Supply Chain Security Programs
Comparing TAPA FSR with ISPS

Farzam Garshasbi
Shahram Pasha Ebrahimi
6/2012
Supply chain security programs: Comparing TAPA FSR with ISPS

Farzam Garshasbi: X090191@student.hb.se
Shahram Pasha Ebrahimi: S093555@student.hb.se

Bachelor thesis

Subject Category: Technology

University College of Borås
School of Engineering
SE-501 90 BORÅS
Telephone +46 033 435 4640

Examiner: Bo Månsson
Supervisor’s name: Daniel Ekwall, PhD
Supervisor’s address: University College of Borås
School of Engineering
SE-501 90 BORÅS
Client: University College of Borås
Date: 26/06/2012
Keywords: TAPA FSR, ISPS, Transport Security, Supply Chain Security, Freight, Cargo
Acknowledgements

Special thanks go to the University of Borås and all the staff of engineering school by whose kind attention and assistance this thesis could be conducted, especially our supervisor Dr. Daniel Ekwall, who patiently directed us through the process.

We should like to thank our parents for their warm support during our studies. Also, we should like to thank dearest Dr. Duangporn Prasertsubpakij for her guidance on technical thesis writing.
Abstract

In this era, where international outsourcing and global distribution systems are thriving, providing the security of products in the logistic system is very crucial now. For corporates, it is highly vital to know how secure high-tech products and materials are handled, warehoused and transported as they move throughout the globe. Different international security standards have been introduced, two of which are TAPA FSR and ISPS. TAPA FSR (Freight Security Requirements) defines the smallest required security standards for goods travelling throughout the supply chain and the suitable approaches in keeping those standards. ISPS (International Ship and Port Facility Security) is another security standard which identifies the tasks of governments, shipping companies, shipboard personnel, and port/facility personnel to find security threats and take preemptive actions against security events influencing ships or port facilities used in global business. This research attempts to study the literature on security of transportation in supply chain. By comparing the requirements of TAPA FSR and ISPS, we aim to find their basic differences and to analyze to what extent the two standards respond to the crucial concepts of security in the supply chain.

Keywords: TAPA FSR, ISPS, Transport Security, Supply Chain Security, Freight, Cargo
## Contents

### Chapter 1: Introduction

1.1 Background of Study ................................................................. 1
1.2 Research Question .................................................................. 1
1.3 Research Objectives .................................................................. 1
1.4 Scope and Limitation of the Study ............................................. 1
1.5 Organization of Thesis .............................................................. 1

### Chapter 2: Frame of Reference

2.1 Components of transportation system ....................................... 4
2.2 Top vulnerabilities, disruptions and mistakes ........................... 4
   2.2.1 Top vulnerabilities ............................................................. 4
   2.2.2 Disruptions .................................................................... 4
   2.2.3 Freight transportation security mistakes ............................ 5
2.3 TQM: higher security with lower cost ...................................... 5
2.4 Resilience and its types .............................................................. 6
   2.4.1 Resilience in corporate organization ............................... 6
   2.4.2 Resilience in supply network design ............................... 7
   2.4.3 Features of a resilient system ......................................... 7
2.5 After 9/11: terrorist acts ............................................................. 7
2.6 TAPA FSR ............................................................................... 7
   2.6.1 Scope ........................................................................... 7
   2.6.2 Freight Security Requirements ....................................... 8
   2.6.3 Required documents ..................................................... 8
   2.6.4 Specifications ............................................................... 8
2.7 ISPS ...................................................................................... 10
   2.7.1 Scope ........................................................................... 10
   2.7.2 General requirements ................................................... 11
   2.7.3 Specifications ............................................................... 11

### Chapter 3: Methodology

3.1 Research Concept ................................................................... 13
3.2 Methodological Framework .................................................... 13
3.3 Detailed Methodology ............................................................. 14
   3.3.1 Formulating literature criteria for data assessment ............ 15
   3.3.2 Categorizing TAPA FSR and ISPS requirements according to five components of transportation system ................................. 15
   3.3.3 Analyzing TAPA FSR and ISPS requirements based on literature criteria ........................................................ 15
   3.3.4 Formulating analysis indicators ...................................... 15
3.4 Data Collection Design ............................................................. 15
   3.4.1 Data collection for formulating assessment criteria .......... 15
   3.4.2 Data collection for assessment indicators ...................... 15

### Chapter 4: Results

4.1 Comparison of basic requirements .......................................... 16
   4.1.1 Security level .................................................................. 16
   4.1.2 Security of ports and facilities ....................................... 16
   4.1.3 Access to facilities ......................................................... 19
   4.1.4 Handling of cargo ......................................................... 21
   4.1.5 Background check and employment termination ............ 21
4.2 Analysis of standards based on literature criteria ..................... 22
   4.2.1 Components of transportation system ......................... 22
4.2.2 Vulnerabilities .................................................................................................................. 25
4.2.3 TQM perspective .............................................................................................................. 26
4.2.4 Resilience ......................................................................................................................... 27
4.2.5 After 9/11 ......................................................................................................................... 28

Chapter 5: Discussion and conclusions .................................................................................. 29
5.1 Discussion ............................................................................................................................ 29
5.2 Conclusions .......................................................................................................................... 29

Appendix 1 TAPA FSR Requirements
Appendix 2 ISPS Requirements
Chapter 1: Introduction

1.1 Background of Study

In the modern world, where distances are becoming shorter, transportation of articles and goods throughout the globe has turned into a serious challenge for corporates and international organizations. One of the most important aspects in supply chain management is the security of transportation, especially following the aftermath of 9/11. Corporates are exposed to different transportation risks such as theft, organized crime, terrorist acts and so on. Dealing with these kinds of risk carries cost, which is moving counter to what businesses are seeking for. Therefore, corporates have been searching for measures to mitigate risks with lower costs. Moreover, suppliers, in order to be qualified to be selected by bigger firms, have also been looking for ways to improve the security of transporting their goods and to reduce the risks.

Furthermore, by reviewing the literature on the security of transportation, we have found that there are some crucial aspects in the security of goods in the supply chain. Chelsea C. et al (2004) define the main components of transportation where security measures need to be applied. In other words, it is vital to identify the types of security measures. In addition, the review of the literature illustrates that experts place special focus on the top vulnerabilities in the security of goods in the supply change. For example, Dan Purvell and James B. Rice, Jr. (2007) demonstrate that most corporates suffer from the top vulnerabilities in their logistics, which are lack of seals, lack of personnel background check and lack of collaboration with the partners in terms of the security of the goods. Accordingly, frequent mistakes and disruptions are vastly discussed in the literature on security in the supply chain. Yossi Sheffi (2008), for instance, illustrates the major disruptions and, Barry Brandman, the president of New Jersey-based Danbee Investigations, stresses out some security mistakes, which both will be elaborately discussed later in this paper. Moreover, the literature review shows that the corporate managements are concerned about the corresponding costs of security measures in their logistics (Barry Brandman, 2001). The other prominent concept in the literature concerns the practicality of the security measures and the possibility of their failure (Yossi Sheffi, James B. Rice, Jr., Jonathan M. Fleck, Federico Caniato, 2003). The corporates’ resilience, the level of their preparedness in case of potential failures, is considered as an important idea in the supply chain to avoid disruptions. Finally, the terrorist acts of September 11th have changed the type of approaching security of goods in the supply chain. The literature review indicates that security plans need to be reconsidered after 9/11 (Peter Kennedy, Charles Perrottet and Charles Thomas, 2003).

Accordingly, quit few security standards for transportation of freight have been established, two of which are TAPA FSR and ISPS. Transported Asset Protection Association (TAPA) is an association of security experts which has established freight security requirements (FSR). The International Ship and Port Facility Security (ISPS) Code is an amendment to the Safety of Life at Sea (SOLAS) Convention (1974/1988) about smallest security measures for ships, ports and government departments. It proposes tasks to governments, shipping companies, shipboard crew, and port/facility crew to "detect security threats and take preventative measures against security incidents affecting ships or port facilities used in international trade” (ISPS Code, Part A, 1.2.1). These standards identify particular requirements for different levels of security. Their application of surveillance and monitoring equipment, security guards and other security measures vary in intensity, frequency and quantity regarding different security levels.
One question for most corporates would be to know the differences between the requirements of ISPS and TAPA FSR. There are different levels of security with different measures to deal with security issues. Our study attempts to describe the requirements of TAPA FSR and ISPS for different security levels. We aim to compare the requirements to indicate the differences in applying the security measures such as surveillance and monitoring equipment.

Moreover, considering the differences among the requirements of the security standards, how the variations can be explained according to related logistics concepts in the literature. In other words, how do the differences between requirements of TAPA FSR and ISPS can be related to academic perspectives mentioned earlier? In this thesis, we also aim to analyze the requirements of TAPA FSR and ISPS based on the literature criteria.

