risk management [43].

As a comprehensive, common and stable set of risk categories used within organizations the risk taxonomy is presented, where it basically encourages the actors involved in risk identification to consider all types of risks the organization could be affected by, and enables them to use key risk management terms – especially Control, Asset, Threat, and Vulnerability – with concrete meanings so it is easier to bridge the language gap that can exist within all the different stakeholders of an organization [25].

The Open Group (2009) [25] presents a Risk Taxonomy that divides risk in two main branches: Loss Event Occurrence (likelihood) and Loss Magnitude (consequences); within the two branches are all the factors that drive both occurrence and magnitude of losses of the possible risk scenarios. Figure 2.2 portrays the taxonomy:

![Risk Taxonomy Diagram](image)

Figure 2.2: Risk taxonomy group, [25]

From a point where risk management meant just buying insurance for the different activities held in the organization, this topic has evolved where several more factors have conspired to make risk management a key...
issue to control [61], to the point by today there are several different type of frameworks and models to manage different types of risk that can appear at an organization. Some of these frameworks will be presented in a coming section.

Knowing risks are contingent (so they depend on decisions), they basically are caused and can be avoided by making decisions.

2.2.1. Risk & Decision Making

To define decision making in a simple way, it can be stated that decisions are communication activities which require a choice between different alternatives to achieve some goal [23]. In order to avoid risk scenarios as much as possible, organizations normally exploit the openness of the future and develop mechanisms for making decisions in uncertain situations: they continuously try to reduce uncertainty and make the future controllable [43].

All decisions made in an organization are done under the “bounded or limited rationality” concept, where it is possible to consider only some alternatives, with the limited information organization hold, and not search for a complete risk free solution when they have found a satisfactory one [62]. In all existing decision making models, the choices made are on the basis of a single criterion: maximum total welfare and minimum risk exposure [67].

Portraying a problem or possible risk scenario as a decision is a way of controlling its boundaries: what counts as part of the risk that can be problematic and what does not, how the scenario will be seen by other parties as also how they will respond to it. Within risk management decision making, organizations get more robust, where they protect themselves from possible damages of the risk scenarios [71]. For businesses, this robustness means that:

1. The decision process must protect individuals within the organization from injuries in all cases, which is also a requirement by ethics and law.
2. The different decisions must protect the organization substantial resources from damage (people, business data, infrastructure, and reputation).
3. The decision process must deliver its intended output.

Decisions with direct impact on the organization also can imply the risk that these decisions entail, even if they are upheld by the decision makers and organizational members, are not accepted or admitted outside the organization boundaries: “Risks are not contained within the boundaries of individual organizations; instead, as powerful players in modern society, organizations have an impact on processes of central societal relevance: organization affects politics, the economy, education, science, and even social work. As a consequence, the decisions of organizations can also entail damages for external parties or groups: shareholders, stakeholders, and customers, even large parts of society, the environment and future generations” [43].

Observation 2: Risk management is an essential element in the management and leadership of organizations and their strategies. Risk has its own taxonomy when being implemented, that needs to be fully understood in order to perform a successful assessment. If risk management is successfully applied within organizations, there will be a shift from "crisis management" to proactive decision-making that avoids problems before they arise.

2.3. Risk Management Frameworks

The evolution of risk management within organizations has evolved since this topic was firstly introduced, where the complexity of both products and the market competition made companies more aware of the environment and the risks they are exposed to. To confront various types of organizations and processes, different institutes and corporations emerged to design frameworks and models to approach and manage risks. Risk management must be an integrated part of the project or process management framework in order to be effective and minimize the impact of the threats. The steps shown in Figure 2.3 represent the general model of the different Risk Management frameworks which must be wrapped in a process that appropriately identifies roles and responsibilities within the organization [26].

For the general plan of these frameworks, it is important to identify the economic and overall environment in which the process is, and how susceptible the organization is to execute the different projects or activities and
the exposure to external risk factors. It is also key that within the business domain, the organization is able to estimate the knowledge, experience and the level of confidence that the different operations can be successfully concluded. These factors define the components of the framework that allows a formal model of the risks to be described [26].

Both Supply Chain and Information Management and the enterprise per se, are some of the areas that have frameworks to assess the risks that can exist within the processes. Some of the most relevant framework will be explained inside this section.

2.3.1. COSO Enterprise Risk Management - Integrated Framework

In the year 2004 the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a principles-based model to implement enterprise-wide risk management. The ERM (Enterprise Risk Management) framework defines essential enterprise risk management components, key principles and concepts, as also expected common ERM language and directions for risk management within the organization: “it is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of the entity's objectives” [13]. Many organizations implement this framework as a way to increase the effectiveness in the risk management activities with the ultimate goal of increasing shareholders value [8].

Enterprise Risk Management is closely related to the concept of integrated risk management at an organization level; integration that promises more efficiency in the use capital, the ability to update business units (according to the amount of capital they place at risk) and coherent insurance strategies for any organization [55]; but to be effective, they must “look beyond technology to establish a culture of risk management throughout the organization” [10].

To set up an effective ERM the organization must first create an appropriate internal environment, that is mainly focused and committed to competences, includes a risk management philosophy and appetite, and expresses governance practices within the risk culture [50]. With that foundation in place the organization is able to set the objectives and goals, identify the possible threatening events, the risk assessment and response, as also for the later control and communication activities [20].

Figure 2.3: General framework of risk management [26]
After the financial crisis in 2008, it has been emphasised that organizations should implement ERM frameworks as a way to regain the lost trust within the marketplace [49] and that ERM must infiltrate all the different practices and behaviour of organizations and its managers in everyday decisions. However, after these recommendations, there were few critical contributions exploring how ERM really works in practice, and even fewer studies addressing how this assessment has evolved and contributes to different risk management styles [55].

ERM presents a new scientific rationality to organizations, marking a potential rupture in the way companies deal, transact and operate with their risk history and sensitivity. However, this transformation inside organizations in reality, becomes more difficult as they encounter pre-existing centres of control and practices, “A shift in the decisional mind-set and context is shown to be dependent on whether risks are represented as ‘real’ problems for managers, instilling urgency in the form of a new moral vocabulary, and by visualizing impacts in a manner close to their actions and responsibilities” [4].

2.3.2. ISO 31000

The ISO 31000 group of standards provide principles, a framework and processes for managing risk within an organization and it provides its guidelines to any area (i.e., finance, engineering, security, among others). Its main goal is to increase the likelihood of achieving objectives, identify opportunities and threats and effectively allocate and use resources for risk treatment [33].

It suggests that companies should continually develop, implement, and control a framework whose main goal is to integrate the different processes that exists for internal control in the organization for managing risks associated with governance, strategy, information management, policies, values, planning and culture throughout the entire organization.

To be effectively implemented in an organization, this needs to fulfil a set of principles and requirements as defined by Purdy, G. (2010) [58]

1. Create and protect value.
2. Be an integral part of all organizational processes.
3. Be part of decision making.
4. Explicitly address uncertainty
5. Be systematic, structured, and timely.
7. Be tailored.
8. Take into account human and cultural factors.
9. Be transparent and inclusive.
10. Be dynamic, iterative, and responsive to change.
11. Facilitate continual improvement of the organization.

With the main idea of having one single vocabulary and common processes for risk assessment and management, ISO introduces new concepts and terminology that is well spread and applied in other frameworks too. Aven, T. (2011) [7] summarizes the concepts:

1. In the definition of risk, it is important to reflect that when considering a scenario, risk expresses that events could happen, and they could have some consequences that have uncertainties (these could be more or less severe, and defined in relation to expected values, objectives or other references).
2. To describe the uncertainty (and hence the risk), the tool to use is probability: where events (and the outcomes) are identified and associated probabilities are determined.

16
3. A probability should be defined, both as knowledge-based (judgmental probability) and as well as chance (frequentist probability).

4. The term likelihood is used in the same way as probability.

5. Other terms should be adjusted in line with the aforementioned understanding of the concepts of risk, probability and chance.

6. A risk source is defined as elements which alone or in combination has the potential to give rise to an outcome.

7. A hazard or threat is a risk source where the consequences relate to harm.

8. The concept of vulnerability can be defined analogously to risk, given the occurrence of a risk source.

Both COSO ERM and ISO 31000 are risk management frameworks that can be executed at organizational level, but there are some differences on their approach for the assessment that need to be considered and compared. As a starting point, the COSO ERM Framework is a more complex and multi-layered framework that is control and compliance based, while ISO 31000 on the other hand provides a more streamlined approach based on a management process, and through tailoring the process it integrates into existing management and strategic initiatives [22]. ISO 31000 has adopted a more pragmatic approach that requires organizations to set or adopt risk criteria as the basis for their decisions.

2.3.3. COBIT

Control Objectives for Information and related Technology (COBIT) is the business framework for the information technology (IT) governance and management of enterprises and businesses created by ISACA (an international professional association focused on IT Governance). COBIT (the latest version) was launched in 2012 and incorporates an update thinking in enterprise governance and management techniques, providing globally accepted norms, principles, analytical tools and models to help increase the value from and trust in information systems [31]. This framework is also the main component for the integrated risk management model that we will analyse in this research, and that is explain in a subsequent section.

The COBIT framework provides an extensive and detailed guidance to ensure the alignment of both business and IT goals by defining a set of processes and procedures; working in different areas of the organization; from strategy to operational development and support, and providing means to evaluate process maturity, and maximize benefits while reducing risk [1].

COBIT aims to link stakeholder needs to business goals to IT goals, including suggested metrics at the higher level based on the business goals that drive IT-related goals, and then are supported by critical processes. As a way to help with it, COBIT provides examples of objectives and metrics at the different levels of the organization: enterprise, process, and management-practice levels [51].

The core of COBIT is its five basic principles:

1. Meeting stakeholder needs.

2. Covering the enterprise end-to-end.

3. Applying a single, integrated framework.

4. Enabling a holistic approach.

5. Separating governance from management.

The topic of risk is key for the whole management and proposed activities in COBIT, as much as it has a complete module dedicated to it: COBIT for Risk, that builds on the COBIT general framework by focusing on risk; it provides a more detailed guideline for IT-related risks. As pointed by Ataya, G. (2013) [6] COBIT for risk presents two perspectives on how to use the framework in a risk context:

- Risk function perspective: Focuses on what is needed in an organization to build and sustain the risk efficient and effective core governance and management tasks.
- **Risk management perspective**: Focuses on the core risk management process of how to identify, analyse, respond to and report on risk.

COBIT defined IT risks as the business risks associated with the use, ownership, operation, involvement and adoption of IT within the organization; they consist of the IT-related events that could potentially impact the enterprise [32]. COBIT categorizes the possible IT Risks in three different groups, as shown in Figure 2.4:

---

**Figure 2.4: IT Risk Categories [32]**

- **IT Benefit/Value Enablement Risk**: Associated with the missed opportunities to use technology as an enabler for new initiatives or improver of efficiency or effectiveness of the organization processes.
- **IT Programme and Project Delivery Risk**: Associated with the contribution of IT to new or improved business solutions.
- **IT Operations and Service Delivery Risk**: Associated with all aspects of the normal ‘day by day’ IT systems and services performance in an organization, which can bring value reduction to the enterprise.

Some examples for each of the IT Risk categories are exposed in Figure 2.4 above.

**Observation 3**: The existing and described standards and frameworks are focused on the internal organization, and frame the direct influence of the system of internal controls, assurance and governance limited to this scope.

---

**2.4. Chains Dependencies**

“One of the most significant paradigm shifts of modern business management is that individual businesses no longer compete as solely autonomous entities, but rather as supply chains. Business management has entered the era of internetwork competition” [40]. Nowadays organizations are no longer battling their competition just with the brand and product itself, but also with the supply chain for the production and distribution of the different materials and products: how effective and efficient are organizations to manage and integrate their network; situation that made the discipline known as supply chain management (SCM) emerge [11] [40].

The Council of Supply Chain Management Professionals (CSCMP) defines SCM as the action that “encompasses the planning and management of all activities involved in sourcing and procurement, conversion, and all logistics management activities. Importantly, it also includes coordination and collaboration with channel partners, which can be suppliers, intermediaries, third party service providers, and customers” [57]; basically indicating that the focus on supply chain management is on the cooperation and trust between all the actors involved in the main organization network (intra- and intercompany), therefore having main emphasis upon
the relationship management in order to achieve a more profitable and be more competitive, thereby increasing customer satisfaction [12]. Situation that has made that SCM is increasing its importance in organization, as by 2010, 51% of the executives stated that the investments in SCM have increased significantly over the last years [48].

As globalization hits in, organizations create new global alliances, and therefore the importance for them to have a clear understanding on how SCM can be successfully applied [27]; especially as they face challenges including mitigation of the risks and disruptions in the new supply chain through the management of the relationships among key stakeholders, the organization functions and all the members of the supply chain [66].

In the new competitive global environment, the performance in most organizations can no longer be determined just by the decisions made inside the firm as the execution of all actors involved in the network contributes to the overall results of the supply chain [48]; situation that made many authors have highlight the need of clear conceptual frameworks for SCM to manage not only their own organization but also the relationship with the organizations in the same supply chain [16] [66]; one of the most known and used framework for SCM is presented below.

2.4.1. Supply Chain Operations Reference (SCOR)
The model known as Supply Chain Operations Reference or SCOR is a reference scheme that helps analyse supply chain processes, providing a distinctive framework that lets the performance metrics, processes, best practices and people to be linked into a unified structure [14]. The SCOR model provides a working framework to several actors of the Supply Chain i.e. suppliers, manufacturers, distributors and retailers. This framework helps in testing, measuring, and evaluating the effectiveness of each operation through the supply chain, and provides the opportunity to compare its performance with similar supply chains [65].

The framework divides the process in five main core business processes: plan, source, make, deliver and return. Each of these processes is implemented through several individual levels that bring different points of detail. The first level defines the scope and content of the model itself, as level two, defines the organizations' operation strategies. Level three defines the inputs, outputs, and flows of each transactional element and business activity, and finally, level four defines the implementation of specific supply chain management practices [48]. The process can be seen in Figure 2.5.

![Figure 2.5: SCOR Framework Levels](Image)

By providing this set of performance metrics, best practices and framework levels, the SCOR model allows organizations to perform fact-based analyses of all the aspects in the current supply chain.

Observation 4: Current awareness of supply chain (and its risk management) has been raised over recent years by a succession of disruptive events affecting the international business environment. As a way for organization to also prepare better to compete, they may find value by recognizing the language in their supply chain and
understand the environment and network in which they compete.

2.5. Risk Organizational Trust

In order to do a correct and valid risk assessment within an organization, the term trust has attracted interest. In today’s working environment, interacting with other actors is a common practice that organizations now rely on, getting involved in interdependent scenarios, where they must depend on the other to accomplish certain goals. A level of trust is a fundamental element of organizational structure and a factor in all market transactions [19].

As noted above, trust requirements are high for organizations for network management and the possible risk scenarios that can emerge. Both across an organization within its network and the various network organizations, building and preserving trust needs to be considered and is as essential as the control systems are considered in the functional form: if all the parties involved in the network do not trust one another and act according to this lack of trust more risk scenarios can emerge and the network will fail [39].

Trust can be defined as the "particular level of the subjective probability with which an agent or organization assesses that another agent or group of agents will perform a particular action, both before he can monitor such action and in a context in which it affects his own action" [21]. And in the same order of ideas, trust is not just taking risk but rather the inclination and predisposition to take a risk in a network.