By looking through the requirements of TAPA FSR and ISPS, it can be found that they differ in demanding security measures for the same area of security. For instance, they demand different requirements for the security of port and facilities. One problem in this thesis is to find the differences between the requirements of TAPA FSR and ISPS.

Moreover, according to the discussion above, it would be beneficial for corporates to know how the descriptions of the requirements of TAPA FSR and ISPS differ, especially when the security of transportation in logistics is concerned. In other words, why their requirements demand different measures for the same security issue?

1.2 Research Question

The main question in this thesis is to find the basic differences between the basic requirements of TAPA FSR and ISPS for various security levels.

1) What are the basic differences between the requirements of TAPA FSR and ISPS for different levels of security?

1.3 Research Objectives

The thesis has two objectives. Firstly, we attempt to review the literature on the security of transportation in supply chain, quality of security and requirements of TAPA FSR and ISPS. Secondly, we aim to compare and contrast basic requirements of TAPA FSR and ISPS. The last purpose of this thesis is to analyze TAPA FSR and ISPS requirements based on the literature criteria.

1) To review the literature on transportation security in supply chain
2) To compare TAPA FSR and ISPS descriptions of basic requirements
3) To analyze TAPA FSR and ISPS requirements based on literature criteria

1.4 Scope and Limitations of the Study

This thesis is based on a theoretical study on relevant concepts on security of transportation in the supply chain. The focus is on the ideas regarding quality in the supply chain.

This study focuses on two security standards namely TAPA FSR and ISPS. Their scopes and requirements are reviewed. The two standards are analyzed based on the literature criteria.

Furthermore, it is essential to note that there are limitations inherent in the study. There are different, even contrasting concepts about quality of transportation security in the literature.
This study only analyzes the standards based on the chosen concepts. The assessment cannot therefore be reliable according to other literature criteria.

Moreover, a comparative approach is applied to compare and contrast how TAPA FSR and ISPS differ in their requirements. The conclusions and the analysis indicators are for the sake of comparison between the two standards. They would not necessarily be reliable in general or in comparison with other standards.

In addition, we cannot make recommendations for corporates on choosing either of the standards since that argument cannot be supported within this research.

1.5 Organization of Thesis

This paper has three main parts: frame of reference, methodology and results. Firstly, the relevant concepts needed to analyze the standards are discussed in the frame of reference to create literature criteria. Secondly, the theoretical method is presented. In the next part, the two standards are compared and contrasted based on the argued concepts and their basic differences are indicated.
Chapter 2: Frame of Reference

In this section, relevant concepts to freight transportation security are reviewed so that an analysis can be made upon TAPA FSR and ISPS in terms of their requirements for the businesses. Therefore, the level of appropriateness of each standard for corporates with different security needs can be analyzed. In this part, crucial concepts about the security in the supply chain are reviewed. Firstly, the components of transportation system are described. Moreover, top vulnerabilities in the transportation of freight along with the most probable disruptions are discussed. In addition, the concept of resilience is introduced and the qualities of a resilient corporate are demonstrated. In the next part of the background, the cost of transportation security is reviewed from the perspective of TQM. What is more, the changes toward security after 9/11 and their impacts on security requirements are argued. Later, we will explain how the two security standards relate to the abovementioned concepts.

2.1 Components of transportation system

In order to be able to reduce the exposed risks of transportation and improve the security measures, we first need to identify the areas composing the transportation system of cargo. According to Chelsea C. et al (2004), the components of the transportation system of freight, which are exposed to the security risks, include:

- Physical structure: airports, seaports, distribution centers, roads, bridges, tunnels, plants, warehouses, pipelines and pipeline pumping stations.
- Information structure: communication structures for mobile resources, traffic operation bases
- Manpower: such as truck drivers
- Freight: containers, hazardous materials
- Means of transportation: trains, trucks (power units, trailers, chasses), ships, airplanes

Categorizing the transportation system of freight into the above categories allows us to better analyze the requirements of the two standards according to each category. For instance, corporates which have their focus on the security of their physical structure could decide whether TAPA FSR of ISPS would better suit their security needs.

2.2 Top vulnerabilities, disruptions and mistakes

2.2.1 Top vulnerabilities

In order to be able to analyze the two standards, it would be convenient to identify the most vulnerable areas in the security in supply chains. As Dan Purtell and James B. Rice, Jr. (2007) claimed in their study on “Assessing Cargo Supply Risk”, the most significant vulnerability for most corporates is how to manage container security inspection. Their study revealed that in most cases, the freight is delivered unsealed to the seaports. The other frequent weak spot in the freight supply risk, according to the study, is the lack of background check on the staff. In addition, Dan Purtell and James B. Rice, Jr. (2007) argue that most corporates do not provide any threat or security awareness trainings for their employees. Their study demonstrates that most business partners are absolutely clueless about whether their partners apply any security measures. We will analyze how the two standards handle these issues and how they differ in requirements regarding these vulnerabilities.
2.2.2 Disruptions
It would benefit corporates to be aware of the major disruptions in the supply chain so that the security risks can be mitigated through applying suitable security standards. Yossi Sheffi (2008) identified the major disruptions as below:

- Random incidents. These are natural events like floods, earthquakes, droughts, and so on.
- Accidents. Accidents are often the effect of many causes.
- Ignorance. This can include both non-compliance with regulations or standards and not managing the public impression regarding the social responsibility of the corporates.
- Deliberate disruptions. Terrorist attacks, corporate espionage and sabotage can be examples of this type of disruption.

2.2.3 Freight transportation security mistakes
To apply the security standards efficiently, it would be advantageous to know the major mistakes made by most corporates in terms of the security of the cargo transportation. In his interview conducted by Logistic Management, Barry Brandman, the president of New Jersey-based Danbee Investigations, which provides professional investigative, auditing, and security consulting services to numerous major corporates, counted three major security mistakes. Barry believes the first mistake is that the security assessments in most corporates are conducted by not experienced and professional people. This results in inefficacy in detecting vulnerabilities in the supply chain. The second mistake according to Barry is the conducting of security audit by means of checklists. He mentions 9/11 event as an example to justify the inadequacy of the checklist in finding the security risks and threats. The third mistake is the lack of improvement program for the security plans. Barry claims that most corporates fail to have a cycle of security plan so that the improvements can be made to fill the previous security holes.

Having considered the above vulnerabilities, mistakes and disruptions, we aim to analyze how TAPA FSR and ISPS differ in considering the mentioned pitfalls and what measures they require to prevent them.

2.3 TQM: higher security with lower cost
Although it is commonly thought that higher quality incurs costs, advocates of Total Quality Management (TQM) believe the opposite. Hau L. Lee and Seungjin Whang (2003) argue that improved quality does not necessarily need higher costs. They criticize screening as an inefficient and costly means to improve security of the freight. If screening improves the quality of the security, the more inspection will result in better quality. However, screening is expensive and it has the risk of type I and type II errors. Even if the 100 percent screening is applied, the result is based on the quality of the screening not on the quantity (Barry Brandman, 2001). Therefore, from TQM point of view, screening is not recommended as an efficient way to improve the security of freight transportation. Instead, a cycle of security plan is proposed, which is called Six-sigma Cycle (Hau L. Lee and Seungjin Whang, 2003). This cycle is composed of five steps:
1. Define: in this step, the security risks are defined and the ways to handle them are identified.
2. Measure: in this level, appropriate actions are taken to improve the quality of the security. It is important to map a visible and simple sketch of the security procedure so that all involved parties can follow.
3. Analyze: in this step, the root causes are identified by means of different risk assessment tools.
4. Improve: the results of the analysis are applied and communicated with staff so that the security quality will be in control.
5. Control: here the assignable causes (root causes) are eliminated or reduced.

We will also analyze TAPA FSR and ISPS regarding the above model. The aim is to indicate whether the TQM concept is present in the requirements of the two standards and if so, how the concept is applied.

2.4 Resilience and its types

In this section, the concept of resilience and its types are discussed. By reviewing the literature on supply chain security, it can be perceived that despite the application of security standards and measures, disruptions can occur (Yossi Sheffi, James B. Rice, Jr., Jonathan M. Fleck, Federico Caniato, 2003). Therefore, it is very critical for corporates to be capable of managing unexpected events. This ability to handle this kind of disruptions is called resilience. According to Yossi Sheffi et al (2003) following the results of interviews with different businesses, resilience can be established into two parts: resilience in corporate organization and resilience in supply network design.

2.4.1 Resilience in corporate organization

Corporates use contingency plans and special training programs for their staff to create resilience within their organizations (Yossi Sheffi et al, 2003). The contingency plans are prepared to projected possible accidents. They focus on the failure modes in the system. More modern contingency plans even foresee the disruptions in the whole supply chain system not only within the organization (Yossi Sheffi et al, 2003). However, having merely a written
description of future failure modes and the relevant procedures does not necessarily lead to resilience. The staff needs to be trained so that they would be capable of following the procedures in the needed times (Yossi Sheffi et al, 2003).

2.4.2 Resilience in supply network design
The probability of accidents in a network is greater than those within one corporate. However, a supply network can be actually more resilient since substitutions may happen in different nodes and connections in the network (Yossi Sheffi et al, 2003). According to Yossi Sheffi et al (2003) two principles can increase the resilience in supply network: redundancy and flexibility. Redundancy can be created by increasing the number of resources. However, redundancy obviously adds to the costs, which is not in favor of management in the supply chain. Flexibility is the degree of the corporate preparedness to response to the sudden volatilities in the supply network.

2.4.3 Features of a resilient system
Yossi Sheffi (2008) argues that for a system to be resilient and flexible, certain factors have to be considered:

- Constant interchange: resilient corporate have continuous communication inside their organization so that in case of a disruptions, everyone is aware of the status of the company.
- Decision power for everyone: allowing all staff regardless of their organizational position to take decisive actions in case of accidents would make the system more resilient.
- Employees’ commitment: corporates should inspire their staff about their mission so that they “go beyond their duty”.

By our analysis, it will be shown how TAPA FSR and ISPS establish resilience for the corporates.

2.5 After 9/11: terrorist acts
In general, the security risks have drastically changed after the terrorist act on September 11, 2001. The effects are significant and enormous. For instance, the airline industry actually faced lower revenues; the rise of military was evident; and the supply chains have been under the risk of disruptions (Peter Kennedy, Charles Perrottet and Charles Thomas, 2003). As a result, some believed that full inspection of all cargo was mandatory (Hau L. Lee and Seungjin Whang, 2003). However, this action is excessively costly. Moreover, apart from the labor costs- which are imposed to all parties in the supply chain- full inspection may cause the increase of lead times due to the high stop time (Hau L. Lee and Seungjin Whang, 2003). In the following parts, the two security standards, TAPA FSR and ISPS are discussed and later, an analysis is made to illustrate how these standards are related to the concepts argued in the background.

2.6 TAPA FSR

2.6.1 Scope\textsuperscript{9}
Transported Assets Protection Association (TAPA) was founded in Europe in May 1999 as a security institute to develop a set of standards and guidelines to help industries improve their security of their cargo against theft (Daniel Ekwall and Luca Urciuoli, 2009). This association not only provides security certificates but also holds programs such as conferences and
seminars to enable interactions amongst the members to enhance their ability to protect against theft (Daniel Ekwall and Luca Urciuoli, 2009).

2.6.2 Freight Security Requirements
One of the certifications of TAPA is Freight Security Requirements (FSR). FSR standards are established to protect the properties of the corporates in the in-transit storage and warehousing (TAPA FSR, 2011). According to FSR standards, suppliers are responsible for the security of assets during the transportation process. Suppliers should have written and substantiated ways to select their contractors. Suppliers must audit their contractors regularly based on the types of the risks. FSR are included in the contract between the suppliers and the corporates in order to clarify the responsibilities in case of theft.

2.6.3 Required documents
- TAPA FSR Certification Process Flowchart: this document illustrates the steps to be followed in order to obtain the certification.
- TAPA Pre-Certification Review Planning: this document shows the results of meeting held to decide whether the supplier enjoys the minimum security requirements.
- TAPA FSR Scoring Matrix: here the supplier is scored from 0.1 to 2.
- TAPA FSR Audit Form: Classifies the requirements into A, B or C and gives calculation for scoring.

2.6.4 Specifications
In this part, the FSR specifications are demonstrated based on the components of transportation discussed earlier. Firstly, FSR classifies the security levels into three levels called A, B and C.

- Security level A: high level of security
- Security level B: medium level of security
- Security level C: low level of security

FSRs are different for each level of security. For the sake of our analysis, the requirements are categorized into 5 categories namely physical structure, information structure, manpower, freight and means of transportation (See Appendix 1).

2.6.4.1 Physical Structure:
TAPA FSR defines sets of requirements regarding the security of infrastructure in its specifications. The related section are called Perimeter Security, Access Control – Office Areas, Facility Dock/Warehouse, and Security Systems each of which requires certain measures for three levels of security.

Perimeter Security: This section specifically defines requirements about fencing, CCTV systems, lighting, alarm detection and doors, windows and any other openings.

- Perimeter Fencing (including gates)
- CCTV Systems
- Lighting
- Perimeter alarm detection
- Perimeter windows, doors & other openings
Access Control-Office Areas: In this part, TAPA FSR identifies the requirements for monitoring the access to the physical infrastructures especially the offices. The requirements include:

- Visitor entry point(s) controlled.
- Employee entry point(s) controlled.
- Access control processes

Facility Dock/Warehouse: TAPA FSR requires special measures to secure the storage points. The required specifications are:

- Access control between office and dock/warehouse
- Limited access to dock areas
- High value storage area
- All external dock and warehouse doors secured
- CCTV coverage
- Motion detection alarms

Security Systems: This section defines the features of security hardware such as CCTV and alarm systems. Some more important requirements are listed below:

- Intruder alarm system:
  - Minimum of 60 day records on system alarms.
  - Restricted access to alarm system.
  - Alarms transmitted and monitored.
- CCTV system
  - All CCTV images are digitally-recorded.
  - Restricted access to CCTV system functions.
  - Minimum 30-day retention of all CCTV recordings.
- Electronic access control system
  - Minimum 60-day record of system transactions.
  - Restricted access to system functions.
  - Quarterly review of access reports.

2.6.4.2 Information structure:
TAPA FSR requirements related to the information structure component of transportation security are mentioned in the specifications section Security Procedures. The first subsection, Documented Security Procedures defines the requirements to secure the information structure.

2.6.4.3 Manpower:
TAPA FSR requirements on security issues regarding the employees are stated in the Security Procedures and in the subsections called Background checks (vetting) and Terminated employees & contractors procedure.

- Background checks (vetting): Criminal history check in place encompassing 5-year criminal history and employment check (vetting within constraints of local country laws).
- Terminated employees & contractors procedure
Termination procedures in place for employees and contractors, ensuring return of IDs, access cards, keys and other sensitive information.

- Procedure in place to prevent systems access to Buyer’s data by terminated employees.
- Records maintained to consider background of previously terminated personnel before re-hiring.

2.6.4.4 Freight:
Requirements regarding the measures to secure the freight in TAPA FSR can be found in the section Standard Truck Security Requirements under the subsection Loading/unloading. However, there are no other requirements on how to handle hazardous material.

2.6.4.5 Means of Transportation:
The main means of transportation in TAPA FSR is trucks. Therefore, there is a special section in the requirements regarding the security measures for trucks carrying cargo in the section called Standard Truck Security Requirements.

- **Cargo truck security**
  - Solid-top, hard-sided or reinforced soft-sided trailers with lockable cargo doors.
  - Tamper-evident security seals for trucks carrying Buyer-only shipments.
  - Vehicle immobilization devices utilized.
  - Two way communication present during entire journey and monitored by Supplier and/or contractor.
  - Written contingency plans in place for reporting unscheduled events (i.e. stops, delays, route deviation).
  - Truck cab and ignition keys secured from unauthorized use at all times.

- **Route Risk Assessment**
  - Risk assessments performed on Buyer-designated routes.

Furthermore, TAPA FSR has additional requirements for security of trucks under the section Enhanced Security Requirements.

- Truck escorts
- Vehicle tracking
- Driver training

2.7 ISPS

2.7.1 Scope
Due to the aftermath of terrorist acts on 9/11, the International Maritime Organization (IMO) established a new set of standards regarding the security of freight in seaports. International Ship and Port Facility Security (ISPS) was a supplement to Chapter XI of Safety of Life at Sea (SOLAS) which included the codes to maintain the maritime safety. After attaching of ISPS code in December 2002, the Chapter XI was renamed to Chapter XI-1 and new added security codes were included in Chapter XI-2. ISPS particularly applies to civilian ships and freight ships weighing 500 Gross Tonnage (GT) and more (Arsham Mazaheri and Daniel Ekwall, 2009). ISPS code includes one mandatory section (A) and a guideline to implement the security measures in part (B) (Arsham Mazaheri and Daniel Ekwall, 2009).
2.7.2 General requirements
ISPS demands measures to ensure the security of ship, ports and facilities. In general, the requirements for ships are:

- Development of ship security plan (SSPs)
- Hiring and training ship security officers (SSOs)
- Appointing and training company security officers (CSOs)
- Using proper security equipment on board

ISPS has general requirements about the security of ports as well:

- Establishing port facility security plans (PFSPs)
- Hiring and training port facility security officers (PFSOs)
- Using suitable security equipment

In addition, ISPS has other requirements to ensure the security of transportation in general:

- Continuous training of staff
- Running exercises and drills
- Control and surveillance of access to the ship or port
- Controlling people activities and freight
- Prepared security communications

2.7.3 Specifications
ISPS code divided the security into three levels: normal, heightened, and exceptional.

- Security Level 1 normal: in this level, ships and facilities operate normally.
- Security Level 2 heightened: this level applied the cases where there is a possible chance of security risks.
- Security Level 3 exceptional: in this level, security risks are probable and impendent.