Mayer, R. C (1995) [45] proposes a model (shown in Figure 2.6) which shows the important factors that help explain the relation between trust and risks and the features concerning organizations to trust each other. The first item are the factors that are consider to affect and explain the trustworthiness on another party: ability, benevolence and integrity; each of these factors encapsulates some important and unique elements of trustworthiness of any party or organization (either as a trustor or trustee). Ability is defined as the set of competencies and skills allowing the actor to have some influence on a specific topic or domain, being a strong ally for the main organization. The second factor Benevolence is defined as the extent to which the third party is assumed to want to act in the proper way to the main organization, aside from the logic profit. As for integrity, it’s explained as the perception of the organization about the partner parties, that they comply with a set of norms and principles that the trustee finds acceptable.

![Figure 2.6: Model of Trust [45]](image)

Risk per se doesn’t affect the trust an organization can put in another party, but the action of trusting is in fact a possible risk for the main actor: “the main difference between trust and trusting behaviours is between a ‘willingness’ to assume risk and actually ‘assuming’ the risk. Trust is the willingness to assume risk; behavioural trust is the assuming of the risk” [45]. Trust increases the likelihood of organizations to take the risk of establishing a relationship with other parties in order to generate some outcomes. If the trust in a third party exceeds the level of perceived risk, it is accurate to say that the trustee or main organization will engage in risk taking over that relationship.
As explained by Delbufalo, E. (2012) [18], organizational trust affects different outcomes within the firm, which can be classified under three different categories:

1. **Direct economic outcomes**: Finding have shown and confirm the strong rationale in the link between trust and financial performance measures like sales growth, cash flow and/or increased Return on Investment (ROI).

2. **Indirect outcomes**: Trust has strong impact on associates’ actions as for example investment in ‘relation-specific’ assets, supplier integration and joint problem-solving.

3. **Relational outcomes**: Positive impact on partner orientation, behaviour, loyalty, expectation of continuity, willingness to invest and satisfaction.

**Observation 5**: Working in a network or chain of organizations involves interdependence, and therefore people and companies depend on others to accomplish the internal goals. Organizational trust shows how both a robust and strong relationship can be built between organizations under a network, being defined by a number of different variables and conditions.

### 2.6. Risk Assurance

Assurance can be described as the activities conducted to certify or validate the business transactions between organizations and its trading partners and consumers, such as internal controls and risk management. Normally these activities are conducted by trusted, independent organizations (private or not for profit) that assure performance of services is as promised, and that all regulatory and/or operating procedures are complied with by each trading partner [37]. The primary drivers behind the emergence of these services, is the increasing role that accountability is playing in organizations, where they want those who affect their activities and processes to be accountable for the responsibilities they have assumed.

Given that today inter-organizational relationships are predominantly characterized by the impersonal nature of them (mainly in online environments and the extensive use of IT solutions) instead of face to face interactions, organizational trust, as explained in section 2.5, needs an extra ingredient by having ways to certify and assure the business partners. Structural assurance is an example of how companies now often negotiate the terms governing their business relationships, involving assurance partners that regulate and guarantee those relations, as they create and manage ‘contracts’ the bilateral affecting factors that affect the relation are customized to the mutual needs of the two partners in a business relationship, playing a more important role than the two trading partners themselves in establishing trust in the relationships [52].

In the specific matter of information assurance (IA), this one is not effectively addressed in most developed organizational or business frameworks, which leads to not be well integrated to the organization processes, indicating also potential for new vulnerabilities [28]. In terms of facilitating conditions, initial assessment of this information and its competence is much more difficult for bilateral institutional trust than having for a dedicated third-party that usually has in-house IT expertise to do such an assessment. And to do so, trusted third parties provide effective means to build inter-organizational trust at early relationship phases [53].

**Observation 6**: As mentioned in observation five organizational trust is an important subject when interacting in a network. But this trust is not easily obtained and sometimes is required to involve a third party that can offer the required assurance (though contracts or legal documents) so the required trust can start building up, offering the complete and essential assurance over the information exchanged by all the organizations in the network.

### 2.7. Supply Chain Information Integration

Supply chain integration must comprise the two main flows: both information and material, and cannot be one without the other. Increased communication and greater coordination of the organization's logistics activities with the different actors in the network are characteristics of higher levels of integration within the chain [56].

21
Information technologies (IT) have impacted and changed the way business is done around the world. With the capability to provide accurate and reliable information, companies rely on IT to improve their performance [41]. In the same grain, IT also has impact on the improvement of supply chain management and the way information is shared among involved actors, when the supply chain integration is the main goal.

With implementation of SCM, all the actors involved in it have to act as partners and their relationship must become a cooperative one where they act as an enterprise to succeed in the process [74]. As a way to achieve this cooperative environment, all related functions across the supply chain must operate in an integrated manner, causing that information systems continue to have a bigger role in SCM as an efficient and helpful integration mean [41].

Quality over the supply chain operations are not possible without appropriate information sharing between the actors and architecture to stand on, as supply chain management emphasizes on executing activities under a quality management, appropriate information sharing and architecture has become an important and relevant competitive factor [74]. “Information integration refers to the sharing of key information along the supply chain network which is enabled by information technology. One of the main purposes of information integration is to achieve real-time transmission and processing of information required for supply chain decision making” [56].

But the integration of information has also its risks: as organizations share their information with their network partners they are allowing this knowledge to become public and risk part of the competitive advantage or edge they have. Situation that makes important a clear definition of the level of integration into the organizations’ processes and depth of collaboration, as the extent to which critical and information is communicated to the supply chain partners [44].

Information technology is identified as one of the critical areas of opportunity in improving supply chain quality management and information integration, as it is crucial to improve the chain quality and control [74]. As a way to test this premise, Li, G., et al. (2009) [41] proposes a conceptual model of the relationship between IT implementation, supply chain integration (SCI) and supply chain performance (SCP). As shown in Figure 2.7, the implementation of IT impacts the performance of the supply chain not only directly, but also indirectly through the impact on its integration. In this research, ‘Supply Chain Performance’ is measured via several dimensions like cost, quality and flexibility; while ‘IT Implementation’ refers specifically to the required capabilities to integrate information among the parties involved in the chain, measuring not only the adoption and implementation levels of IT, but also the degree on how embedded it is across the chain. As for ‘Supply Chain Integration’, it refers to the ability of an organization to integrate and perform exchange-related activities with partners within the supply network [41].

As result of the research, and with the growing awareness in organizations about the benefits of implementing IT, it was recognized its profound impact on supply chain, where its power to provide accurate, reliable and timely information creates an expectation over the improvements on the supply chain performance and integration. But its shown that "IT implementation has no direct effect on Supply Chain Performance, but rather, that it contributes to the improvement of SCP through its positive impact on SCI" [41]; which shows the importance of promoting supply chain integration with IT as an enabler.

As supply chains become overly complex, they need constant improvement: data deficiencies, information gaps and an outdated paper trail are some of the activities holding back complete SCI resulting in financial, safety, visibility and planning risks. This situation increases even more with international supply chains, where trust within the parties is more complex and difficult to handle [29].

Figure 2.7: Supply Chain Conceptual Model [41]
One first point of improvement for supply chain and information integration is that the organizations must be supported by the information flow from downstream to upstream (consignor to retailer/consignee) [56]; where the consignor as the first party involved in the chain is one of the first actors who has all the information available about the goods and the people involved, ensuring that for example that the logistic information matches the commercial information [29].

To improve such integration and provide timely information, the need for IT related solutions has become clearer, where solutions like providing electronically all the data and information that is related to the goods and parties involved in the chain, can improve the security and visibility of the trade lane, where the timely provision of information acquired at the source (depends on the required data) in the supply chain can be realized via a data pipeline, entailing all the different data sources and IT systems in the network [38].

The concept of data pipeline can be defined as the IT platform for information sharing within a supply chain, enabling access to and linking of the actors’ information systems used in the process, providing one integrated point of access to all the required data that already exists split in the chain [38]. As shown in Figure 2.8, with the IT data pipeline concept, each of the parties involved in the international supply chain will set the data in the pipeline at the moment it is available, and the access to it (from all the other organizations involved in the chain) is controlled in a way that only authorized actors can see it [38].

The data pipeline is a concept that helps improving supply chain visibility (accessing the data that is necessary for a specific actor in the network to assess what is actually happening in the supply chain), which at the same time helps improving the supply chain and information integration, creating a better environment for real-time data exchange, responsiveness, collaboration, synchronization, and real-time visibility across the entire supply chain [74].

But having this type of platform to improve the information and supply chain integration entails also the need to improve the controls and manage the integration risks; normally, with the monitoring of isolated events, some information is probably missed and risks in the chain are higher. Supply chain visibility will improve supply chain risk analysis and the data pipeline mechanism will decrease the administrative burden since it is based on already available supply chain data [30].
2.7.1. Document Sharing
Besides containing key information about the transported goods, the documents exchanged also can give sufficient evidence to one party that the other actors have fulfilled their task (i.e. with a document like the Airway Bill, the buyer organization can have sufficient evidence that the seller has indeed shipped the goods via air). In supply chain processes it can be seen that the sharing of information becomes essential, therefore the documents containing the data also play a crucial role [70].

In these type of processes, it is important to model the obligations between all the different actors (i.e. buyer, seller, freight forwarder, authorities, etc.), where the obligations are the relations (or information exchanged) between two of these parties. Such interactions between the actors can be divided in two different ways: direct obligations and indirect actions [70]. The direct obligations can be defined as the relations between two parties when they interact with each other without third parties involved, and the exchange of both goods and documents is direct. The indirect actions are stated when one party has the obligation to do something, but he is delegating the execution of this action to another actor, therefore the exchange of information is not a direct relation but between two organisations, as it involves more parties.

As transfer of obligations and rights are crucial in international trade procedures, it is important to be able to formally reason about such transfer of documents and information as a way to analyse the success of the chain information integration.

**Observation 7:** Competitive pressures have forced companies to increase supply chain collaboration throughout the whole supply chain, having also to share and cooperate with information. Supply Chain Management has become now more dependent on the information flows, as it can be characterized as the enabler of collaboration and improvement. The visibility of information allows companies to have broad and plain visibility over the logistical flows and can leverage this information about the processes and supply chain management, and for that, solutions like the data pipeline are introduced.

2.8. Towards Integrated Risk Management (CANTOR)
The propagation of services and dependencies within the supply chain as a way to integrate the information and improve the visibility, allows them to have major benefits for the organization (as for example bring more complex services), but it also leads to new vulnerabilities and negative outcomes if the organization is unable to control the associated risks [5]. In order to mitigate the new threats, specific control measures are required for assurance not only in the organization, but in the whole supply chain, where the traditional methods of risk analysis and determining controls within both the information systems and supply chain services are no longer sufficient, as they are not entirely clear and detailed about the interactions and working of an inter-organizational or network service [72].

When chains and networks are used efficiently, mutual trust and alignment of their goals are essential for the design of the whole enterprise [47]; and to accomplish it, collaboration levels between the organization and its partners in the supply chain grows, being an important factor that they develop a more committed and standardized relationship, which, at the same time, can justify the different investments necessary to enhance the collaborative relation and lower the risk levels that can emerge; and this is where it hasn't been enough studies and research [5]. As mention in a previous section, risk management is becoming a key strategic focus within organizations, but not much is still known on how they assess risk in supply chain relationships and the processes used to minimize it.

To cope with the situation, Wijk, Y. W. v., et al. (2014) [72] proposes the CANTOR approach (Chain Assurance Network based on Transference of Obligations Risk control), based on internal control in the chain that is extended through the organizations in the network, where the chain control is defined as the activity designed to provide assurance in the achievement of the goals in both efficiency and effectiveness of the united chain and compliance with required regulations, approaching the complete chain and all the actors involved as a "virtual organization".

Internal control and information assurance are the bases in auditing and in order to structure them, several risk management frameworks (like the once explained above) were developed, trying to ensure that the quality
of information complies with the organization’s goals. But when the risks lie outside the limits of influence of the internal control systems, it is where the traditional frameworks can no longer be fully applied and a model that considers all the connections in the network needs to be applied.

To perform the chain assessment, the CANTOR approach can be applied within two different perspectives: the chain Service Content Network (SCN) and the chain Service Delivery Network (SDN), as shown in Figure 2.9. The first network, the SCN, refers to the business value chain content and the actual services or goods that are communicated and transferred between the actors in the chain and validating that the provided information is the correct information and the content is according to what is expected. It is basically the flow of information throughout the IT in the chain, it usually goes through a series of operations and transformation before it reaches the end of the process [69]. While the service delivery network refers to the manner of delivery within chain infrastructure. It is the IT used to transfer the services or goods mentions in the SCN, stating the ‘how’ information is transmitted and transferred from one actor to another in a way that meets the required standards. It focuses on the manner of distribution within this channel in terms of security and reliability [69].

The CANTOR approach designed by Wijk, Y. W. v., et al. (2014) [72] works under four key drivers for the assurance framework on the supply chain:

**Atomic approach of a service chain:**
To attack the increased vulnerability and complexity on the integrated supply chain, the risk approach should validate the chain in its smallest possible way: ‘the chain atom’, which is defined as the smallest chain or network, consisting of two intra-organization relations that involves three participants. If the risks and controls are assured at this minimum level (in each of the chain atoms of a network), it can be assumed that the whole chain is assured as well.

As shown in Figure 2.10, each of the actors involved, request a service or product and has a result delivered back: actor A as the initiator of the atom chain requests a service from organization B, whom at the same time has a service dependency over actor C. Both B and C add some value to the requests made by A and B respectively, and based on these relationships and the norms that they must comply to, the assurance framework can assess.
the risk and controls within the chain complete link.

**Transference of Obligations of Risk and Control (TORC):**
The collaborative nature in the chain implies a network approach, which at the same time implies that the traditional Service Level Agreements (SLAs) between each of the actors need to be aligned. The TORC is required in the chain to align and balance the different actors in the network and frame the chain as a whole. The individual SLAs between all the actors is not enough due to the complexity of the network and relations in the chain, entailing that all the risk control measures need to be expressed as norms that are transferred through the whole chain.

The individual risk-control values of each actor are expressed as a norm that is transferred throughout the chain. An as shown in Figure 2.11, these are the TORC norms that originate from the control measures from actor A, and the TORC describes how in each stage the responsibility for taking mitigation measures to control the risks are distributed to, and aligned with, other chain links in the network.

![Figure 2.11: TORC (72)](image)

**Chain Internal Control System (CICS):**
Internal control based on the concept of “virtual” organization of the whole chain, where instead of been intra-organizational and individual, it needs to built on all the organizations within the network (as shown in Figure 2.12). The CICS norms and tolerances are transferred in the network to coordinate and aim towards control of the complete chain, where each of the TORC points (as previously defined) will be the base and audit evidence for the defined chain internal control system.

![Figure 2.12: CICS (72)](image)

There are three mayor phases:

1. **Audit Strategy:** Auditing the chain differs form the established organization audit, in this case is based on chain policy.
2. **Operation of the Audit and Monitoring:** Carried out in the chain by the actors involved, by cooperating, sharing responsibilities and formal communication measures within the actors to state the norms in the chain. The CICS is based on the individual chain control measures transferred by the TORC.
3. **Attest to Audit Opinion:** The feedback as a result of the previous step, where the audit and monitoring of the chain is perform.
Chain Governance:
To define the chain governance is required the cooperation of the three previously described major components of the framework, which originates from the three design drivers mentioned above: Strategic Chain Policies, Chain Risk Management and Chain Audit and Monitoring.