As discussed earlier, we divide the ISPS security requirements into different categories according to the components of freight transportation security (See Appendix 2).

2.7.3.1 Physical structure:
ISPS requirements regarding the security of physical infrastructures can be found under section Monitoring the Security of the Ship. The requirements differ according to the level of security. The ISPS requirements are rather descriptive and qualitative. They describe what measures need to be taken, but they do not require the exact quantity of for example CCTVs. Some of the requirements on the security of ships are listed below:

- Lighting
- watch keepers
- security guards
- security and surveillance equipment

ISPS describes how the above measures have to be done in different levels of security.

2.7.3.2 Information structure:
Under the section of requirements Delivery of ship’s stores, ISPS defines security measures
regarding the information component of transportation security. Certain requirements are as following:

- checking to ensure stores match the order prior to being loaded on board
- ensuring immediate secure stowage of ship’s stores

2.7.3.3 Manpower:
ISPS does require background check of the personnel. It has focus on restricting the access of people to ship under the section *Access to the ship.*

- checking the identity of all persons seeking to board the ship
- ensure that vehicles destined to be loaded on board car carriers and other passenger ships are subjected to search prior to loading

2.7.3.4 Freight requirements:
ISPS states special requirements in the section *Handling of cargo* regarding the security of freight.

- checking of seals or other methods used to prevent tampering
- checks to ensure that cargo being loaded matches the cargo documentation
- ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening

2.7.3.5 Means of transportation:
The major means of transportation in ISPS is ships and almost all security requirements regarding the means of transportation concern the security of ship. Most of these requirements overlap with the physical infrastructure requirements, since ships are considered as perimeters in ISPS.

- surveillance equipment capable of recording activities on, or in the vicinity of, the ship
- preparation for underwater inspection of the hull of the ship

We will use the above data (also see Appendixes 1 & 2) to analyze how TAPA FSR and ISPS requirements respond to literature criteria. In the next part, the approach by which we have conducted our analysis is explained.
Chapter 3: Methodology

This chapter describes the mechanisms of developing the study. Research concept, methodological framework, selection of study area and method of data collection are explained. These parts are discussed in order to achieve the objectives of the study which have been previously proposed.

3.1 Research Concept

In order to compare and contrast TAPA FSR and ISPS requirements, this research analyses the standards based on the literature criteria. Different concepts regarding the security of transportation in supply chain are discussed so that the requirements of the two standards can be analyzed in a comparative approach to illustrate the basic differences between the requirements of TAPA FSRS and ISPS. The discussed concepts include:

- Components of transportation system:
  This study demonstrates in what areas of transportation the security measures need to be applied. Therefore, by comparing TAPA FSR and ISPS requirements, the study aims to assess how the standards deal with the security in different areas in transportation.

- Top vulnerabilities, disruptions and mistakes:
  Through describing the major mistakes and weak spots regarding the security of transportation in supply chain, we aim to assess TAPA FSR and ISPS requirements based on the extent to which they prevent these vulnerabilities.

- TQM: higher security with lower cost:
  Traditionally, improving the security may incur additional costs in the supply chain. However, according to the advocates of Total Quality Management, it can be possible to increase the quality of security with lower costs by applying the Six Sigma cycle. Our study, through comparing TAPA FSR and ISPS requirements based on the criteria, demonstrates the level of their appropriateness to the concepts of TQM in order to enhance security of transportation, yet at lower costs.

- Resilience and its types:
  Despite the provisions of security standards and measures, accidents and unexpected disruptions can occur. The crucial factor to prevent disruptions in the supply chain despite the occurrence of accidents is the corporates’ resilience, the level of preparedness in case of emergency. Comparing TAPA FSR and ISPS requirements based on these literature criteria illustrates to what extent they contribute to the resilience of the corporates and supply chains.

- After 9/11: terrorist acts:
  The terrorist acts on 9/11 have drastically altered the perspective towards security especially the security of global transportation. It is, consequentially, vital to change and modify the already used standards in order to prevent disruption in the supply chain. Hence, we aim to analyse how TAPA FSR and ISPS requirements deal with security needs in the aftermath of 9/11.
3.2 Methodological Framework

In order to achieve our objectives and the methodological concepts, the methodological framework is created to suitably explain the major tasks in this study (See Figure 2). First, the literature on transportation security in supply chain is reviewed. Second, the requirements of TAPA FSR and ISPS are studied. Third, TAPA FSR and ISPS are assessed based on the literature criteria. Finally, a conclusion is formulated to recommend the applications of TAPA FSR and ISPS for corporates with different security needs.

![Methodological Framework Diagram]

Figure 2 Methodological Framework
3.3 Detailed Methodology

This section demonstrates how we achieved our objectives in three parts.

3.3.1 Formulating literature criteria for data assessment

Literature on five areas of transportation security was reviewed. These areas were namely components of transportation, top vulnerabilities, disruptions and mistakes, TQM: higher security with lower cost, resilience and its types, and after 9/11 terrorist acts. The purpose of reviewing these areas is to create an assessment framework so that TAPA FSR and ISPS requirements can be analysed upon this literature criteria.

3.3.2 Categorizing TAPA FSR and ISPS requirements according to five components of transportation system

In order to be able to assess the requirements based on the literature criteria, the requirements of the two standards are classified into five categories based on the components of transportation system. These categories include:

- Means of transportation
- The information structure
- Manpower
- Freight
- Physical structure

The requirements, therefore, are arranged in accordance with the above components and they can be assessed more appropriately (See appendixes 1 & 2).

3.3.3 Analyzing TAPA FSR and ISPS requirements based on literature criteria

In this phase, the extent to which the requirements of TAPA FSR and ISPS relate to the literature criteria is assessed. Through assessing the level of correspondence between the requirements of TAPA FSR and ISPS and literature criteria, we analyse how strongly the requirements respond to concepts in the literature review.

3.3.4 Formulating analysis indicators

In order to do the assessment, assessing indicators are created to illustrate the level of appropriateness of the requirements of TAPA FSR and ISPS for each concept of literature criteria. To indicate the level, qualitative attributes are used. The attributes include: Strongly, Fairly, Slightly, and Weakly. These qualitative attributes indicate the extent to which the requirements of TAPA FSR and ISPS respond to the literature criteria.

3.4 Data Collection Design

The data needed for achieving the objectives of this thesis was collected in two ways.

3.4.1 Data collection for formulating assessment criteria

The data for the creation of literature criteria for assessing the requirements of TAPA FSR and ISPS was collected by reviewing the literature on transportation security in supply chain.

3.4.2 Data collection for assessment indicators

To indicate the level of TAPA FSR and ISPS correspondence with the literature criteria, the relevant data was collected by reviewing the latest official documents of the two standards published by their authorities.
Chapter 4: Results

In this part, the aim is to compare and contrast the two security standards-TAPAFSR and ISPS- according to the concepts argued the in the literature review. The purpose is to find how TAPAFSR and ISPS requirements differ regarding dealing with the different concepts in security of transportation as discussed above. The findings will illustrate the appropriateness of each standard for different security needs. We use assessment indicators to show how strongly the requirements of TAPAFSR and ISPS correspond with the literature criteria. Our analysis part has two major parts. In the first part, we compare and contrast some requirements of TAPAFSR and ISPS in particular. The aim is to demonstrate how the descriptions of the requirements differ. In the second part, we analyze the standards according to the literature criteria in general. We aim to assess TAPAFSR and ISPS requirements based on the related concepts in logistics.

4.1 Comparison of basic requirements

To start comparing the two standards, we select certain common areas in the descriptions of TAPAFSR and ISPS requirements. In the following part, it will be demonstrated how TAPAFSR and ISPS requirements differ in the common areas.

4.1.1 Security level

Both standards identify three security levels so that appropriate level of security measures should be applied.

TAPAFSR: It defines three levels of security namely A (high), B (medium), and C (low).

ISPS: It identifies the security levels as 1 (normal), 2 (heightened), and 3 (exceptional).