The strategic chain policy needs to define how the transference methods of chain risk-controls will be used, describing the essential risk management and audit maturity levels. The chain risk management refers to the alignment of the strategic chain policy and risk management as the chain audit and monitoring defines and verifies the norms and tolerances for monitoring and directing the chain.

Observation 8: Assurance is an essential condition for trust in a collaborative supply chain, and current models and frameworks don't offer a clear solution to avoid and work over the complex business risks that can show up. The CANTOR approach is a conceptual solution for assurance and governance in supply chains, by designing a framework based on business strategy, the management of risk-control obligations and the audit of the chain.

2.9. Summary and Gap Analysis
As noted in the observations at the end of each section, there are some shortcomings found from the literature review. As pointed out in both observations four to seven, in integrated chains, companies deepen their relationship with partners and thus become more dependent on each other, and although there are many benefits and opportunities in integrated supply chains, there are also several risks that need to be addressed as well, and there is a gap on the way to treat them. Non-disclosure of information, inappropriate disclosure, lack of information quality, lack of use of security, are some of the risks associated with chain integration that may impact upon the organisation.

Within these risks that emerge in integrated chains one concept becomes important to outline: trust, that in cooperative supply chains it becomes important mainly due to the fact that it supports the level of formal norms and regulations that will backup the process and connections within organizations: if one party fails as a trusted actor, formal control mechanisms need to be implemented, therefore also affecting the risk levels on the chain (observation five).

To cope with the risks, different models, standards and frameworks have been established: ISO/IEC, Cobit5 or COSO ERM, among other. As an example, Cobit5 for Risk increases the enterprise risk-related capabilities and helps understanding how effective IT risk management optimises the business processes and value, improving the quality and reduced waste and costs.

But as noted in observation three, each of these mentioned models and frameworks are mostly focused in a single enterprise and the management of the risks over its processes, which can be hardly implementable to build the risk framework for an integrated chain. In this collaborative environments or scenarios it is common to have several companies with their own objectives and goals, and therefore stating different risks that need to be handled and controlled, and where some of them are mutually dependent within the network of organizations; factors that are not considered in the above standards.

This part of the research has provided an overview of the current risk management models to assess both Supply Chain and Information integration and their limitations. CANTOR is the suggested approach to analyse the processes and risks in an integrated supply chain and validate the dependencies inside the network explained in section 2.6 is a way to cope with these limitations and provide a solution to properly execute a risk management model for integrated supply chains. The following part of this thesis addresses the proposed model, and evaluates if it is a proper approach or solution to assess risk over the information integration in a supply chain.
In this chapter, there will be a detailed explanation of the current status of the document exchange process in the Kenya Air Trade Lane. First, each of the stakeholders in the process is presented, as their role, importance and main activities. Additionally, all the major highlight points and important remarks within the process. This chapter gives an overview of what the process is and where the risk assessment will be executed. The models and overview of the process were designed specifically for this research, based on the analysis after performing different interviews and email exchanged with different actors inside the trade lane as well as the company’s supervisor.

During the project, for the first 3 to 4 months, and for at least twice a week, there were both virtual and physical meetings with the Freight Forwarder, Customs and Dock Services, and mainly with Roel Huiden, that besides being the supervisor, in his role of Supply Chain consultant at FloraHolland, has complete knowledge of the process.

3.1. Stakeholders Analysis
The FloraHolland air trade lane from Kenya to the Netherlands runs from farms in various regions in Kenya, via the Nairobi airport and Amsterdam Schiphol airport in the Netherlands, to FloraHolland in Aalsmeer, and transports flowers for commercial partners in the FloraHolland cooperation. From here the flowers are delivered to the end customer, or prepared for auctioning (delivery via an import agent).

The Trade Lane has several stakeholders that are key and essential for the success of this process. All of them influence the behaviour of the chain. This section recaps all the stakeholders.

Growers
The growers are key actors, as they trigger the process. In the Kenya trade lane, besides growing fresh cut flowers (roses), they are all members (owners) of FloraHolland, and trade their products mainly through this company. As the initiators of the process, they are the primary source of the product and important information, documents and certificates on the Trade Lane.

As a supplier, the grower has a direct relation with both final customers and with FloraHolland, who, if required, assists the grower with necessary paperwork and logistic services. The fact that they are part of FloraHolland, doesn’t mean that growers are obliged to process their products through Flora Holland and their services.

**Chain Objective:** Grow, prepare and deliver high quality flowers on time to their final customer.

Overseas Road Transport
The overseas road transport operator is hired by the grower to pick up the goods at the grower’s facilities and transports them to the warehouse where the products will be held before bringing it to the export Carrier. Some Freight Forwarders offer road transport. Also some large growers have own means of transportation.
**Chain Objective:** Deliver the goods from its origin to the required destination in time and preserve low temperatures of the goods.

**Overseas Logistic Service Provider**
In case of consolidation shipments of goods from different growers, the overseas LSP is responsible to perform this task and elaborate the required paperwork about the consolidated shipment. This agent works in collaboration with the overseas freight forwarding company and shares the facilities at the airport. It also acts as the cargo broker, providing the carrier (in this case airline) with the information of the shipment.

Once the shipment is (administratively) consolidated and ready for export, the overseas freight forwarder hands the goods to the carrier.

**Chain Objective:** Offer high service airfreight, with optional consolidation services to reduce the transport costs for smaller shipments.

**Overseas Freight Forwarder**
The overseas freight forwarder receives the products and is responsible for physically preparing them for the shipment to the Netherlands. The freight forwarder delivers goods on a ULD to the cargo handler on the airport.

The freight forwarder is responsible for some of the documentation with respect to the export of the goods (and the different contracts with the carriers). For this, they rely on information that is provided by the growers.

All boxes are scanned and weighed at their facilities while also the temperatures are measured. While the products are held in their facilities the phytosanitary inspection takes place; and when approved, the certificate is provided. From here the goods are handed to the cargo handler for preparing the ULD’s.

**Chain Objective:** Building the airfreight plates (ULD) and deliver to the carrier (via cargo handler), including the required airfreight documentation.

**Overseas Horticultural Authority**
The Agriculture, Fisheries and Food Authority (AFFA), formerly known as Horticultural Crops Development Authority, is the state corporation in charge of regulate the production, processing, marketing, grading, storage, collection, transportation and warehousing of the different agricultural products.

The agency is responsibly of certifying the goods that will be exported by stamping and approving the invoice and export certificate.

**Chain Objective:** Regulate, develop and promote the flower production and agricultural goods exported from the Origin country.

**Overseas Phytosanitary Inspection Agency (Plant Health Inspectorate Service)**
Kenya Plant Health Inspectorate Service (KEPHIS) is the government parastatal whose responsibility is to assure the quality of agricultural inputs and produce to prevent adverse impact on the economy, the environment and human health. In this trade lane KEPHIS is responsible of assuring that goods containing organisms are not exported to countries where these organisms are considered harmful (no pests or plant diseases), and that the goods meet specific phytosanitary requirements.

The agency organizes inspections to check all cut flowers before export, and, if approved, provides a phytosanitary certificate validating the goods information.

**Chain Objective:** Assure the quality of the products being exported by providing an approve certificate over the goods.
**Overseas Customs Authority**

The Kenya Revenue Authority (KRA) is, as Customs Authority, the actor responsible of doing the assessment, collection, administration and enforcement of laws relating to the revenue of exporting goods according to the country's regulations. Their main duty is the taxation over the exportation of the goods.

The agency provides the export declaration form (Single Administrative Document), after the phytosanitary inspection is approved, which are required for exporting goods (plus providing of the certificate of origin (for export to Europe) the EUR1 form when applicable).

**Chain Objective:** Ensure the security and facilitation of the international trade of goods from the origin country.

**Overseas Cargo Handler**

This actor offers ground handling services at the airport, who is responsible for the safety loading of the shipment and other cargo to the carrier. The cargo handler is responsible of bringing the goods from the freight forwarder to the airplane that will ship it to the destination country.

**Chain Objective:** Stag, secure and load cargo on airplanes by calculating the aircraft's centre of gravity and assess the quantity of cargo.

**Carrier**

For the Air Trade Lane, the carrier is the airline in charge of transporting the goods from the origin country to the destination country. Airline is responsible for the entry summary declaration for the entry of the products in the destination country.

At arrival, the airplane is unloaded and goods are picked up by the cargo handler and passed to the Freight Forwarder. Goods may be scanned by customs for the first time at this stage.

**Chain Objective:** Provide safe and secure air transport services for traveling freight and goods.

**Cargo Handler**

This actor offers ground handling services at the airport, who is responsible for the safety loading of the shipment and other cargo to the carrier. The cargo handler is responsible of bringing the goods from the freight forwarder to the airplane that will ship it to the destination country.

If inspections are required in the airport facilities while the cargo handler company is unloading the goods, they are (by law) liable for delivering support during the check and inspection.

**Chain Objective:** Secure and unload cargo from airplanes and bring them to a safe location to keep the process.
**Customs Authority**
Customs is the agent that checks the safety of goods traffic crossing the borders. The task of Customs is to ensure that goods that constitute a safety risk enter the country.

Based on a risk analysis, Customs selects which products would be selected for inspection. They can remove goods from its logistic chain to inspect them. Once the required documentation is presented and approved Customs releases the goods into free circulation.

**Chain Objective:** Promotes the safety of goods traffic crossing the country's external borders, ensuring that the goods don't constitute any risk by entering the Netherlands.

**Food and Consumer Product Safety Authority**
The NVWA (Dutch translation for Netherlands Food and Consumer Product Safety Authority) is an independent agency linked to the Ministry of Economic Affairs and the Ministry of Health, Welfare and Sport. The institution is in charge to protect human and animal health, monitoring animal welfare, food and consumer product safety and enforces the country's nature legislation.

The main tasks of the NVWA are: supervision, risk assessment and risk communication.

**Chain Objective:** Validate the information of the imported goods by verifying the documentation from the origin country.

**Freight Forwarder (FF)**
The local freight forwarder is responsible for releasing the goods and transport them to the premises of FloraHolland. The FF is responsible for the clearing process with respect to the import of the goods (and contracts with the local road transport providers), relying in the information provided by the growers and the overseas freight forwarder.

**Chain Objective:** Handle the details of importing the goods and assist the main organizations on managing the flow of products in the supply chain, by dealing with the different certificates and declarations required to release the goods.

**Road Transport**
Road transport operators are hired by the freight forwarder if own means of transportation are not available.

Customer (buyer or import handling agent) pick up goods. Boxes are unpacked and flowers are put on water and prepared for transport to end customers (retailers, wholesalers, etc.) or prepared for auctioning.

**Chain Objective:** Effectively and efficiently deliver the goods from its origin to the required destination.

**FloraHolland Dock Services**
It is the arrival point of the goods at FloraHolland's facilities. Is the point where most of the times the ULDs are unloaded and sorted by order of its customer (buyer or import handler). Dock Services is a licensed inspection facility for phytosanitary inspections. Product's inspections (phytosanitary and/or import) can take place at the warehouse facilities, depending on the specifications by the Freight Forwarder and final customer.

**Chain Objective:** Offer on loading and sorting services for imported products to it's customers.

**Import Agent**
The import agencies play the role of final customer when other companies require the services from someone who can assist them in acquiring the goods from countries abroad. In this case they are in charge of organizing and manage the import of the products for FloraHolland, so they can be later auctioned.

**Chain Objective:** Assists a business in buying and delivering the goods from a foreign country, to later be auctioned.
FloraHolland
FloraHolland is a cooperative organization of growers of horticultural products and provides a world-covering, dynamic marketplace, both physical and online, where trade, knowledge and innovation in floriculture come together. The company focuses on achieving maximum returns for the growers’ member by contributing to high sales revenues at low sales costs.

The services provided by FloraHolland is to improve the growers’ sales revenue by expanding the service network and bring together both supply and demand chains as also adding value in the sales, market and distribution of flowers and plants, reinforcing the position of the Netherlands as an international horticultural cluster and ensuring an efficient and capable organization.

In this trade lane, all Kenyan suppliers are member of the cooperative. Dock Services is a service provided by FloraHolland.

Final Customer
The customer is usually an importer of flowers, or a large retail organization. The customer is responsible for sales and distribution of the goods to the final consumer.

Chain Objective: Acquire high quality products in the required and expected time.

3.2. Process Description
Bringing the goods from Kenya to the final customer in the Netherlands via the air trade lane doesn’t involve just the transfer of products between the actors, but also lots of documents and information that is required for the success of the process. Certificates, invoices and other documents are exchanged between the actors, to validate data about the goods.

The air trade lane process is big and complex enough so for a better understanding of it, the total map was divided in six sub-processes, three in Kenya and three in Netherlands. Below is the detailed list of the six processes followed by the description of each of them. They describe the informational flow of documents, the organizers, operators and involvement of governmental agencies.

3.2.1. Process 1: Document Preparation
It all starts with the grower (seller) after the harvest of the flowers starts the packing process. At this point, triggered by a purchase order from the final customer or just to be auctioned by FloraHolland, the grower consolidates the order of what will be ship to the customer(s), and via FreshTrack (FloraHolland’s supportive software system to facilitate logistics flows in the airfreight), Excel, email or other internal systems, notifies the Import Agency (in case of auctioning products) or the final customer with the detail of the order.

Afterwards, the grower prepares the invoice and the packing list either in Excel, Freshtrack or the internal system (i.e. SAP), prints them and finish organizing the rest of documents required for the export of the goods: certificate of origin (when applies), security declaration and the delivery note needed to transport the goods from the farm to the freight Forwarder facilities.

At the time the packing into boxes is conducted, sellers fill the request for the mandatory phytosanitary inspection via the Kenya Plant Health Inspectorate Service (KEPHIS) electronic certificate system (ECS), entering the required information so the phytosanitary authority schedules the inspection. Normally these inspections take place at the freight forwarder warehouses close to the airport later on the process.

Once all documentation is complete, both the Delivery Note and the Security Declaration are passed to the road transport agent (along with the goods) to be send to the freight forwarder warehouse. The rest of the paperwork is send directly to the document office via mail or their own system. This activity can also be outsourced to either the freight forwarder or logistic service provider in Kenya.

The Road transport provider signs the delivery note and once it gives the goods to the Freight Forwarder ware-
house, it also delivers the security declaration. At this point the goods are separated from the documentation, as the grower’s office receives the documents from its own farm while the products were delivered by the road transport and are held in the freight forwarder warehouse.

3.2.2. Process 2: Shipment Approval
Many of the growers have an office close to the airport facilities that receives and handles the documentation at first. This office is in charge to validate that all information is correct (Invoice number, country of destination, etc.) while supervising the inspections. If no application for the Phyto-Inspection has been filled at the farm, the person in charge of the document office will fill the ECS form. After receiving and validating the documentation, they prepare the products that are in the freight forwarder warehouse for inspection.

KEPHIS will perform the inspection in the scheduled date at the freight forwarder facilities, where the inspection is guided by the grower’s document officer. If KEPHIS doesn’t give an approval, the document officer needs to contact the farm to fix the problematic information. If the inspector approves both the information and goods, the invoice proforma is both signed and stamped, as also the phyto certificate is generated online, to be picked later in the process. This inspection sometimes takes too long because the person in charge checks one invoice at the time for all the different shipments, in FIFO order.