In this thesis, we aim to analyze the security requirements based on the security levels. For example, we seek to find the differences between the basic requirements of TAPAFSR and ISPS for each security level separately. Therefore, for the sake of this analysis, we have linked TAPAFSR security level A to ISPS security level 3, B to 2 and C to 1. Although their descriptions of the security levels may not be necessarily equivalent, the linkage is applied for the convenience of comparative analysis of description of basic security requirements of TAPAFSR and ISPS.

4.1.2 Security of ports and facilities

Requirements of ensuring the security of ports are one of the main parts in both TAPAFSR and ISPS. However, they seem to have different requirements to establish the security of ports. We describe their requirements below to indicate the difference between TAPAFSR and ISPS in this regard.

Normal Security level (C or 1)

TAPAFSR:

For low level of security (as it can be seen from Appendix 1), TAPAFSR requires CCTV coverage of all external dock area. It also requires sufficient lighting both exterior and interior for having high quality of CCTV images and recording. In addition, TAPAFSR requires alarm system for all facility external doors to alert unauthorized entering. The alarm must be connected to the main alarm system. In general, for the security level C regarding the security of ports and facilities, TAPAFSR requires CCTV, lighting and alarm system.
ISPS:

According to the guideline in Part B of ISPS Code (see Appendix 2), to maintain the security of ports at security level 1, security and surveillance equipment must be used. The requirement for using security equipment is general and the details about types, quantity and quality of them are not described. Moreover, ISPS requires lighting to ensure the visibility at ports. Furthermore, it requires using human force such as watch keepers and security guards to keep the ports and facilities safe at normal security level.

As it can be seen from comparing the requirements of the two standards for normal security level, the main difference is using of human surveillance such as watch keepers and guards in ISPS. Unlike ISPS, there are no requirements about security guards in TAPA FSR for normal security level. Moreover, TAPA FSR explicitly mentions what kind of security equipment to use. For instance, TAPA FSR requires using CCTVs for external dock areas. It also requires high quality of images of CCTV by providing appropriate lighting. However, the description of requirements for surveillance equipment is open to interpretation in ISPS.

Medium security level (B or 2)

TAPA FSR:

Some of the requirements for this level of security overlap with ones in level C. TAPA FSR has additional requirements to maintain the security of ports in security level B. The maximum lighting must be used around the loading/unloading areas. In addition, TAPA FSR requires reinforcing the exit doors from warehouse through installing steel doors and frames or any other proper options. Moreover, the exterior walls and roof must be resistant against penetration, that is, the building fabric cannot be removed, cut or rammed by vehicles. Therefore, TAPA FSR additional requirements for security level B regarding security of ports and facilities are flood lighting, reinforcing of doors and walls.

ISPS:

For security level 2 regarding the security of ports and facilities, ISPS requires additional measures to level 1. Firstly, ISPS requires the intensifying the level of lighting for more visibility. It also demands to use greater amount of security and surveillance equipment. Finally, the number of security guards needs to be increased in medium heightened security level. ISPS, therefore, requires more lighting, surveillance equipment and security guards for preventing disruptions in security level 2 regarding the security of ports and facilities.

Following the explained trend, TAPA FSR focuses on the security equipment to increase the security for this level, whereas ISPS requires more patrol and guards in addition to proper use of security and surveillance equipment.

High security level (A or 3)

TAPA FSR:

In addition to requirements for levels C and B, the following measures have to be applied for high level of security. TAPA FSR requires installing CCTVs to cover the external parts of shipping and receiving yard and entry/exit points. These CCTVs must record the movement of vehicles and individuals. The windows and doors of the warehouses must be equipped with reinforcing measures and physical barriers to prevent and delay forced opening through using
portable hand tools or ramming by vehicles. Hence, TAPA FSR special requirements for the light security level regarding the security of ports and facilities are additional CCTVs and physical barriers.

**ISPS:**

Besides the measures for levels 1 and 2, the following requirements have to be fulfilled for security level 3. ISPS requires that all lightings must be switched on. In addition, all security equipment capable of recording must be turned on at maximum recording capacities.

In the exceptional level of security, TAPA FSR requires more preemptive measures for this security level such as stronger dock doors and windows. On the other hand, ISPS requires more surveillance equipment especially those which can record.

**Comparison results:**

In general, by considering the requirements for all levels of security, the main difference between TAPA FSR and ISPS regarding the security of ports and facilities is in using manpower for security. TAPA FSR does not require guards to patrol in vicinity of the port, whereas ISPS requires them even in the normal security level.

There are advantages and disadvantages of using guards based on the literature criteria. First of all, since accidents and unexpected event can always occur, merely using security equipment might not guarantee prevention of disruptions. Therefore, using manpower in addition to security equipment to establish the security of ports may result in more resilience and hence, fewer disruptions. Moreover, ISPS requires continuous training and running of drills for the manpower so that they would be prepared for emergent situations, which-as discussed earlier- increase the resilience of the corporates in their logistics. Further, as far as the terrorist acts and organized crime are concerned, ISPS requirements, especially using guards, may seem more appropriate to avoid disruptions in that sense.

On the other hand, according to TQM, using additional security measures such as guards may incur costs. As stated in the frame of reference, the quality of security is the key to avoid disruptions. Therefore, solely using guards might not prevent disruptions, but the quality of their effectiveness. The success factor for the effectiveness of using security guards depends on to what extent they are trained and prepared to act and pro-act in the case of emergencies.
4.1.3 Access to facilities
In this part, we compare the requirements of TAPA FSR and ISPS about monitoring and restricting the access to facilities in three different levels of security.

Normal Security level (C or 1)

TAPA FSR:
The requirements for the normal security level to control the access to facilities can be categorized into three parts: control of human access, monitoring of the stores assets on-site, and monitoring of docks.

The requirements demand controlling of access to facilities both during and outside the working hours. Only authorized supplier staff and visitors must be allowed inside. Moreover, in case they should enter the warehouse, escorting is required.

Regarding the securing the access to assets staged on-site for more than 6 hours, TAPA FSR requires high-grade security mesh, chain link or hard walls. In addition, CCTVs must be installed on the top roof to monitor the access.

To ensure the restriction of access to facilities, TAPA FSR also requires CCTVs to monitor internal dock doors and dock areas.

ISPS:
For low level of security of access to facilities, ISPS requires measures as the following.

For the facilities to be secure, the access points must be locked and monitored. ISPS requires surveillance equipment including CCTVs to control the areas.

Besides the surveillance equipment, ISPS requires using of guards or patrols to control the access to the facilities.

ISPS also demands automatic intrusion detection devices in order to alert when unauthorized access occurs.

Medium Security level (B or 2)

TAPA FSR:
In security level B, TAPA FSR requirements to secure the access to facilities significantly increase compared to normal security level.

Firstly, the entry points both for visitors and employees must be controlled. The monitoring should be implemented by using guards, card access and CCTVs with intercom.

In addition, the buyer-designated assets in the supplier facility must be under 100% CCTV surveillance. TAPA FSR does not require full floor coverage; instead it requires full CCTV coverage of buyer’s assets from dock to pallet breakdown/buildup areas and to high-value cage/vault.
Furthermore, motion detection alarms must be installed inside warehouses so that the malfunctioning of the warehouse operational processes can be detected.

**ISPS:**

There are not many additional requirements for the medium level of security for the access to facilities.

ISPS focuses on the intensity of controlling measures. For example, it requires assigning more staff to patrol deck areas during silent hours to prevent unauthorized access.

Moreover, ISPS requires decreasing the number of access points to the facilities so that the intensity of security measures increases.

In the security level 2, additional specific security briefings must be provided for the entire staff about the potential threats. During these sessions, the security measures and procedures must be re-emphasized.

**High Security level (A or 3)**

**TAPA FSR:**

The requirements for the security level A do not differ significantly with those for the security level B. However, TAPA FSR requires that access to assets staged on-site for more than 2 hours (in security level B, for more than 6 hours) must be restricted by high-grade security mesh, chain links or hard walls as well as CCTVs on top roofs.

**ISPS:**

For heightened level of security, ISPS stresses on greater intensity of the security measures defined the previous parts, especially the restriction of access only to those responding to the security events.

**Comparison results:**

By comparing the requirements of TAPA FSR and ISPS regarding the security of access to facilities in three security levels, it can be seen that ISPS requirements of surveillance, patrolling and blocking seem almost the same for all security levels. They differ in the intensity and frequency. For instance, using security guards are mandatory for all security levels, but the number of guards and the frequency of patrolling change according to the level of security.

On the other hand, TAPA FSR requirements significantly differ for the levels of security, especially for levels A and B compared to level C. For example, in normal security level, no unauthorized access detection alarm systems are required (whereas ISPS requires that for all security levels). TAPA FSR requires detection alarm system for security levels B and A.

To sum up, TAPA FSR requirements for normal security level seem less demanding compared to those of ISPS, especially in using guards and unauthorized access detection alarm systems.
4.1.4 Handling of cargo

In the following section the requirements of TAPA FSR and ISPS regarding the handling of cargo will be described.

TAPA FSR:

The requirements for handling of cargo are similar for all security levels. TAPA FSR especially focuses on three areas. Firstly, the trailers carrying the cargo must be solid-top, hard-sided or reinforced soft-sided with lockable doors to avoid tampering and theft. Secondly, the trucks have to be equipped with vehicle immobilization devices in all security levels. Finally, TAPA FSR requires written contingency plans for reporting unexpected incidents such as stops, delays and route deviations.

ISPS:

Similarly, ISPS has the same requirements for the three levels of security. In addition to measures to ensure the accuracy of loading the right cargo on board, ISPS requires 100% screening and searching up of the unaccompanied baggage. It requires X-ray screening for this kind of cargo.

Comparison results:

As illustrated above, X-ray screening required by ISPS can be considered as its most significant difference with TAPA FSR regarding the measures for handling the cargo.

4.1.5 Background check and employment termination

In this section, we aim to compare and contrast the requirements of TAPA FSR and ISPS about the security issues regarding the employees and the personnel.

TAPA FSR:

The requirements of TAPA FSR about the security issues regarding the staff concern two aspects: the background check and the security issues after the termination of employment.

The background check requirements demand two types of employees’ records. The first one is the criminal history check of the past five years. The other history check relates to the employment check. That means TAPA FSR requires checking of deviations occurred during the employment, which are not generally considered as crime. For instance, over speeding can be found in the employment history check but not in the criminal record.

Moreover, TAPA FSR requires special termination procedure for employees and contractors. It is crucial that IDs, access cards, keys and other sensitive information are returned after the employment termination.

In addition, TAPA FSR demands that terminated employees must not have access to buyer’s data.

Furthermore, in case employees should be rehired, the employment records must be kept for future background checks.
ISPS:

Neither in Mandatory Part A nor in the guidelines in Part B does ISPS Code describe clear requirements about background checks.

Comparison results:

As described earlier, background checks are important part of security in transportation and accordingly, appropriate measures must be applied to reduce corporates’ vulnerability of this matter and increase their resilience. By reviewing TAPA FSR requirements in this regard, it can be seen that two specific phases are described to reduce the vulnerability of corporates from their staff. Both criminal and employment histories must be checked. It also requires special procedures for the terminated staff to prevent unauthorized access to facilities and data. On the other hand, ISPS does not specify clear parts regarding the background check of employees.

4.2 Analysis of standards based on literature criteria

In this part of our analysis, we scrutinize the two standards based on the literature criteria. In the frame of reference, five general concepts about the security of transportation were discussed namely components of transportation system, top vulnerabilities, Total Quality Management, resilience and the aftermath of 9/11. In the following part, we compare and contrast TAPA FSR and ISPS by analyzing to what extent they relate to the literature criteria.

4.2.1 Components of transportation system

In the following part, TAPA FSR and ISPS requirements will be analyzed based on the five components of transportation system in order to indicate their differences in responding to the security measures described for each component according to the literature review.

TAPA FSR:

As discussed earlier, the risks in security of transportation of freight can be traced into five categories of physical structure, information structure, manpower, freight and means of transport for each of which different security measures need to be developed to mitigate the risks. The Freight Security Requirements are actually divided in a way to address the security risks in different components (See Appendix 1). For instance, FSR has a part called “Premier Security” which defines different requirements for different levels of security. This part refers to establishing security measures for physical structure. Moreover, FSR specifies “Documented Security Procedures” to respond to information structure requirements. To cover the manpower requirements, FSR defines certain measures in “Background Check” and “Terminated Employees and Contractors Procedure”. FSR has also a specific category of requirements to ensure the security of cargo truck. However, there are not any specific requirements regarding the materials. In other words, FSR does not require particular measures how to handle hazardous materials.

Therefore, the analysis of TAPA FSR requirements (See Appendix 1) on to what extent they cover the security of the components of transportation reveal that TAPA FSR strongly covers physical structure component security by establishing a wide range of related requirements. There are additional security measures for the physical security according to the level of security. For instance, in Security Level A, in case the assets must be on site for more than
two hours, TAPA FSR requires restricted access with protected surroundings with walls or chains and CCTV on roof and walls.

Regarding the information structure, TAPA FSR fairly secures this area. There are some requirements for this purpose, but not to a great extent. In general the requirements guarantee the availability of information in the need time, but there are not specific procedures to prevent the theft of information in actions like cyber-attacks.

In addition to criminal record, TAPA FSR requires employment check of the personnel within the past five years. The later reveals more about the staff since some potential dangerous behaviors are not generally recorded in the criminal records such as over speeding of a truck driver and such. TAPA FSR fairly covers to require security measures to fully insure this component.

TAPA FSR requires “solid-top, hard-sided or reinforced soft-sided trailers with lockable cargo doors and tamper-evident security seals for trucks carrying Buyer-only shipments to provide the security of cargo component of security of transportation. It also requires training and contingency plans. However, we could not find specific requirements for procedures of handling the materials especially hazardous materials. However, there are requirements about the loading/unloading security. It could be seen that TAPA FSR fairly covers the requirements for the security of this component.

For the security of means of transportation, TAPA FSR requires special measures only for Security Level A. It demands escorting of the truck and installation of GPS device on the trucks carrying the Buyer’s asset to make the tracking possible. Regarding the requirements, TAPA FSR strongly complies to cover this component of transportation security.

Figure 3 summarizes how TAPA FSR relates to the components of transportation security. The assessment indicators have been established by categorizing FSR requirements into the five categories of components and analyzing to what extent they cover the areas. The indicators would make sense when compared to those of ISPS. By saying TAPA FSR strongly covers the requirements for one given component, we mean in comparison with ISPS, not in general.

<table>
<thead>
<tr>
<th>TAPA FSR</th>
<th>Components of transportation</th>
<th>Strongly</th>
<th>fairly</th>
<th>slightly</th>
<th>weakly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information structure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Manpower</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cargo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Means of transportation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 3 Level of compliance with the transportation components

ISPS:
In this part we analyze how ISPS requirements cover the five components of transportation security. To address physical structure security, ISPS has established different measures for different levels of security. For example, in one part of requirements namely “Monitoring the security of the ship”, various measures are defined to ensure the security of the ship (See
Appendix 2). ISPS has also identified requirements regarding the information structure security in the part called “Delivery of ship’s stores” (See Appendix 2). To cover the next transportation component-manpower- ISPS requires checking of people having access to the ship and different areas. However, there are no specific requirements about background check of the staff. ISPS, on the other hand, elaborately defines the requirements for handling the cargo. ISPS requires checking the sealing of the freight.

Regarding the first component of transportation, physical structure, ISPS, compared to TAPA FSR, strongly requires measures for the security of ports, warehouses and such. The major difference between ISPS and TAPA FSR in this area is that ISPS more focuses on patrolling and surveillance. TAPA FSR, on the other hand, focuses on preemptive security measures such as locks, sealing and CCTVs. ISPS, in its Security Level 3, requires underwater search around the ship to prevent possible attacks.

About the next component, information structure, ISPS does not list very strong requirements (compared to TAPA FSR). There are typical requirements to secure the loading and loading of the right goods and articles.

ISPS defines requirements for restricting the personnel to some areas and demands the recording of the traffic of people. However, ISPS does focus on background check, be it criminal or employment. Compared to TAPA FSR, which not only requires background check prior to employment but also demands following checkups after the contract termination of staff, ISPS slightly covers the manpower component of transportation security.

ISPS, in addition to defining requirements for security of cargo against theft and tampering by means of locks and seals, it demands detailed procedures how to handle cargo especially hazardous materials. In the later sense, ISPS seem to have stronger requirements to cover the cargo component of transportation security compared to TAPA FSR.

ISPS requirements regarding the means of transportation are mostly about ship, whereas in TAPA FSR, the main means of transportation is truck. ISPS requires extreme measures to provide the security of ship by mentoring and restricting the access to the ship as well as by patrolling inside, outside and even underwater surroundings of the ship.

Figure 4 indicates how ISPS relates to the components of transportation security. The assessment indicators have been established by categorizing ISPS requirements into the five categories of components and analyzing to what extent they cover the areas. The indicators would make sense when compared to those of TAPA FSR. By saying ISPS strongly covers the requirements for one given component, we mean in comparison with TAPA FSR, not in general.
4.2.2 Vulnerabilities

In the next step, we aim to analyze the description of the requirements with regards to the top vulnerabilities explained in the frame of reference.

TAPA FSR:
We argued earlier that the most vulnerable part in security of cargo transportation is the security of containers, especially the sealing of the cargo. Most of cargo is delivered unsealed. TAPA FSR, however, has not established certain measures to deal with this type of vulnerability. TAPA FSR requires trucks carrying the cargo to be sealed (See Appendix 1), but there are no requirements for the sealing of the cargo itself.