With the KEPHIS approval, the document officer picks up the phytosanitary certificate generated, as then proceeds to go to the Horticultural Authority (now known as AFFA: Agriculture, Fisheries and Food Authority) and arranges the export certificate required to export the goods (as also the certificate of origin if applies). Once the AFFA generates and stamps the document, all the paperwork is passed to the Logistic Service Provider (LSP) who in case of consolidation of a shipment, will create the required documentation for the consolidated order: consolidated invoice and phyto certificate; and proceed with the required stamps by both the KEPHIS and the Customs authority.

With goods still in the freight forwarder warehouse (with temperature checks), the paperwork is now also handed to them so they can finish the shipment approval process. After validating the documents, the freight forwarder requests the C17 form (export declaration) to the customs authority (KRA: Kenya Revenue Authority) by login into their system: Simba.

Once the KRA authorization is completed, the freight forwarder processed to create and complete the House Airway Bill (HAWB).

3.2.3. Process 3: Carrier Arrangement
With the main documents approved, stamped and completed, the freight forwarder carries on to inform on shipment details to the airline, providing details on the products like quantities, weights and volumes, so the carrier can inform the freight forwarder via email with the flight updates as also the ULD information (positions, sizes, etc.).

The freight forwarder scans all the documents and certificates into their internal system (i.e. CargoWise), so the counterpart in Netherlands can start with the process of the required authorizations in the Netherlands. After all documentation is properly scanned, they are passed with the goods to the cargo handler so they can load on the airplane. While this is being processed and after the Freight Forwarder receives the C17 form from Customs, a copy of it is sent to the seller, so they can apply for a tax refund.

When the carrier receives all the paperwork and before the airplane is fully loaded, the airline needs to fill the Master Airway Bill (MAWB) with the required details about the transported goods.

3.2.4. Process 4: Entry Process
While the goods are being transported in the airplane, Customs requires the carrier to fill the Entry Summary Declaration (ENS) with at least four hours in advance of arrival (for flights that take more than 4 hours, as the case of Kenya). Therefore, the first task required by the carrier is to fill the information for the ENS via the Aangiftesysteem (or AGS system), to which customs answers with a Movement Reference Number (MRN)
compulsory to allow the goods to enter the country.

After the aforementioned ENS, the carrier requires also to fill and process a Summary Declaration for Temporary Storage (SAL) required for the goods that will be unloaded in the Netherlands, as is this case. The SAL is also filled up online in the AGS system. After both declarations have been filled and approved, the airplane is unloaded by the cargo handler, who also receives all the documentation straight from the carrier.

If Customs specify through the SAL declaration that either a physical or just documents inspection is required, the company where the inspection will happen, is (by law) accountable for delivering support during the check. In most of the cases, goods are still in the cargo handlers control, therefore they are in charge of looking after the inspection before sending the documentation and goods to the Freight Forwarder.

3.2.5. Process 5: Import Process

Process starts when the Dutch Freight Forwarder applies for the phytosanitary approval from the local authority (NVWA: Nederlandse Voedsel-en Warenautoriteit), while the entry process is still ongoing. This application is held online through the authority's portal called CLIENT Import, where the Freight Forwarder provides the preferred time and location. The inspections can also be performed by the KCB (Quality Control Bureau in Dutch), which is an independent governing organization supervised by the Ministry of Economic Affairs that performs public duties, like the phytosanitary inspections.

After the NVWA processes the application they will notify via email the Freight Forwarder about it; answer can be either three things: No inspection required, only document inspection required and physical inspection required. Normally at this point, the Freight Forwarder also receives the physical original documents from the cargo handler, with which they send a notification (word or email) to Dock Services including the details of the products that will be sent the same day. Dock Services also receives notification from both the Import Agents and Final Customers about their shipments and the goods they are about to receive by the internal form or document “Customer Packing List”.

Going back to the NVWA notification, in case of no inspection required, the authority will send a new email notification to the Freight Forwarder with the P2 codes for the shipment so they can start the process of the Import Declaration. If the shipment is required for inspection the NVWA will send a second email with the details about the inspection and the date (closely to the suggested one before).

When physical inspection is required, this can only happen in facilities that are certified by the NVWA, like Dock Services, where most of the time the inspections are held (is also possible to perform the inspection at final customer warehouses or partners of the FF if they are certified for it). To be able to transport the goods while they are still under customs control, it is necessary to request a transit declaration (T1) with this authority. Once the T1 is processed, the FF notifies Dock Services about the inspection (via email), to prepare both the documents and products. The shipment is sent through a road transport provider who will process the CMR document required for the transference of the products. Once the products are in Dock Services they will be prepared for the scheduled inspection by the NVWA, whom after proper validation will approve the goods and notify the Dock Services with the P2 code, that will later be forwarder to the Freight Forwarder to start the process of the Import Declaration.

In case the NVWA requests a document inspection, the Freight Forwarder send the required information via mail (the original certificate its required to be send within 48 hours) to the NVWA (or KCB), and in the meanwhile continues to process the Import Declaration without waiting confirmation of approval from the NVWA.

The Freight Forwarder processes the import declaration and awaits the response which, similar to the NVWA notification, can be either that no extra inspection is required, only document inspection is required or a physical inspection is required. When no extra inspection is in place, the FF immediately releases the goods, and if they are already at Dock Services, they notify them via email that goods are free to be released, in case they are not in the Dock Services facilities, the FF will arrange the transfer with the road transport provider to deliver the goods.
If customs require an inspection, the freight forwarder will notify the actors who is in charge of the goods at the moment (as they can be in the airport with the cargo handler if no NVWA inspection was previously required, or already in Dock Services) about the inspection so the shipment can be prepared. Once customs approve the release, as in the previous case, if goods already in Dock Services facilities, the Freight Forwarder will notify them via email that products are free to be released, in case they are not in the Dock Services facilities, the FF will arrange the transfer with the road transport provider to deliver the goods, and keeps the documentation for their registry.

3.2.6. Process 6: Customer Delivery
After the Freight Forwarder releases the goods and notifies Dock Services, the shipment is ready to be carried to the customer. If goods aren't for auction, they are delivered directly to the final customer, while if the products will be auctioned, they are sent to the Import Agent, who will fill the EAB form (Elektronische Aanvoerbrieven / Electronic Delivery Form) required to notify FloraHolland that the goods are meant for the auction. A copy of the EAB is delivered both digitally and physically.

With this information, FloraHolland receives the goods and organize them to be auctioned in the upcoming morning.

3.3. Document Flows
As seen in the Kenya Air Trade Lane described in the previous section (Chapter 3.2) much of the documents and information generated is transferred across the different actors in the chain. Therefore, it is important to explain the flow and how they are hand on between the different actors.

The content of the documents is mainly about the goods but is formatted in a specific form according to the document or certification. Besides these documents additional documents are used between pair of actors in the supply chain. For instance, between the Dutch freight forwarder and FloraHolland Dock Services, several emails and notifications are exchanged. Generally, information sharing is only between two parties, and not directly shared with any of the other actors.

The communication or transfer of document between parties can also have different purposes: stamping (S), fill out (FO), transport (TR), validation (V) or by request (R); as its stated in the third column of the table in the figures below. Stamping is when the document needs to be send to an authority to have the legal approval and inscription so the goods can continue the process. Fill out refers to when the forms are send empty or are required to fill some information, as they are incomplete. Transport indicates that the document is simply moved from one party to another because of the logic of the trade lane, where documents need to pass through one party to reach the next one. The validation type of communication is stated when the document needs to be forward to the next party because an approval or legalization is required by that actor. And request refers to the requisition mandatory to obtain the mentioned document.

Not all documents are transported through the whole chain (from beginning to end). While some of documents and certificates are used only in Kenya or in the Netherlands, there are also some that travel with the goods and reach a destination not always being the final customer, as for example parties like the Dutch Freight Forwarder keep most of the documents for internal control and traceability.

3.4. IT Platforms and Communication Systems
All the documents referenced above in Section 3.3 are managed and stored by each stakeholder in different ways and information systems (IS) according to their needs. Each information system is normally only accessed by the own organization and nor accessible by other actors, only the authorities' information systems are usually accessible by other organizations to process and generate the required authorizations and certificates. Each grower, freight forwarder or other third party has its own platforms, making the total of system that is estimated to be more than twenty, not including emails, fax or similar communication methods.

To some extent, some of the authorities’ systems have been simplified to one user interface often referred to as a single window system. The documents are filed in at least three different systems of the authorities (both
in Kenya and Netherlands). The other actors also have various information systems which they utilize in connection with the shipment. Each of the service providers also utilize a range of enterprise information systems e.g. for operation, for customer relation and for accounting.

Table 3.1 below is an overview not only of the IT systems involved but also the communication and transference systems (like physical mail, email and shared IS like Freshtrack). As detailed in the table both mail and email are the main communication systems used, without much security and protocols involved.

<table>
<thead>
<tr>
<th>System</th>
<th>Seller</th>
<th>LSP (Overseas Road Transport)</th>
<th>LSP (Overseas)</th>
<th>Auth (Kenya, HCDA)</th>
<th>Phyto (Kenya)</th>
<th>Cut (Kenya)</th>
<th>Agent (Overseas Cargu Handler)</th>
<th>Cut (Holland)</th>
<th>Phyto (Holland)</th>
<th>F (Holland)</th>
<th>Consignee (F/R), Export Agent</th>
<th>Consignee (F/R), Import Agent</th>
<th>Consignee (F/R), Final Customer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FreshTrack</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Grower Internal System (i.e. SAP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KN Phyto System: EC5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KRA SIMBA System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT, Internal System (i.e. Cargowise)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom System: AGS System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NL Phyto System: CLIENT System</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.5. Process Critical Path

The critical path in a supply chain process help to identify the path inside the different options and ‘routes’ that can appear within the supply chain that can denote major risk of interruptions or delays in the process or have a negative impact in any step of it. It can be the case that the critical path is not the most frequent or the one that reach more actors in the chain, the key factor to determine the trail is the impact it can have over the stakeholders and the whole chain.

In the case of the Kenya Air Trade Lane, the critical path is defined by the impact of the risks that are found over one of the possible routes of the whole chain, and although is not the most frequent trail, the negative impact of the risks held in it, turns it into the critical path of the process. The detail on the risk scenarios found over this path are explained in the following chapter.

The critical path is based on the current process explained in Section 3.2 of this chapter. It starts in Kenya with the Grower organizing the purchase order by sending it to the Import Agent, who in this case is the Final Customer of the goods that will be shipped for Auction. The grower will then create the initial documentation while the goods will be transported to the freight forwarder warehouse, via the road transporter, where the Phyto inspection will be held. Both the document officer and the grower must validate the correctness of the documents (i.e. the packing list) before the Phyto inspection take place, so there are no errors or delays that can affect the process.

With the Phyto-approval, the document officer arranges the certificate and the stamped invoice, to later on organize the export certificate with the applicable authority, situation that leads to pass all the paperwork to the Kenya Logistic Service Provider (LSP). After receiving and validating the documentation, the LSP will consolidate, from different growers, the diverse batches of goods that will be consolidated and shipped: once all the information is gathered, the LSP creates a consolidated invoice and certificate to later on arrange the stamping and validating of them with both Customs and the Phyto authority.

After the consolidated documentation is complete and with goods still in the freight forwarder facilities, the paperwork is now handed to them so the shipment approval process can be finalized. After endorsing the doc-
lements, the freight forwarder requests the C17 form (export declaration) with the customs authority. Once the KRA authorization is completed, the freight forwarder processed to create and complete the House Airway Bill (HAWB) and the MAWB with the airline.

With details of the flight arranged with the carrier, the freight forwarder later on scans all the documents and certificates into their internal system, so the counterpart in Netherlands starts processing the required authorizations in the destination country. This step is important and key so the Freight Forwarder is able to have all documentation in time to carry out the goods as soon as they arrive.

After all documentation is properly scanned, is passed with the goods to the cargo handler so they can start the load of products first on pallets and then the airplane. When the carrier receives all the paperwork, fills the Master Airway Bill (MAWB) with the required details about the goods to ship. While the goods are being transported, the carrier fills the information for the ENS as required by Customs, to which customs answers with a Movement Reference Number (MRN) compulsory to allow the goods to enter the country. After it, they also process the Summary Declaration for Temporary Storage (SAL). After both declarations have been approved, the airplane is unloaded by the cargo handler, who also receives all the documentation straight from the carrier.

After Customs validate the information of the ENS, and if is specified that the shipment must be inspected, the cargo handler is in charge of looking after the inspection before sending the documentation and goods to the Freight Forwarder.

Simultaneously, the Freight Forwarder applies for the phytosanitary approval from the NVWA, while the entry process is still ongoing. At the point, the Freight Forwarder is being notified about the required inspection, they also receive the physical copies of the documents from the cargo handler, notifying Dock Services with the details of the products that will be sent the next day. While at the same time Dock Services receives notification from the Import Agents about their shipments about to receive, so they can organize and fix the schedule.

Knowing that there will be a document inspection by the NVWA, the Freight Forwarder send the required information via mail to the authority, and immediately continue to request the transit declaration (TI) to be able to transport the goods to DS, and then with process the Import Declaration without actually waiting for confirmation of receipt and approval from the NVWA. All documentation must be in place for the inspection so there are no delays in the release of the goods.

The Freight Forwarder process the import declaration and awaits the response which, in this case, also indicates that the shipment is required for inspection. So the freight forwarder will notify Dock Services about the inspection thereby the shipment can be prepared. Once customs approve the release, the Freight Forwarder will notify DS via email that products are free to be release.

With the releases notification, the shipment is ready to be carried to the final customer by Dock Services. With the products being for auction, they are sent to the Import Agent, who will fill the EAB form required to deliver the goods to FloraHolland for the sale. With this information, FloraHolland receives the goods and organize them to be auction in the upcoming sale.

### 3.6. Process Critical Data

With the definition of the critical path in the trade lane it is possible to identify the critical data that must always be visible, complete and correct so the supply chain works effectively. Without the critical data the trade lane can suffer delays and even be costly for the parties involved in the chain as some activities must be reprocessed to get the correct data.

The data is separated in four different categories:

- **Document**: Header information about the documents and certificates involved in the trade lane, as for example invoice numbers, IDs and authorization codes.
- **Parties**: Detailed data about the parties involved in the different transactions related to the trade lane.
Information about the seller, consignee or transporter is stated in this category.

- **Product + Packing:** This division collects all the details about the goods that are shipped, as number of boxes, weights, volumes, among other data.

- **Transports:** The complete data about the mean of transportation, shipment details, destination and important dates are gathered under this category.

With the information about the critical path on the trade lane detailed in the previous section and the whole data set contained in the different documents, it was possible to evaluate and validated which data is recognized as critical within the Kenya trade lane. With the premise that all the documents and information is essential for the trade lane, the critical path of the process has in fact some documents that are more relevant than others: the invoice proforma, phyto certificate or the HAWB are an example of these key documents that are required for the flow of the trade lane. The most relevant documents required for the critical path of the process are marked in colour green in the figures below.

At the same time, within these documents there is key data that is essential for the authorities to certify the goods and its source, as also for the other actors to successfully process and progress the goods and information within the chain; details about the goods, consignee and seller as also the invoice number, are among this data.
Risk scenarios help to make risk more understandable for everyone involved and allows for a proper analysis and assessment [32]. It helps to estimate the impact or decrease in value in case of an unfavourable event determining where both the value or possible liabilities exist.

Every risk scenario describes the possibility of occurrence of an event that leads to operational or administrative loss, estimating the event frequency and impact, loss forms, as also the possible options to reduce the scenario frequency and impact. For a good analysis, the risk scenario description must include elements such as the actors or stakeholders involved, the threat type, events and assets or resources.

Using risk scenarios to analyse the trade lane allow us to frame the issues in a way that is understandable and that explains the subject and what is intended to complete, as also identifying the participants and the inputs so a complete picture of the scenario can be draw. They allow us to have more detailed information on the critical points that can be benefit from the implementation of a chain assurance.

FloraHolland through its Kenya air trade lane interacts with many parties that potentiate the amount of possible risk scenarios regarding the data and information that is created and shared, as each of these actors has also individual interests and problems that affects the chain. As the CANTOR approach follows COBIT methodology to identify and write down risks, we will use the same methodology so the evaluation can be standardized. Going by the aforementioned framework’s methodology and also by interviewing some of the main actors in the chain, we were able to categorize (both by the impact level of the risk (i.e. low, medium and high) and the main area of affected by it) and recognize some of the most influential risks on the trade lane. Based on interviews with the main affected actors by the defined risks, each of them is categorized and rated according to the frequency of occurrence and impact it has over the whole chain, while also explaining the main vulnerabilities, country of occurrence within the trade lane and the consequences for the process and the actors involved.

Based on the mention interviews and further analysis with the company’s supervisor, a total of seven risk scenarios were identified and are analysed up next. Each of them has the main name (threat event), rating, category (as defined above), difficulty to detect, vulnerability and consequences.
<table>
<thead>
<tr>
<th>Risk</th>
<th>1 of 7</th>
<th>Rating: MEDIUM LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of Occurrence</td>
<td>Kenya</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Threat Event</td>
<td>Inaccurate goods' weights data from growers.</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>Information</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Validations and checks are manual, and each actor has its own weights calibrated and not synchronized within the chain.</td>
<td></td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Inaccurate invoicing, over billing / under billing from airlines, agents and suppliers. Safety implications and is considered a criminal act. An agent under-declaring weights would in addition to criminal action being taken, would lose its IATA license allowing it to conduct business within airline/s.</td>
<td></td>
</tr>
<tr>
<td>Rating Explanation</td>
<td>Although the checks are manual and that increases the probable magnitude of the risks, the validations are done in regular bases and in several steps of the process that reduce the possible frequency of the risk and impact as well.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>2 of 7</th>
<th>Rating: VERY LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of Occurrence</td>
<td>Kenya</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Threat Event</td>
<td>Miscommunication between grower and unpacker (re-box count).</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>Physical Operations</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>Validations and counts are manual, and no formal policies and standard forms of communication between the growers and the unpackers in the airport</td>
<td></td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Suspicion of missing boxes or stolen product.</td>
<td></td>
</tr>
<tr>
<td>Rating Explanation</td>
<td>The suspicion of something happening to the goods is always present but there are secure mechanisms implemented as well as partnerships with trusted partners.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>3 of 7</th>
<th>Rating: HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of Occurrence</td>
<td>Netherlands</td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Operations</td>
<td></td>
</tr>
<tr>
<td>Threat Event</td>
<td>Lack of alignment between the actors in Inspection's requests in the Netherlands.</td>
<td></td>
</tr>
<tr>
<td>Target</td>
<td>Communication Operations</td>
<td></td>
</tr>
<tr>
<td>Detection Difficulty</td>
<td>Difficult. Lack of standardized communication.</td>
<td></td>
</tr>
<tr>
<td>Vulnerability</td>
<td>No formal policies and standard forms of communication between the parties in the Netherlands</td>
<td></td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Criminal research of the actions in Dock Services, as also lose the license as an approval place to conduct the Phyto Inspections</td>
<td></td>
</tr>
<tr>
<td>Rating Explanation</td>
<td>Although the frequency of the event is not as recurrent the impact that it can have over the chain is very high, as Dock Services can be suspended of its activities and leads to additional costs and longer lead times in the chain.</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>4 of 7</td>
<td>Rating:</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>Country of Occurrence</td>
<td>Kenya</td>
<td>Category</td>
</tr>
<tr>
<td>Threat Event</td>
<td>Electronic Certificate being blocked by KEPIIS</td>
<td>Target</td>
</tr>
<tr>
<td>Detection Difficulty</td>
<td>Medium. Manual Checks of the goods, but system check of actors.</td>
<td>Vulnerability</td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Denying exit of the product and causing delays or even the destruction of the goods</td>
<td>Rating Explanation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>5 of 7</th>
<th>Rating:</th>
<th>MEDIUM HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of Occurrence</td>
<td>Kenya / Netherlands</td>
<td>Category</td>
<td>Information</td>
</tr>
<tr>
<td>Threat Event</td>
<td>Sensitive data wrongly captured</td>
<td>Target</td>
<td>Information</td>
</tr>
<tr>
<td>Detection Difficulty</td>
<td>Difficult. Manual checks.</td>
<td>Vulnerability</td>
<td>Errors on capturing and entering the data when applying to the required certifications (i.e. wrong quantities, uncompleted information).</td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Delays in the trade lane and reprocess of some of the activities. Lower quality of the product by the end of the process. A delay is not a penalty but affects the overall performance in the supply chain [that can also lead to a penalty, depending on the circumstances]</td>
<td>Rating Explanation</td>
<td>High frequency (at least twice a month) with big impact over the chain as it causes delays in the process therefore lowering quality of the product.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk</th>
<th>6 of 7</th>
<th>Rating:</th>
<th>LOW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country of Occurrence</td>
<td>Kenya</td>
<td>Category</td>
<td>Regulatory Compliance</td>
</tr>
<tr>
<td>Threat Event</td>
<td>Failure to submit a EUR1 invoice.</td>
<td>Target</td>
<td>Physical Operations</td>
</tr>
<tr>
<td>Detection Difficulty</td>
<td>Easy. Known required document.</td>
<td>Vulnerability</td>
<td>Lack of visibility in consolidated shipments</td>
</tr>
<tr>
<td>Consequence(s)</td>
<td>Dutch customs charging Logistic Service Provider for customs duties as also payments cannot be recovered from the exporter, representing a large financial loss for this type of operation. The party can also be marked in the black list of Dutch authorities.</td>
<td>Rating Explanation</td>
<td>As the EUR1 invoice is one of the required documents when the shipment exceeds a total amount of €6000, organizations are aware of its importance, so the frequency of this risk is low.</td>
</tr>
</tbody>
</table>
Once all risks are collected and tabulated, it's necessary to collect them under one matrix so all of them can be prioritize and scale. Every enterprise needs an end-to-end aggregated view of the risks to prevent a false sense of security or a false sense of urgency, allowing a proper review of risk inclination and tolerance, instead of only having single views of individual risk items as previously defined [32].

As we use the same metrics to analyse the risks within the complete trade lane and for each individual player (both frequency and impact), all of them can be combined in a same risk matrix. Based on COBIT for Risk all the scenarios are put on the same matrix or map as visualized in the figure below (Figure 4.1).

Based on the analysis over the risk scenarios matrix, the goals of the research (scenarios that involve more than one party) and validating both the risks overall impacts and frequencies, three of the risks setups are selected for further evaluation: risks scenarios 3, 5 and 7.

In the upcoming section, each of these selected scenarios will be detailed and analysed further. This information is input for the evaluation of the current status of assurance in the trade lane, as they provide evidence of the existing risk weaknesses in the chain.
4.1. Risk Scenario 3: Lack of alignment between the actors in Inspection requests in the Netherlands

**Actors:** Freight Forwarder, NVWA, Customs-NL, FloraHolland Dock Services.

**Risk Category:** Architecture.

**Threat Event:** Miscommunication between the actors in the Netherlands can create errors while presenting the proper and required documentation to the Dutch authorities (both NVWA or Customs), situation that can entail monetary penalizations for the Freight Forwarder or temporary loss of the necessary licenses to FloraHolland Dock Services to work the trade lane.

4.2. Risk Scenario 5: Sensitive data wrongly captured

**Actors:** Grower, Kenya Freight Forwarder, Dutch Freight Forwarder, NWVA, Customs.

**Risk Category:** Information.

**Threat Event:** Errors on capturing and entering the data when applying to the required certifications (i.e. wrong quantities, uncompleted information), entails that there can be monetary penalties as also delays in the process to release the goods, affecting the quality of them and final customer satisfaction.

4.3. Risk Scenario 7: Lost of information in consolidated shipments

**Actors:** Grower, Overseas Logistic Service Provider, Customs, NWVA, Freight Forwarder.

**Risk Category:** Regulatory Compliance.

**Threat Event:** When a consolidated shipment is organized, the information about the consignor changes from the multiple growers to FloraHolland Services Kenya. As a result, the custom authorities in the Netherlands loses visibility over the real information and can't authenticate the information about the original source and confirm the legitimacy of the growers.

One other affected actor within this scenario is the overseas logistic service provider, in charge of all the paperwork of the consolidated shipment. Giving the wrong weight information to the airlines in the consolidated certificates has vast safety implications and is considered a criminal act. An agent under-declaring weights can, in addition to criminal action being taken, lose its IATA license allowing it to conduct business with an airline.
This chapter will cover how the analysis of the risks on the Kenya air trade lane will be managed as well as the application of the CANTOR approach to validate the current state of the trade lane and evaluate the possible assessment for the defined scenarios in Chapter 4. First a small summary of the chain risk management approach explained in Chapter 2 will be addressed; followed by the theory on how structured interviews to analyse the current risk state is developed and the configuration of the hypotheses and complete analysis.

5.1. Chain Risk Management

As shown and detailed in the literature review, there are lots of frameworks and standards for risk management as ISO 31000, IS/EC 27005, COSO ERM, COBIT for risk among others; which are useful to analyse and assess organizational risk. However, for a network of organizations that interact through a chain, the risk management function and perspective have a different scope. The CANTOR approach adds an extra view to the chain that includes the transference of risk in the chain, and creates control points and measures when necessary.

The whole approach and model is referenced in the intra-organizational risk components of COBIT for Risk framework; however, translated to chain environment. The chain component for CANTOR are presented in Figure 5.1.

![Figure 5.1: CANTOR Components (73)](image)

These components lead and are one of the main sources for the the risk management structured interviews designed to analyse the current state of each of the actors in the chain. This will be further developed in the next section.
5.2. Chain Risk Management Questionnaire

In designing the questionnaire to validate the current state of the chain the theoretical aspects about reliability and validity, explained by Y. W. van Wijk (2015) [73], were followed and applied:

Reliability is defined as the degree of stability exhibited when a measurement is repeated under identical conditions [42]. A lack of reliability can occur when there are divergences between observers or instruments of measurement, or instability of the attribute being measured.

Validity can be defined as how well a questionnaire measures what it sets out to measure as the main goal. It can be measured in four forms [42]:

- **Face validity**: Cursory review of survey items by untrained judges.
- **Content validity**: Subjective measurement of how appropriate the item seems to a set of reviewers who have some knowledge of the subject matter.
- **Criterion validity**: Measure of how well one instrument stacks up against another instrument or predictor.
- **Construct validity**: How meaningful the scale or instrument is when it is in practical use.

In the execution of the questionnaire the different forms of Litwin regarding the measuring of reliability and validity will be applied where possible.

The questionnaire will be provided to the actors via email as they are situated in locations difficult to approach either personally or by regular mail. Regarding the questions, the goal is to evaluate the and measure the levels of risk control and awareness each of the actors have, as well as the differences that can exist between them; for this we will elaborate questions in an interval scale, measuring each response from 1 to 5, with 1 being 'Strongly Disagree, all the way to 5 being 'Strongly Agree'.

The Kenya Air trade lane process analysis described in Chapter 3 provide the proper and required information to validate and define the risk scenarios explained in Chapter 4, as also the mandatory data for the process to work correctly. Both sets of facts help to corroborate the missing information in each step in the trade lane as also the mismatches that can appear. Such information was fundamental for the design of the structured interview, as it also helps to understand the important points to address and the ones that require more focus.

The questionnaire was designed as a qualitative structured interview developed within the complex trade lane using inductive reasoning and focusing both on the process as well as the required outcomes so it can cover all the required points for the CANTOR approach, as is the base lane to evaluate the trade lane and assess the defined risks. As CANTOR is, at the same time, based on the COBIT for risk framework, this was set as the starting pillar to define the different questions for the structured interview, so the results can be analysed later on in the CANTOR approach perspective. The questionnaire is divided in seven different sections according to the enablers defined in COBIT, where each of these sections represent factors that influence and support the governance and management over the enterprise's information, ensuring an effective and efficient risk control function [32]. Based on COBIT, the seven 'enablers' or categories for the survey are:

1. **Principles, Policies and Frameworks**.
2. **Processes**.
3. **Organisational Structures**.
4. **Culture, Ethics and Behaviour**.
5. **Information**.
6. **Services, Infrastructure and Applications**.
7. **People, Skills and Competencies**.

48
The risk management questionnaire will contribute to conclusions in four main topics:

1. **The Service Content Network (SCN):** Validating the overall chain operational efficiency.

2. **Service Delivery Network (SDN):** Results on adequate protection against external attacks and intrusion, among other sources.

3. **Data Pipeline Information Quality:** Monitoring services for security-related events.

4. **Enterprise Assurance Evaluation:** Authorities declarations and certificates throughput time.

The four points will be tested in the first set of risk management structured interviews on the current individual organizations in the Kenya air trade lane, where the analysis of the answers will then be placed in the context of the complete chain, so this can be interpreted as a single organization. Figure 5.2 displays the categories, hypothesis structure and following steps after the questionnaire.

The results of the risk questionnaire will represent the current situation of the organizations in the chain. First, and to reach the chain objectives an alignment of objectives within the chain needs to be established by transfer of obligations risk-control (TORC), and the conclusions help accomplish this goal.

Based on the results, an evaluation of the questionnaire will be reported to all organisations and stakeholders. In this evaluation also a set of new questions will be submitted interpreting the individual organization point of view towards the chain point of view.

Appendix A contains the complete questionnaire that was sent to the different actors in the trade lane. The questionnaire was design and later forwarded online in Google Forms, so each actor can have an easier access to fill it in.

### 5.3. Risk Management Questionnaire Results

In the Kenya - Netherlands Air trade lane for flowers there are a total of eighteen types of actors involved that exchange information to ensure that the chain works correctly.

From this group, a representative number of organizations were requested to fill in the questionnaire; based on the risk scenarios, their impact on the trade lane and the role of the actor in the chain. This resulted in a

---

**Figure 5.2: Chain Assessment and Hypothesis Structure**

Appendix A contains the complete questionnaire that was sent to the different actors in the trade lane. The questionnaire was designed and later forwarded online in Google Forms, so each actor can have an easier access to fill it in.
selection of six of the eighteen actors to fill in the study: Growers, Overseas Logistic Service Provider, Freight Forwarder, Carrier, Dutch Customs Administration, and FloraHolland. The questionnaire was sent to 10 partner organizations that were part of the group, in each of the targeted organizations, with collaboration of the FloraHolland supervisor, we selected a person that works in each of the companies that has the complete knowledge of the trade lane and the information exchanges that take place within (i.e. supervisors, account managers, etc.). The structured interview resulted in a response rate of 60%. Based on the responses we made conclusions about the current state of the actors in the chain regarding risk control policies and information management processes.