The other vulnerability discussed earlier is the lack of background check. TAPA FSR specifically requires background check of the staff for all the three levels of security. It demands a 5-year criminal record check (See Appendix 1). Moreover, apart from the criminal record, TAPA FSR requires the employment record check. The later, dramatically reduces the security risks of manpower since quit few manpower abnormalities are not included in the criminal record; for instance, over speeding of a truck driver.

The other area where most corporates are vulnerable at is the lack of training for the employees so that they would be prepared for possible security actions. TAPA FSR explicitly requires training for truck drivers on how to act in case of robbery and theft (See Appendix 1).

Figure 5 shows how TAPA FSR deals with the three top vulnerabilities. This matrix is made by analyzing the TAPA FSR requirements to figure out how they prevent the three areas. The assessment indicators (strongly, fairly, slightly and weakly) make sense when TAPA FSR requirements are compared with those of ISPS. They do not necessarily be reliable in general or in comparison with other standards.

<table>
<thead>
<tr>
<th>TAPA FSR</th>
<th>Strongly</th>
<th>fairly</th>
<th>slightly</th>
<th>weakly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Checking of the seals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Background check</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training of staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ISPS:
To deal with the first type of vulnerability mentioned above, ISPS explicitly defines requirements to check sealing of the cargo or to apply other methods to prevent tampering. ISPS requirements for security of cargo seem elaborate and complete. There are also some
other supplementary requirements in addition to the sealing of the cargo to ensure the prevention of tampering. For example, routine checking of cargo prior, during and after is required by ISPS. In this sense, ISPS requirements seem stronger than those of TAPA FSR to deal with the first vulnerability- checking of the seals. Background check, the other frequent vulnerability, does not seem to be intensified in ISPS. There are, however, measures to check the people who have access to the cargo and ship. Nevertheless, according to the requirements of ISPS, checking the criminal record and employment record is not perceived to be of that significance, whereas in TAPA FSR specific requirements are defined both prior to employment and after termination of contract or employment. ISPS has a special section of requirements in its mandatory part A, "Training, drills and exercises on ship security," which demands training of the staff, especially the ship crew about the procures in case of unexpected events. As argued earlier, experts believe that the security assessments and quality controls are not done by experienced people. ISPS exactly requires that the skilled and experienced employees have to assessment. ISPS, in comparison with TAPA FSR, identifies more detailed requirements for the training of staff about the security of transportation.

Figure 6 presents how ISPS respond to the three top vulnerabilities. This matrix is made by analyzing the ISPS requirements to find how they prevent the three areas. The assessment indicators (strongly, fairly, slightly and weakly) make sense when ISPS requirements are compared with those of TAPA FSR. They do not necessarily be reliable in general or in comparison with other standards.

<table>
<thead>
<tr>
<th>ISPS</th>
<th>Vulnerabilities</th>
<th>Strongly</th>
<th>fairly</th>
<th>slightly</th>
<th>weakly</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Checking of the seals</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Background check</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training of staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 6 The extent to which the top vulnerabilities are covered

4.2.3 TQM perspective

The following section scrutinizes the requirements of TAPA FSR and ISPS according to quality concepts about security of transportation especially based on TQM perspective.

TAPA FSR:

From the viewpoint of advocates of TQM argued above, it is actually possible to increase the quality of security at lower costs through applying the Six-Sigma Cycle. TAPA FSR, however, aims to prevent security risks by focusing on screening and monitoring. This kind of requirements may result in type I and type II errors because the critical point is that how the screening and the auditing are implemented, i.e., the quality of the security measures is more important than the quantity. In addition, TAPA FSR does not lead to the elimination of the mistakes and errors in the earlier stages. According to TQM principles, root causes of the problems in the security have to be detected and reduced or eliminated. TAPA SFR merely provides a comprehensive checklist of security provisions. There are not specific requirements to lead in removing of the security errors so that the process of the security of transportation will be under control at lower costs, which is meant by TQM. The elimination of the assignable causes may reduce the costs through reducing waste and ultimately increase the quality. TAPA FSR does not require this cycle according to the concepts of TQM discussed earlier.
ISPS:
Unlike TAPA FSR, checklists of security measures are not provided by ISPS. Instead, there are certain mandatory requirements and a guideline to implement them. Therefore, ISPS seem to focus more on the quality of the security procedures than on the quantity of them. According to TQM concepts about the inefficiency of merely focusing on the monitoring and inspection due to creation of type I and types II errors, we can see that ISPS requirements are not in the checklist format instead the quality of the inspections are stressed, which can increase the quality of security at lower costs. Moreover, ISPS requires skilled and experienced staff to implement the assessment and security check, which implies the stress on quality. This approach, according to TQM, may increase the quality of security while at lower costs. By comparing ISPS requirements with those of TAPA FSR, it can be perceived that ISPS requirements are more compatible with the quality concepts such as TQM or Lean due to the more qualitative requirements than quantitative ones like checklists.

4.2.4 Resilience
Below is our analysis of the description of the requirements from the viewpoint of resilience and stability.

TAPA FSR:
Resilience is the level of corporates preparedness when unexpected events occur. We mentioned that resilience can be established in two forms: resilience in the corporate organization and resilience in the supply chain network design. For corporates to be resilient within inside, they need to have training programs for their employees on how to act and react in case of unexpected events. TAPA FSR requires training for the truck drivers. In the “Documented Procedure”, it demands security awareness training (See Appendix 1). It can, therefore, be seen that TAPA FSR can provide resilience in the organization as a result of mandatory training programs for the staff. Therefore, TAPA FSR would establish a resilient corporate within inside due to devising training procedures for the staff so that they know what to do in case of accidents and ultimately avoid disruption. However, there are requirements for the training but they do not necessarily guarantee whether the staff will be prepared for the emergencies because there are not requirements for practices or exercises. Furthermore, most corporates are part of a supply chain network. That means a disruption for a supplier leads to the distribution of the stop in the network. So, interactive collaboration is needed to establish resilience in the supply chain network design. TAPA FSR has not formed any requirements for the supplier-buyer collaboration. Therefore, applying TAPA FSR does not seem to bring about resilience in the network because of the lack of requirements to engage the security processes of the involved parties. Not collaborating with the other involved parties may result in disruptions the supply chain.

ISPS:
Regarding the resilience within the organization, ISPS has gone beyond training of the staff. It also requires drills and exercises of the security measures to ensure that the employees are actually ready and prepared to act in case of unexpected events. Compared to TAPA FSR, ISPS seem to focus more on the resilience of the organization. The requirements oblige the corporates not only to train their staff but also examine their actual level of preparedness through running exercises and drills.
Again, it seems that ISPS does not require collaboration amongst the parties involved in the supply chain sharing the risks either. The lack of requirements for collaboration between the parties may result in disruptions since the supply network may not be resilient.

4.2.5 After 9/11
In the following part, we compare TAPA FSR and ISPS with regards to organized crime and terrorist acts following the aftermath of 9/11.

TAPA FSR:
The dreadful event on September 11th changed the conventional perspective towards security measures. However, TAPA FSR does not define specific requirements to address the new types of threats and dangers after 9/11 such as terrorist acts. There are some security requirements about the general measures to prevent tampering and theft, especially regarding the security of the truck. As well, the perimeter security requirements seem to guarantee the prevention from crime committed in normal situations. There are no measures regarding the unconventional situation like what happened for the twin towers.

Consequently, applying TAPA FSR would not be very suitable for security of transportation of businesses which function in areas under the potential risk of terrorist acts. As 9/11 showed, security threats can always be new and unprecedented. So what is more important here is that the corporates should be resilient. In other words they must be ready how to act in case of emergencies. As discussed earlier, TAPA FSR requires training of the truck drivers. However, the quality of the training and the level of staffs’ preparedness are will establish resilience, which applying TAPA FSR may not guarantee.

ISPS:
On the other hand, ISPS was naturally created to cope with the drawbacks in ordinary security standards in dealing with security threats after 9/11. The requirements strictly demand new types of checking of physical infrastructure, especially ship and containers. For example, ISPS requires that the guards need to monitor the areas outside the physical infrastructure. It means they have to be on alert to be proactive rather than be reactive. Moreover, the more detailed requirements about the level of lighting, frequency to patrolling and the areas to be patrolled illustrate the appropriateness of ISPS to cope with the terrorist acts and similar security threats.

In general, ISPS appears to be a more resilient standard compared to TAPA FSR, especially when security threats and risks like that of 9/11 are concerned. It has additional requirements about quality of training, drills and staff preparedness. Compared to TAPA FSR, the requirements for establishing the security of perimeters and physical structure (ship) are more designed to preempt attacks or terrorist acts.