In Appendix B the detailed outcomes are presented, where the pie chart results for each of the questions is displayed with the final outcomes. The main idea for the questionnaire, besides measuring the alignment of the parties and current state of the chain, also allowed us to grasp, which of them have some level of security and internal assurance. They are the main source of analysis for the first group of conclusions about the current state of information sharing risk management within the trade lane. For every question we have interpreted the responses in a short analysis.

After the analysis of the answers, the main conclusion is that the Kenya Air trade lane chain has a lack of alignment of chain policy regarding documentation and information's internal activities, processes and policies as well as risk control. We concluded that there are large differences in the so called risk maturity levels of the individual chain participants, and that there is not much standardization, alignment and defined processes regarding risk controls within the chain. As such, we see organizations with well documented and well controlled processes, policies and services, while others have low levels of risk awareness and internal control. This may result in wrongly estimated risks, costly controls at inefficient points in the chain and possible redundant checks.

The intended approach, to treat the chain as one enterprise (Kenya Air Trade Lane Chain Enterprise), can have several benefits over the trade lane for all the actors involved. Establishing standard, transparent and distributed risk-control processes in the trade lane, the efficiency levels in the chain can improve as well as decrease the overall chain risks and have lower border inspection levels. By implementing adequate, aligned and auditable information management processes, there can be some perceived potential savings in the overall investment to reach compliance level with the authorities as also improved quality of the information in the trade lane and the information sharing processes. Ultimately leading to faster/reliable throughput of the shipments.

5.4. Additional Chain Enterprise Questions
Based on the first questionnaire results analysed in the previous section, and the Kenya Air Trade Lane Chain Enterprise point of view, we generalized towards four statements, that will be validated:

1. **Data Pipeline Information Quality:** If Information monitoring and alerts/warnings security notifications (or services) are established and aligned within the chain of organizations, the overall security and quality of the information in the chain can be established at a relative lower total chain cost (yet to be calculated), within the same overall risk exposure.

2. **Service Content Network (SCN):** By multiple actors in the chain, much effort is put in compliancy related activities (certificates, authorizations and inspections if required). If the risk-control quality is (proved) to be increased by executing proper measures in the early stages of the trade lane (i.e. Improving assurance levels), there can be potential savings in the overall investment on risk mitigation.

3. **Service Delivery Network (SDN):** If information security is formalized and communicated as a requirement at chain level, the assurance and awareness levels in the chain can be established by relative lower investments (yet to be calculated). This can be realized by adequate protection, and security measures implemented in the most crucial links in the trade lane.

4. **Enterprise Assurance Evaluation:** In case of distributed chain assurance and awareness, certain risk-control measures which were necessary in the past (for example data quality checks), can be cancelled. This will lead to increased chain efficiency, perceive lower total costs by investments at the right place in the chain.
These four statements are based on our analysis of the first questionnaire. In order to evaluate the statements, a second qualitative structured interview is designed which are based on the idea of having the Kenya Air Trade Lane as a *Chain Enterprise* as explained before. The final conclusions of the research will be evaluated considering both set of results.

Appendix C contains the complete new questionnaire that was sent to the different actors in the trade lane. The structured interview was design and later forwarded online in Google Forms, so each actor can have an easier access to fill it in.
6

FINDINGS AND RESULTS

Chapters 2 to 5 provide broad answers to the set of research sub-questions defined in the first chapter. The sub-questions were answered based on the risk management frameworks involving a deep analysis between the existing theory and the new proposed model to manage chain risks, what is ought to be according to the required guidelines, and the analysis of the actual current state of the entire process. The goal of this Chapter is to answer the main research question of the thesis: “Is the CANTOR approach a suitable framework to execute Risk Management for Information sharing that copes with international regulations and trade compliances within the trusted trade lane for shipping flowers from Kenya to the Netherlands by air?”.

On the one hand, answering the main research question is done by reflecting on the finding of the second questionnaire, and the application of the CANTOR approach in the risk scenarios. Moreover, it is done by integrating all the results from Chapters 3 to 5 in order to properly validate and analyse the risk maturity levels of the chain based on CANTOR. Doing this will help to design short, medium, and long term recommendations. The final recommendations are orientated towards the applicability of the CANTOR approach to similar processes.

6.1. Interplay of the Findings

In chapters 2 to 5 it was preformed both a literature study and definition of a case study, in order to gather several points related to the evaluation of an integrated risk management model in the Kenya Air Trade Lane for FloraHolland. It was mentioned several times the process to evaluate the integrated risk model, its pros and cons, and the current state of the trade lane where the evaluation will be achieved. Moreover, in this research numerous other connections could be established between the results, helping to design recommendations and further researches.

6.1.1. Integrated Supply Chain Risk Management

Supply chain processes as the Kenya Air Trade Lane, imply that companies expand their relationships and network with the partners involved in the process and hence become dependent on each other. Risks are a known variable in these activities that have impact upon either one organisation or even the entire chain.

To cope with this risks, different frameworks have been established so organisations are able to cope with this risks, as for example ISO 31000, COSO ERM or Cobit5. But each of this frameworks are mostly focused to assess risks within the limits of one single organisation and they are hardly implementable to build the risk framework for an integrated chain, like the mentioned trade lane. In this cooperative and shared environments it is normal to have individual goals, where each company in the process are confronted by different risks to control; some of them are mutually dependent within the network; situation that is not considered in the above mentioned frameworks.

CANTOR is the suggested approach to analyse the processes and risks in an integrated supply chain and validate the dependencies inside FloraHolland’s air Kenya trade lane, that can cope with the limitations of the existing risk management frameworks.
6.1.2. Kenya Air Trade Lane

Bringing the goods from Kenya to the final customer in the Netherlands involves the exchange of a great deal of information for the process to work and flow correctly. Authorities certificates, packing lists, invoices and other documents are exchanged between all the actors, making the process big and complex enough that for the complete analysis of the process was necessary to divide it in six sub-processes as detailed in Chapter 3. To analyse and assess the risks within the complete trade lane, the existing frameworks can seem incomplete and partial as they can't provide a chain view to evaluate the whole process and both the interactions and information exchanged within the organisations.

To evaluate if the CANTOR approach is suitable and fitting solution to assess the different information sharing risks that can emerge in the Kenya Air Trade Lane it is important to first collect the evidence to verify the current state of the chain and its flow: actors involved, documents exchange, critical data and path, as also IT platforms and systems that support the process.

Further, it was found that the process has a total of eighteen actors and more than ten different documents exchanged and distributed in the trade lane, making the sharing of information process complex enough to evaluate the applicability of the CANTOR approach to assess the risks.

6.1.3. Risk Scenarios

The risk scenarios allowed us to frame the issues in an understandable way so it is easier to identify the key actors and critical activities in the trade lane. Through the analysis of the current process of FloraHolland Kenya Air trade lane, it was possible to identify a total of seven risks related to information sharing within process.

From these set of possible risks in the chain we followed COBIT’s 5 mapping and prioritization methodology to select the three of them that have bigger impact in the process based on the analysis over the risk scenarios and the applicability of the CANTOR approach over them. The main evaluation for the research and the validity of CANTOR to assess chain risks, are done upon the three selected information sharing risk scenarios in the Kenya Air Trade Lane.

6.1.4. Trade Lane Risk Analysis

With the risk scenarios well defined it was required to validate the current risk awareness levels in the trade lane. Based on the CANTOR approach (and COBIT), a questionnaire was design to cover all the required points and evaluate the current state of the trade lane.

With this questionnaire, it was possible to conclude that the FloraHolland's Air Kenya trade lane is unaligned and divided process regarding chain policies concerning information sharing, management and risk control activities. The risk maturity level of each actor is different and a lack of standardization was found. This input helped to designed a final structured interview to ask each of the actors the point of view about the implementation of different control measures to improve the information sharing risk control levels in the chain.

6.2. Chain Enterprise Evaluation

The questionnaire detailed in Appendix G was sent to the same group of representative organizations as the first one (detailed in sections 5.2 and 5.3), which resulted in the selection of seven key actors: Growers, Overseas Logistic Service Provider, Freight Forwarder, Carrier, Dutch Customs Administration, and FloraHolland (+ FloraHolland Dock Services). The structured interview was sent to 11 organizations that were part of this group and participated in the previous questionnaire (as a way to have consistent results). It had a response rate of 63.64%, and based on the responses we made conclusions about whether the CANTOR approach is valid or not and the recommended assessment and evaluation to improve information sharing risk control in the chain.

Below, the chart results for each of the four statements is presented, as also the general comments made by some of the organizations that took the questionnaire, and the final conclusions on the assertions. For every statement we have interpreted the responses in a short analysis at the end of each statement.
6.2.1. Statement 1: Monitoring and Alert Security Notifications

If information monitoring and alerts/warnings security notifications (or services) are aligned within the chain of organizations, the overall security and quality of the information in the chain can be established at a relative lower total chain cost (yet to be calculated), within the same overall risk exposure.

Answers Analysis

Parties in the trade lane agree that improving information security services is a way to develop the overall security levels of the chain, but is important to also improve the communication practices so the other actors are aligned and aware of the measures and no double checks are necessary or required.

6.2.2. Statement 2: Collaboration in Kenya Air Trade Chain

Additional specific investments in risk management, control and security measures in the early stages of the trade lane, will improve the total quality of control and assurance within the chain, and will lead to perceived lower total chain costs by cutting specific additional control measures, which eventually lead to increased chain efficiency.

Answers Analysis

There is a general agreement that improving the security and control measures for information at the first stages of the trade lane can bring benefits to the whole chain like increasing the efficiency and risk control levels on the chain. But is also important to develop the communication level so all parties are aware of the extra control measures at the begging of the trade lane.
6.2.3. Statement 3: Information Security
If information security is formalized and communicated as a requirement at chain level, within the Kenya Trade Lane, the overall assurance and awareness levels in the chain can be established by relative lower total investments (yet to be calculated). Therefore, the overall chain risks can be decreased and lead to lower compliancy costs and inspection levels.

Answers Analysis
Although there is an overall agreement on the importance of formalization and communication in the information security measures taken on the chain, there is also an important remark on the standardization and alignment on the required steps and activities each of the actors need to perform.

6.2.4. Statement 4: Risk-Control Measures
In the Kenya Trade Lane chain some additional risk-control measures taken by your organization, which were necessary in the past can be cancelled, when your organization has assurance that proper risk-control measures are already taken elsewhere in the chain. This will lead to perceived lower total costs by investments at the right places in the chain (and eventually a decreased chain throughput time).

Answers Analysis
Parties agree that proper communication, awareness and distribution of the risk control measures across the chain can lead to perceive lower costs in the trade lane operation and decrease the overall chain throughput time. However, currently there is doubt and uncertainty of the measures taken in Kenya, that prevent the success of these measures.
6.3. Analysis of Results

With the information provided by both questionnaires is possible to conclude key points regarding the trade lane and the chain enterprise approach:

From the first structured interview it was concluded that in the current situation there is no real alignment of the strategies between the actors in the trade lane, where each organization works to achieve the individual goals. This situation implies that there is no transference or distribution of the control points over the chain, and each actor is responsible for its own goal without any communication between them. Therefore, there are no chain risk awareness and auditing methods established in the trade lane.

Based on these results, and aiming to establish better assurance levels in the chain organizations, the second questionnaire allowed us to conclude the view each of the actors have on the chain enterprise approach and the govern, audit and control strategies to implement based on the CANTOR approach. According to it, all of the participants in the chain did recognized the fact that if a chain policy is implemented where all the norms and requirements are well communicated in the chain and proper risk control measures for sharing information, according to the aforementioned policies, are implemented for all the organizations in the trade lane (mainly for the actors at the beginning of the chain, i.e. actors in Kenya), a chain enterprise assurance level can be established in the trade lane.

In this way, both the number of inspections and throughput time in the trade lane can decrease as efficiency improvements. But, trust between the actors within the chain (mainly for the actors at the beginning of the chain) and overall inefficiency in the trade lane are mayor factor that affect the perform of the process as it continues to require additional risk controls over the information shared in (mainly the end of) the chain.

The CANTOR approach provides a strategy for establishing assurance in chain organizations, by a governing strategy, risk management, audit and control. In the case of FloraHolland's Kenya Air Trade Lane it can be assumed, based on the questionnaires results, that in order to successfully implement CANTOR approach for chain as enterprise assurance evaluation, it is first required to improve the trust and awareness levels every organization participant of the trade lane have with each other: the actors are aware of the benefits of the chain enterprise approach but currently there is not enough trust or control measures that supports the implementation of the model.
In this final chapter we present the summary of the research, the overall obtained results and main conclusion. Also depict the limitations of the research and whether the obtained results are applicable in a broader sense than the research area explained in this thesis. Later on, we will present advice on possible further research, recommendations and concluding remarks.

7.1. Research Summary and Conclusions

“In contemporary competitive business environment, it is imperative for businesses to continuously work on improving the performance of their supply chains. Consequently, integrated supply chain decisions and coordination across supply chains are frequently sought for improving performance of supply chains” [36]. Collaboration is no longer restricted to dedicated rooms within single organizations with teams working together. Nowadays, and with a more globalized market and competition, organizations have to be able to work together with their partner companies and collaborators, independent of the barriers of time and place, and so have more competitive processes.

As information sharing between organizations becomes more relevant in integrated supply chains, also the collaboration between them becomes key to be aware of the different risks that can emerge in the process and establish assurance through the whole chain.

In this thesis we focussed on the evaluation of an integrated approach for risk control and assurance in a trade lane process, validating the collaboration and awareness levels on the specific case study of FloraHolland's Kenya air trade lane.

The research project is explorative, with focus on a specific case study, where the findings gave us assurance in answering the research sub-questions and the main research question. The main research question within the master thesis was:

*Is the CANTOR approach a suitable solution to perform Risk Management for Information sharing that copes with international regulations and trade compliances within the trade lane for shipping flowers from Kenya to the Netherlands by air?*

This main research question is fragmented in four research sub-questions that helped to specify our focus within the field of our research:

- *What are the stakeholders and the current process related to information sharing and border control in the Kenya trusted trade lane by air, and the information infrastructure, main norms and policy strategies that supports it (based on the CASSANDRA outcomes)?*
- *What are the main characteristics of the CANTOR approach that differentiate it from other risk management frameworks and allow it to be more suitable to evaluate the study case?*
In our research we used the case study approach, where to address the research questions and the main problems, we focused in FloraHolland’s Kenya Air trade lane, and within, three different risk scenarios to validate the model. This approach yielded our main conclusions. We will present the main conclusions for every research sub-question that will lead to the conclusion of the main research question.

RQ1: What are the stakeholders and the current process related to information sharing and border control in the Kenya trade lane by air, and the information infrastructure, main norms and policy strategies that supports it (based on the CASSANDRA outcomes)?

In order to evaluate the applicability of the CANTOR approach, and come to a clear description of the possible risks in FloraHolland's Kenya Air trade lane, one must first know and have clear understanding of the current process. For a complete comprehension of the trade lane and the information shared on it, we determined different core points to focus that provide valuable input on the status of the chain:

- Involved stakeholders and role in the trade lane.
- Complete description of the activities and flows on the trade lane.
- Description of the norms and policies that support the activities in the process.
- Route or path for each of the documents exchanged between the actors.
- Information systems used for the exchange of documents and data.
- Trade lane critical path and data.

These components allowed us to describe the complete process and validate the current status of the trade lane and have a complete understanding of the information shared between the organizations participant of the process. With the validation of the critical path and critical data it was possible to corroborate and support which are the key actors and activities that require major consideration and are key in the analysis of the risk points to describe and evaluate.

RQ2: What are the main characteristics of the CANTOR approach that differentiate it from existing risk management frameworks and allow it to be more suitable to evaluate the study case?

To properly understand the main characteristics and extra value of CANTOR and how its approach towards risk management is different from the existing frameworks, is first important to come to clear understanding of what risk exactly is and how the existing frameworks work in order to assess the different hazards that the information in the trade lane is exposed.

The literature on some of the most known frameworks (i.e. COSO, COBIT, ISO 31000) suggests that risk is assess only at organizational levels, where the enterprise risk-related capabilities are evaluated to help understanding how an effective risk management optimises the business processes and value, improving the quality and reduced waste and costs can be defined. Although COBIT is a good example of a business framework that focuses on risks related to information and the technology platforms that supports it (as the case study), as the other mentioned frameworks, they are mostly focused in a single enterprise and the management of the risks over its processes, which can be hardly implementable to evaluate risks and establish assurance in an integrated chain.

The CANTOR approach helps to establish assurance in integrated chains, and also brings four new key drivers that allows to have a governing strategy, risk audit and control at the chain level and not individual per organization. The four drivers are:
• Atomic approach of the complete chain.
• Transference and distribution of the obligations of risk and control.
• A chain internal control system.
• And chain governance model.

These four drivers were published at the ICEIS conference proceedings 2014 (Wijk, Y.W., 2014) and are further detailed in the dissertation of YW van Wijk (University of Groningen, Delft University of Technology) which is planned at the end of 2015.

By designing and developing these four drivers, complex trade lanes like FloraHolland’s Kenya Air one, with multiple actors and several documents exchanged in the process, consents to have assurance at the chain level and assess the different risk scenarios in a complete way by analysing all the interactions within the trade lane, while with the other risk frameworks possible risks will be evaluated only at the enterprise level independent of the environment and set-up where they surface.

RQ3: What are the main and more critical information-sharing risks scenarios in order to assess the way information is transferred in the Kenya trade lane by air?

After all the information about the current state of the trade lane is gathered, the risk scenarios description includes elements such as the actors or stakeholders involved, the threat type, events and assets or resources. Using the scenarios allowed us to analyse the trade lane in a way that is understandable and that explains what is intended to complete, as also identifying the participants and the inputs, and be able to evaluate the applicability of the CANTOR approach.

The risk scenarios allowed us to evaluate specific situations and settings suitable for the CANTOR approach by corroborating conditions that cope and meet the requirements of the model: complex scenarios that have multiple actors involved, documents and information exchange, different IT platforms that support the activities, etc. The known risk management frameworks have the assumption that risks are independent, which can be correct in intra-organization. However, in chain organizations they are not, risks are environment dependent and influence each other mutually. For this, we selected three specific risk scenarios that allowed us to analyse intricate and difficult conditions that have big impact on main organization: FloraHolland, and the Kenya trade lane. The settings were the first and main input to later evaluate the applicability of the CANTOR approach in the supply chain of the case study.

RQ4: How can the CANTOR approach assess the risk scenarios established in RQ3 in order to enhance the integrity levels of the information shared across the Kenya trade lane by air?

Before evaluate if CANTOR is suitable as an approach to assure information sharing risk control in the Kenya air trade lane and validate how can assess the defined risk scenarios (if possible), it was important first to certify the current status of the control and assurance methods in the trade lane, by implementing a risk analysis of the chain. For the analysis of the current status of the trade lane, we designed a questionnaire with the support of the CANTOR approach expert and based on the seven enablers defined in COBIT for risk, as this framework is both the base for the mentioned model and its focus is mainly in information management and technologies.

With the risk scenarios defined, was possible to outline and state which of all the group of actors in the trade lane were the key ones to consider for the structured interviews. The responses and results of the structured assessment regarding the current status of the trade lane, presented important points as it showed the lack of alignment of a chain policy regarding documentation and information’s activities, processes and policies as well as overall risk control.

Having clear insight and knowledge of the status of the trade lane, again with the cooperation of the specialist of the model, the second questionnaire was design to validate the idea of having the complete trade lane as a
chain enterprise and establish assurance in the organizations as a whole chain, and creating a governing strategy, risk audit and control.

The results of the second structured interview allowed us to conclude that although all the main and key actors in the trade lane recognize the fact that if a chain policy is implemented where all the guidelines and norms are communicated and well spread in the whole chain, with proper risk control measures for sharing information, a chain enterprise assurance level can be established in the trade lane. However, it was also established that trust between the organizations within the chain (mainly with the ones at the beginning of the chain in Kenya) is a mayor factor that affects the performance and efficiency of the process as it continues to require additional risk controls over the information shared in the chain.

Trust is usually mistaken with similar terms like collaboration or cooperation, but it is actually not the same as organizations can cooperated under some risk control mechanisms without the requirement of trust [45]. This situation is visible in the Kenya air trade lane, as the cooperation levels of the parties is high, but as the questionnaire showed, the trust degree is not that much.

Therefore, and in order to successfully have chain assurance within the trade lane, and assess the different risks that exist in it (i.e. the defined risk scenarios), it is first required to improve the trust and awareness levels every organization participant of the trade lane have with each other. There is a general awareness that there is no control and alignment within the chain, without established communication or an enterprise assurance evaluation. With the implementation of the CANTOR approach, through the design of assurance points in the network, trust can be build.

As some progress has been done with the data pipeline concept, and its implementation in FloraHolland's Kenya trade lane (though the CORE project), having the capacity to link and access the actors' information systems and improving their visibility over the used information, can be set as a first step towards the required trust in a chain assurance. Improving the chain information integration and visibility allows the interested parties to validate how their partners are performing and certifying the quality of the information being shared, helping them being more reliance of the network.

At the same time, and either with or without the support of the data pipeline platform implemented, parties that consider that the assurance levels with some specific partners are low, can renegotiate the exiting agreements and design new SLAs that empowers the network association and trust can be built upon these new contracts.

These solutions can highlight the value the CANTOR approach can have over the assurance of the trade lane, as it builds over them and improve the established assurance in the chain. If chain policy and norms are clearly communicated within the chain, and control measures are implemented for all the participant organizations (but mainly in the beginning of the chain i.e. Kenya), then assurance can be established, and both the number of inspections and throughput time can potentially decrease, which both are efficiency improvements.

### 7.2. Thesis Reflections

As a way to analyse and evaluate the applicability of the CANTOR approach in the trade lane defined as a case study we addressed a total of four research questions as a way to be as clear and consistent as possible with the topic. Just the subject of risk management is complex enough in the amount of information that can be found in the literature, so a detailed approach was necessary from the beginning. Regarding the main research question was also a little difficult as, although the main topic of the research was clear and defined, the approach we wanted to take with CANTOR was a little unclear. Thanks to the help of Roel Huiden (supervisor in FloraHolland), Joris Hulstijn (first supervisor at TU DELFT) and Ype van Wijk (author of the CANTOR approach) who took the time to discuss in several different meeting the different possible approaches to the matter, it was decided to focus first only in the Air Trade Lane and the information exchanged within. As the research and the trade lane were complex enough it was believed that it was better to focus the evaluation of the model in three specific scenarios that had the necessary conditions and settings to assess, making the research more interesting in terms of diversity of possible scenarios and the complexity of the entire trade lane.
The output of this research is basically an evaluation of how the new model for establishing assurance in chain organizations is applicable in the type of supply chains that meet similar conditions as the one studied for FloraHolland. As it was concluded that with the current status of the trade lane, the CANTOR approach (i.e. Chain policy, risk management and audit and control), was not implemented. However, the output of this research can also be considered as a set of recommendations on what needs to be the minimum aspects that need to be considered in a proper supply chain.

As it was concluded that with the current status of the trade lane, the CANTOR approach is not suitable, the output of the research can also be considered as a set of recommendations on what needs to be the minimum aspects that need to be considered in a supply chain, so fits and is suitable to implement the chain assurance model.

This research can be seen as a starting point on the types of chains where the CANTOR approach can be applied and the aspects that is required to fulfil for a successful implementation. Yet, it is up to the FloraHolland team to decide weather to apply or not the model in the current process or not.

Most of the research projects have their limitations, and this one wasn't except to that. I distinguish two notable limitations in the study. First of all, the time constrain was a big impact on how the analysis and evaluation was performed, as it took a longer time to understand and define the goals for the project, so we had shorter amount of time to perform the required activities to evaluate the model. This resulted in fact that we might not collect enough empirical data to come to ‘hard’ conclusions, and although we collect the necessary data from the required actors, the conclusions are based on first experiences. Further empirical testing and development should lead to ‘harder’ conclusions.

Second, as CANTOR is a new approach to assess and assure chains, there is not a big amount of literature and information about it, and most of the theory and requirements are based on the knowledge of one expert on the subject.

But despite these few difficulties related to project, and the gathering of all the information and data, it was an interesting project that increased my knowledge base in regard to risk management, assurance in supply chains and information management.

7.3. Further Research Projects

Further research related to this thesis should, first of all, include additional empirical data for the evaluation of the model, involving either other not so significant parties in the chain or more partners from the defined key actors. This could lead to a refinement of the criteria and approaches used in this research. There is still a large area for research regarding the assurance in chains. We in this case based the research only in the Air trade lane of FloraHolland, so there are still processes like the Sea trade lane with more complex activities and controls that can bring new finding to the topic.

As part of the conclusions and remarks of the research there are some percept cost saving, that unfortunately were not calculated due to the short time frame of the project. Further research related to the analysis of the real cost savings and efficiency improvements to validate the conclusions of this project can be made.

In this research we focused in a chain within two different countries with high amount of collaboration among them but not aligned in control processes. What about chains in the same country or area, how can the model provide assurance in chains with more aligned risk control processes and better information technologies, how can it assess where more key actors are involved? These are some of the questions that remain unanswered in our research but are worth investigating. The model, while is new and still in develop, offers a lot of benefits with clear and simple measures to advanced and well stablished chains that should be investigated, and researches should be accomplished on further possible applications.
This questionnaire was designed to evaluate the current status of risk management and transfer of information within the flower trade lane from Kenya to the Netherlands. This is part of a thesis project in Delft University of Technology and FloraHolland in the Netherlands, in which we are evaluating the possibility of doing risk assessment on the whole chain instead of individually in each of the organizations involved.

The answers will be kept anonymous, without specifically naming each of the actors. Results at the end of the research will be shared with FloraHolland's partners if requested. The questionnaire is designed specifically to see the alignment among all the chain actors in risk assessment.

The questionnaire is divided into seven different topics that cover aspects of information sharing risks. It was designed following the COBIT framework on risk management, and reflects the maturity levels for internal control which are similarly applied by European customs organizations for the AEO self-assessment.

When answering the questionnaire, the focus of the respondent should be on the risks involving electronic information or documents that are used in the trade lane and on the internal processes that involve these documents. Each question has a total of four possible answers, and space for further explanation.

For a better understanding of what is being analysed, Figure A.1 below shows an overview of the process being evaluated in this research.
A.1. Principals, policies

1.1 Are there any policies or principles describing what actions should be taken in order to protect your computer systems, documents and information from unauthorized and risky intrusion?

1. No.
2. Yes, but not documented, communicated and formalized.
3. Yes, documented but only communicated to key people.
4. Yes, policies are documented and everyone is aware of the them.
5. **Explain further (optional):**

1.2 Are the information security guidelines embedded in the everyday activities and processes (i.e. sending/receiving emails, applying for online forms, opening attachments, etc.)?

1. No.
2. Yes, but not standardized or communicated.
3. Yes, but each employee applies them to their judgment.
4. Yes, and all employees should follow them through their activities.
5. **Explain further (optional):**

1.3 Do you have in-house compliance guidelines to meet authorities’ regulations?

1. No.
2. Yes, but not documented or communicated.
3. Yes, documented but only communicated to key people.
4. Yes, guidelines are documented and everyone is aware of the them.
5. **Explain further (optional):**

1.4 Are there requirements defined to choose business partners (i.e. security declarations, contractual requirements, trade partners with own AEO- status or ISO standards)?

1. No.
2. Yes, but not documented or communicated.
3. Yes, flexible and not standardized requirements.
4. Yes, requirements are documented and every business partner needs to comply to them.
5. **Explain further (optional):**

1.5 Is there an available document for all stakeholders in the supply chain that states the acceptable levels of risks the organization is prepared to accept regarding incorrect documents or information?

1. No.
2. Yes, but only to management levels.
3. Yes, documented but only communicated to key people.
4. Yes, acceptable risk levels are spread and everyone is aware of the them.
5. **Explain further (optional):**
1.6 Are there policies on what information can or can't be shared with the partners you have relations with?

1. No.
2. Yes, but not documented, communicated and formalized.
3. Yes, documented but only communicated to key people.
4. Yes, these processes are documented and everyone is aware of the them.
5. Explain further (optional):

1.7 Are there security and safety policies for trade partners in order to avoid abuse of information (e.g. endangering of the process through unauthorised transfer of shipping details)?

1. No.
2. Yes, but not documented and formalized.
3. Yes, but they are not applied in regular bases.
4. Yes, these procedures are documented and every partner is aware of the them.
5. Explain further (optional):

A.2. Processes

2.1 Are there defined processes that describe the actions you have taken to avoid risk in your information technologies (i.e. Firewalls, antivirus-programmes, password protection)?

1. No.
2. Yes, but not documented, communicated and formalized.
3. Yes, documented but only communicated to key people.
4. Yes, these processes are documented and everyone is aware of the them.
5. Explain further (optional):

2.2 Are there processes and practices on how to manage supply chain related documents (i.e. required certificates, export/import requirements)?

1. No.
2. Yes, but not documented, communicated and formalized.
3. Yes, documented but only communicated to key people.
4. Yes, these processes are documented and everyone is aware of the them.
5. Explain further (optional):

2.3 Are there documented procedures (manuals, work guidelines, information sheets, etc.) for notifying and reporting documentation or information risks?

1. No.
2. Yes, but only to management levels.
3. Yes, documented but only communicated to key people.
4. Yes, everyone is aware of the them and report them within the established methods.
5. Explain further (optional):
2.4 Are there documented general safety and security procedures?

1. No.
2. Yes, but only to management levels.
3. Yes, documented but only communicated to key people.
4. Yes, everyone is aware of the them and report them within the established methods.
5. **Explain further (optional):**

2.5 Are there documented procedures (manual, work guidelines, information sheets, etc.) of reporting security issues?

1. No.
2. Yes, but only to management levels.
3. Yes, documented but only communicated to key people.
4. Yes, everyone is aware of the them and report them within the established methods.
5. **Explain further (optional):**

**A.3. Organization Structure**

3.1 Is there a defined department within the organization in charge of internal control (i.e. regulations and policies)?

1. No.
2. Yes, but each department in the organization do their internal auditing with no formalized standards.
3. Yes, but each department in the organization do their internal auditing with formalized standards and processes from the organization.
4. Yes, there is a department in the organization in charge of controlling and auditing each department.
5. **Explain further (optional):**

**A.4. Culture Ethics Behaviour**

4.1 Are there policies concerning communication and employees’ behaviour (i.e. codes of conduct)?

1. No.
2. Yes, but not documented, communicated and formalized.
3. Yes, documented but only communicated to key people.
4. Yes, policies are documented and everyone is aware of the them.
5. **Explain further (optional):**

4.2 To what extent is compliance awareness embedded in the organizational culture (Is everyone aware of possible compliance issues)?

1. Is not embedded.
2. Is embedded, but only at management levels.
3. Is embedded, but each employee applies them to their judgment.
4. Is embedded in the culture and everyone is aware of possible risk situations.
5. **Explain further (optional):**
A.5. Information

5.1 Does the organization have an information system or dashboard to manage the major risks and control the everyday activities?

1. No.
2. Yes, but is not used.
3. Yes, but rarely updated.
4. Yes, and is updated constantly so everyone is aware.

5. Explain further (optional):

5.2 Do you have procedures for verifying the accuracy of the documents (correct and reliable) required for the export (as Kenya actor) or import (as Dutch actor) process?

1. No.
2. Yes, but not documented and formalized.
3. Yes, but they are not applied in regular bases.
4. Yes, these procedures are documented and every partner is aware of them.

5. Explain further (optional):

5.3 Do you have procedures for verifying the completeness of the documents required for the export (as Kenya actor) or import (as Dutch actor) process?

1. No.
2. Yes, but not documented and formalized.
3. Yes, but they are not applied in regular bases.
4. Yes, these procedures are documented and every partner is aware of them.

5. Explain further (optional):

A.6. Service, Infrastructure and Applications

6.1 Is there a group of people, processes, and technologies that help to establish the business architecture to minimized information risks within the organization?

1. No.
2. Yes, but each department in the organization has its own people, processes and technologies and no organizational architecture.
3. Yes, but the group is not meet in regular basis to update the architecture.
4. Yes, there is a group of people in charge of the business architecture and validate the possible risks in the organization.

5. Explain further (optional):

6.2 Is there a set of experts or advisors who help to ensure that new processes or technologies do not introduce unacceptable levels of risk?

1. No.
2. Yes, but each area in the organization has its own people and no organizational architecture.
3. Yes, but the group is not meet in regular basis to update the architecture.
4. Yes, there is a group of people in charge of the business architecture and validate the possible risks in the organization.

5. Explain further (optional):
A.7. People Skills Competence

7.1 To what extent do the employees know and have the ability to identify the goals and strategies of the organization and the key relationships with partners?

1. *It is not a stablished ability in the organization.*
2. *Only recognizable at management levels.*
3. *Is stablished but not key that employees knows them.*
4. *Is stablished in all the departments of the organization.*
5. *Explain further (optional):*

7.2 Is it important for employees in the organization to have both interpersonal and communication capabilities in order to have a better interaction with partners within the network?

1. *No.*
2. *Yes, but only at management levels.*
3. *Yes, but is a plus but not key that employees have them.*
4. *Yes, everyone is trained to have those capabilities.*
5. *Explain further (optional):*

7.3 Is security and safety training provided for employees?

1. *No.*
2. *Yes, but only at management levels.*
3. *Yes, but not on regular basis.*
4. *Yes, everyone is trained to have those capabilities.*
5. *Explain further (optional):*
APPENDIX B - RISK MANAGEMENT QUESTIONNAIRE RESULTS

B.1. Principals, policies

1.1. Are there any policies or principles describing what actions should be taken in order to protect your computer systems, documents and information from unauthorized and risky intrusion?

Answer Analysis: The policy to protect IT systems differs within the chain. There is no alignment or distribution of risks and/or control measures between the actors. To establish assurance at chain level, at least 2/3 of the involved organizations in the process has to adopt and implement the defined Trusted Trade Lane basic chain policies.
1.2. Are the information security guidelines embedded in the everyday activities and processes (i.e. sending/receiving emails, applying for online forms, opening attachments, etc.)?

Answer Analysis: In general, the information security within the chain is not embedded in the organizations. This can be a fundamental issue for establishing chain assurance as well as guaranteeing the data-pipeline information quality.

1.3. Do you have in-house compliance guidelines to meet authorities' regulations?

Answer Analysis: The compliance guidelines to meet authorities’ regulations is in general not implemented in all of the involved chain organizations. There is no alignment on how the actors pursue and trail the regulations.
1.4. Are there requirements defined to choose business partners (i.e. security declarations, contractual requirements, trade partners with own AEO-status or ISO standards)?

Answer Analysis: In majority there are no formalized, standardized and/or communicated constraints to become part of the Kenya Air trade lane.

1.5. Is there an available document for all stakeholders in the supply chain that states the acceptable levels of risks the organization is prepared to accept regarding incorrect documents or information?

Answer Analysis: The risk management function with respect to information quality in the chain is not available.
1.6. Are there policies on what information can or can’t be shared with the partners you have relations with?

**Answer Analysis:** The risk management function with respect to information quality in the chain is not available to everyone. Each actor defines what information wants to share according to each case.

1.7. Are there security and safety policies for trade partners in order to avoid abuse of information (e.g. endangering of the process through unauthorised transfer of shipping details)?

**Answer Analysis:** The risk management function with respect to information quality in the chain is not available.
B.2. Processes

See the analysis at the end of this section.

2.1. Are there defined processes that describe the actions you have taken to avoid risk in your information technologies (i.e. Firewalls, antivirus-programmes, password protection)?

2.2. Are there processes and practices on how to manage supply chain related documents (i.e. required certificates, export/import requirements)?

2.3. Are there documented procedures (manuals, work guidelines, information sheets, etc.) for notifying and reporting documentation or information risks?
2.4. Are there documented general safety and security procedures?

2.5. Are there documented procedures (manual, work guidelines, information sheets, etc.) of reporting security issues?

**Process Answers Analysis:** Basically, the information technology risk management is dependent on all involved organizations in the chain. At this moment, there is no chain policy defined or communicated within the process. At least half of the chain participants does not have a formalized and standardized management of document flows and/or procedures for information quality, safety and security.
**B.3. Organization Structure**

3.1. Is there a defined department within the organization in charge of internal control (i.e. regulations and policies)?

![Pie chart showing the distribution of responses]

- **No**: 50%
- **Yes, but each department in the organization do their internal auditing with no formalized standards**: 17%
- **Yes, but each department in the organization do their internal auditing with formalized standards and processes from the organization**: 33%
- **Yes, there is a department in the organization in charge of controlling and auditing each department**: 0%

**Answer Analysis**: Half of the chain participants does not have a formalized internal auditing function or process to review and check the internal activities.

**B.4. Culture, Ethics and Behaviour**

*See the analysis at the end of this section.*

4.1. Are there policies concerning communication and employees’ behaviour (i.e. codes of conduct)?

![Pie chart showing the distribution of responses]

- **No**: 33%
- **Yes, but not documented, communicated and formalized**: 50%
- **Yes, documented but only communicated to key people**: 0%
- **Yes, policies are documented and everyone is aware of the them**: 17%
4.2. To what extent is compliance awareness embedded in the organizational culture (Is everyone aware of possible compliance issues)?

![Pie chart showing compliance awareness]

**Culture, Ethics and Behaviour Answers Analysis** Only a minority of chain participants has formal embedded cultural behaviour and compliance awareness policies.

**B.5. Information**

*See the analysis at the end of this section.*

5.1. Does the organization have an information system or dashboard to manage the major risks and control the everyday activities?

![Pie chart showing information system status]

*Yes, and is updated constantly so everyone is aware*
5.2. Do you have procedures for verifying the accuracy of the documents (correct and reliable) required for the export (as Kenya actor) or import (as Dutch actor) process?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>33%</td>
</tr>
<tr>
<td>Yes, but not documented and formalized</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, but they are not applied in regular bases</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, these procedures are documented and every partner is aware of them</td>
<td>33%</td>
</tr>
</tbody>
</table>

5.3. Do you have procedures for verifying the completeness of the documents required for the export (as Kenya actor) or import (as Dutch actor) process?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No</td>
<td>50%</td>
</tr>
<tr>
<td>Yes, but not documented and formalized</td>
<td>16%</td>
</tr>
<tr>
<td>Yes, but they are not applied in regular bases</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, these procedures are documented and every partner is aware of them</td>
<td>17%</td>
</tr>
</tbody>
</table>

**Information Answers Analysis:** Within the chain there is no formalized policy regarding information accuracy, completeness as well as risk awareness. Only few actors in the trade lane have defined activities to control information accuracy and risk's control.
B.6. Service, Infrastructure and Applications

See the analysis at the end of this section.

6.1. Is there a group of people, processes, and technologies that help to establish the business architecture to minimized information risks within the organization?

6.2. Is there a set of experts or advisors who help to ensure that new processes or technologies do not introduce unacceptable levels of risk?

**Service, Infrastructure and Applications Answers Analysis:** Within the chain there is no formalized policy regarding information architecture and new technologies.
**B.7. People, Skills and Competencies**

*See the analysis at the end of this section.*

7.1. To what extent do the employees know and have the ability to identify the goals and strategies of the organization and the key relationships with partners?

<table>
<thead>
<tr>
<th>Percentage Distribution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33%</td>
<td>Only recognizable at management levels</td>
</tr>
<tr>
<td>17%</td>
<td>Established but not key that employees know them</td>
</tr>
<tr>
<td>17%</td>
<td>Established in all the departments of the organization</td>
</tr>
<tr>
<td>33%</td>
<td>It is not a established ability in the organization</td>
</tr>
</tbody>
</table>

7.2. Is it important for employees in the organization to have both interpersonal and communication capabilities in order to have a better interaction with partners within the network?

<table>
<thead>
<tr>
<th>Percentage Distribution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>17%</td>
<td>Yes, but only at management levels</td>
</tr>
<tr>
<td>17%</td>
<td>Yes, is a plus but not key that employees have them</td>
</tr>
<tr>
<td>33%</td>
<td>Yes, everyone is trained to have those capabilities</td>
</tr>
<tr>
<td>33%</td>
<td>No</td>
</tr>
</tbody>
</table>

7.3. Is security and safety training provided for employees?

<table>
<thead>
<tr>
<th>Percentage Distribution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>33%</td>
<td>Yes, everyone is trained to have those capabilities</td>
</tr>
<tr>
<td>50%</td>
<td>No</td>
</tr>
<tr>
<td>17%</td>
<td>Yes, but only at management levels</td>
</tr>
<tr>
<td>0%</td>
<td>Yes, but not on regular basis</td>
</tr>
</tbody>
</table>

**People, Skills and Competencies Answers Analysis:** Within the chain there is no standard policies regarding people's competences as well as safety and security awareness.
C.1. Statement 1: monitoring and alert security notifications
To ensure that the chain enterprise’s risk appetite and tolerance are understood, articulated and commu-
cicated, a process for monitoring and alerts/warning is necessary. If all chain participants are aligned on risk
appetite and chain risk tolerance, risks are properly identified and managed on chain level, the potential for
compliance failures can be minimised.

Within the Kenya Air Trade chain risks are mutually dependent. Therefore, the monitoring of key goals and
metrics of the risk management is a chain collaborative process to enhance how deviations or problems will
be identified, tracked and reported for remediation.

The current risk management in the Kenya Air Trade chain is not aligned, which make redundant control mea-
sure necessary. Therefore, the overall chain costs are higher than necessary.

Your opinion on Statement 1:  If Information monitoring and alerts/warnings security notifications (or
services) are aligned within the chain of organizations, the overall security and quality of the information in the
chain can be established at a relative lower total chain cost, within the same overall risk exposure.

<table>
<thead>
<tr>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongly Disagree</td>
<td>Disagree</td>
<td>Neither</td>
<td>Agree</td>
<td>Strongly Agree</td>
</tr>
</tbody>
</table>

Comments:

C.2. Statement 2: Collaboration in Kenya Air Trade Chain
The highest costs activities in the Kenya Air Trade chain are currently concentrated at the end of the chain,
because chain-link related activities yet cannot rely on control measure and risk management systems earlier
in the chain. For example, a high rate of inspections are necessary to establish assurance in this part of the
chain. In case adequate control measures are guaranteed and trusted in the early stages of the chain, hence
establishing chain-assurance, the number of inspections can be decreased. Therefore, chain assurance can
only be established by trustworthy collaboration.

Additional specific investments in risk management, control and security measures in the early stages of the
trade lane, will improve the total quality of control and assurance within the chain, and will lead to lower total
chain costs by cutting specific additional control measures, which eventually lead to increased chain efficiency
and faster/reliable throughput for the shipments.
Your opinion on Statement 2: Additional specific investments in risk management, control and security measures in the early stages of the trade lane, will improve the total quality of control and assurance within the chain, and will lead to lower total chain costs by cutting specific additional control measures, which eventually lead to increased chain efficiency.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
<td>Disagree</td>
<td>Neither</td>
<td>Agree</td>
<td>Strongly Agree</td>
</tr>
</tbody>
</table>

Comments:

If all chain participants embrace and communicate the same control and security policy fundamentals, the overall Kenya Chain can operate more efficient and effective, at lower costs.

To ensure that information security is integrated into the Kenya Air Trade Lane chain, it is important to show and communicate how information security can complement the key business and risk management process. A trusted trade lane can only be built on mutual trust to protect information and help manage information risk both now and in the future. If the chain aligns its information security policy, the Kenya chain overall will be better off.

Examples:

- Ensure that information security is integrated and communicated to chain participants.
- Deliver quality and value to the Kenya chain by guaranteeing that you comply to information security to your chain partners.
- Ensure to comply with relevant legal and regulatory requirements to your chain partners. By this, avoid criminal penalties for your organization and the other chain participants.
- Provide timely and accurate information on information security performance to your chain participants to enhance chain information risk management.
- Evaluate current and future information threats for your organization and inform your chain partners accordingly, so timely action can be taken within the chain to mitigate this risk.
- Promote continuous improvement in information security (culture), inform your chain partners accordingly, to improve the overall chain efficiency and effectiveness.

In the current situation in the Kenya chain we see no alignment of information security policy. This leads to redundant control measures within the chain - the same checks are done by more participants. If all chain participants comply to chain security policy and ensures this to the other chain partners, the overall chain can establish assurance while cutting double control measures.

Your opinion on Statement 3: If information security is formalized and communicated as a requirement at chain level, within the Kenya Trade Lane, the overall assurance and awareness levels in the chain can be established by relative lower total investments. Therefore, the overall chain risks can be decreased and lead to lower compliancy costs. Inspection levels.

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
<td>Disagree</td>
<td>Neither</td>
<td>Agree</td>
<td>Strongly Agree</td>
</tr>
</tbody>
</table>

Comments:
C.4. Statement 4: Risk-Control Measures

To a certain extent, in the Kenya Air Trade Chain, assurance and awareness can be established by responsible information security behaviour. This can be promoted by: (1) acting in a professional and ethical manner to ensure that information security-related activities are performed in a reliable, responsible and effective manner, and (2) to foster an information security-positive culture to provide a positive security influence on the behaviour of end users, reduce the likelihood of security incidents occurring, and limit their potential business impact.

In the current situation there is minor alignment, unawareness and no collective chain policy. This possibly resulted in the past in necessary (redundant) additional control measures, causing inefficiency within the chain.

**Your opinion on Statement 4:** In the Kenya Trade Lane chain some additional risk-control measures taken by your organization, which were necessary in the past can be cancelled, when your organization has assurance that proper risk-control measures are already taken elsewhere in the chain. This will lead to lower total costs by investments at the right places in the chain (and eventually a decreased chain throughput time).

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strongly Disagree</td>
<td>Disagree</td>
<td>Neither</td>
<td>Agree</td>
<td>Strongly Agree</td>
</tr>
</tbody>
</table>

**Comments:**