Chapter 5: Discussion and conclusions

5.1 Discussion

In this thesis, basic requirements of the two security standards, TAPA FSR and ISPS, are compared and contrasted to find their differences. The aim is to illustrate the basic differences in their descriptions of requirements and to analyze the standards’ requirements based on the literature criteria. Moreover, in order to achieve the purpose of this thesis, we review the literature on the security of transportation to create literature criteria to work as frame of reference. The differences are considered in three levels of security for each of which different measures with different intensity are required. In our analysis of the basic differences of requirements, four areas of security are chosen to compare and contrast the requirements according to. These areas include Security of ports and facilities, Access to facilities, Handling cargo, and Background check and employment termination. Our comparative approach would illustrate the basic differences between TAPA FSR and ISPS for different levels of security. The basic differences between the requirements of TAPA FSR and ISPS can be concluded in using manpower for security of ports and facilities, intensity and frequency of using security measures and equipment for different levels of security, using X-ray screening of cargo, and background check and employment termination procedures.

5.2 Conclusions

Basically, four main differences between TAPA FSR and ISPS are illustrated in the thesis. Firstly, TAPA FSR does not require guards to patrol in vicinity of the port, whereas ISPS requires them even in the normal security level. In addition, ISPS requirements of surveillance, patrolling and blocking seem almost the same for all security levels. They differ in the intensity and frequency, whereas TAPA FSR requirements significantly differ for the levels of security, especially for levels A and B compared to level C. Moreover, unlike TAPA FSR, ISPS mandates X-ray screening of cargo in special cases. Finally, TAPA FSR defines background checks (both criminal and employment) and identifies employment termination procedures, while ISPS does define such requirements.
## Appendix 1

- Physical structure requirements:

### 1. Perimeter Security

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cargo handling and shipping and receiving yard enclosed by perimeter fencing</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>CCTV external coverage of shipping and receiving yard, including entry / exit point, to cover movement of vehicles and individuals</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CCTV coverage of all external dock area</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CCTV system able to view exterior sides of the facility</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flood lighting of loading/unloading areas</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dock doors illuminated externally at night</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Exterior and interior lighting levels support high quality CCTV images and recording</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All facility external doors alarmed to detect unauthorized opening and linked to main alarm system</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All windows and any other openings in warehouse walls and roof secured</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Floor-mounted warehouse windows (at ground floor) and street-level dock doors protected by anti-ram posts or other physical barrier</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dock doors of sufficient strength to delay forced entry by use of portable hand tools or ramming by vehicle</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reinforced exit doors from warehouse (steel doors and frames or suitable alternative)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exterior walls and roof designed and maintained to resist penetration (by removing building fabric, cutting or ramming by vehicle) or alarmed</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>External access to roof secured (ladder or stairs)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 2. Access Control – Office Areas

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visitor entry point(s) controlled</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Employee entry point(s) controlled</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Access control processes both during and outside normal operating hours to ensure access is granted only for authorized Supplier employees and visitors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 3. Facility Dock/Warehouse

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security controlled access points (e.g., Guard, card access or CCTV with intercom)</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Only Supplier’s authorized employees and escorted visitors permitted access to dock/warehouse</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restricted-access, caged/vault area for assets staged on-site for more than 2 hours: High-grade security mesh, chain-link or hard-wall, including top/roof; CCTV, controlled access</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted-access, caged/vault area for assets staged on-site for more than 6 hours: High-grade security mesh, chain-link or hard-wall, including top/roof; CCTV, controlled access</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All external dock and warehouse doors closed and secured when not in active use</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Internal dock doors and dock areas covered by CCTV</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Buyer-designated assets under 100% CCTV surveillance while in Supplier facility (this does not require 100% of floor coverage, rather 100% coverage of Buyer’s assets e.g. CCTV from dock, to pallet breakdown/buildup area, to high-value cage/vault)</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Motion detection alarms inside warehouse and activated when warehouse operational activity has stopped</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24x7x366 monitoring post; secure from attack</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All security system alarms responded to in real-time 24x7x366</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Minimum of 60 day records on system alarms</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restricted access to alarm system</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Alarms transmitted and monitored</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All CCTV images are digitally-recorded</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restricted access to CCTV system</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Minimum 30-day retention of all CCTV</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Minimum 60-day record of system transactions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Restricted access to system functions</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Quarterly review of access reports</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Information structure requirements:**

<table>
<thead>
<tr>
<th><strong>Documented security procedures</strong></th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal containers (defined as lunch box, backpacks, coolers, purses, etc.) controlled in the warehouse</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Searches or inspections performed on exit from secure areas used for Buyer’s assets</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Personal vehicles access to shipping and receiving yard/area controlled</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Box and pallet integrity verified upon receipt</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Control of cargo-handling equipment</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Integrity of container or trailer</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Documented maintenance programs in place for all technical (physical) security installations/systems (CCTV, Access controls, Intruder detection, Lighting)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Un-interrupted Power Supply (UPS) in place to ensure all electronic systems are able to function, even during power loss scenario</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Documented security procedures</td>
<td>Security Level A</td>
<td>Security Level B</td>
<td>Security Level C</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Local documented procedures for handling Buyer’s assets and escalation procedures for communicating security incidents to Buyer</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Process for timely reporting of lost, missing or stolen Buyer’s assets. Incidents to be reported by the Supplier to the Buyer within 12 hours; Obvious thefts reported immediately</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Emergency Buyer and local management contacts for security incidents listed and available</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Supplier Security Policy Statement available and communicated to all employees</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Awareness Training provided</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All employees and contractors issued and display company photo-ID badge</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Procedures in place to restrict Supplier’s employees, visitors and contractors access to Buyer’s assets</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Visitor policy in place</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Control of shipping documents/information so that details of Buyer’s assets are restricted to those with a “need to know”</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All drivers identified using government-issued photo-ID (e.g.; drivers' license; passport or national ID card, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Keys controlled in areas where Buyer’s assets are transiting or stored</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Random trash inspection procedures in place for trash removal from dock/warehouse</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security incident reporting system and method of tracking local security incidents</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Pre-loading or post-delivery storage of Buyer’s assets in trailers/containers.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
• Manpower requirements:

<table>
<thead>
<tr>
<th>1-Background checks</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Level A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Criminal history check in place encompassing 5-year criminal history and employment check (vetting within constraints of local country laws)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2-Terminated employees &amp; contractors procedure</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Level A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Termination procedures in place for employees and contractors, ensuring return of IDs, access cards, keys and other sensitive information</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Procedure in place to prevent systems access to Buyer’s data by terminated employees</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Records maintained to consider background of previously terminated personnel before re-hiring</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

• Means of transportation requirements:

<table>
<thead>
<tr>
<th>1-Cargo truck security</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Security Level A</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Solid-top, hard-sided or reinforced soft-sided trailers with lockable cargo doors</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Tamper-evident security seals for trucks carrying Buyer-only shipments</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Vehicle immobilization devices utilized</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Two way communication present during entire journey and monitored by Supplier and/or contractor</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Written contingency plans in place for reporting unscheduled events (i.e. stops, delays, route deviation)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Truck cab and ignition keys secured from unauthorized use at all times</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Requirements</td>
<td>Security Level A</td>
<td>Security Level B</td>
<td>Security Level C</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>2-Route Risk Assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk assessments performed on Buyer-designated routes</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>3-Loading/unloading</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proof of shipping and receiving records (Proof of Delivery, Bill of Lading, Waybill, etc.)</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy in place requiring driver to be present for loading and unloading when allowed</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4-Driver training</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supplier to provide robbery response training, detailing safe and secure actions to be taken during the event driver is threatened. Details of training are to be available to Buyer</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Awareness training provided to drivers on mitigating risk. Details of training are to be available to Buyer</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-Truck escorts</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capability to provide truck escorts with real time communications to base and local police; written documentation in place.</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Documented response procedures and training for escort personnel</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>6-Vehicle tracking</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GPS or similar technology installed and monitored on vehicles transporting Buyer’s assets</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
### Appendix 2

- **Physical structure requirements:**

<table>
<thead>
<tr>
<th>Monitoring the Security of the Ship</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship’s security personnel to observe the ship in general, and barriers and restricted areas in particular</td>
<td>increasing the frequency and detail of security patrols</td>
<td>switching on of all lighting on, or illuminating the vicinity of, the ship</td>
<td></td>
</tr>
<tr>
<td>the ship’s personnel should be able to detect activities beyond the ship, on both the shore side and the waterside</td>
<td>increasing the coverage and intensity of lighting or the use of security and surveillance equipment</td>
<td>switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship</td>
<td></td>
</tr>
<tr>
<td>coverage should include the area on and around the ship</td>
<td>assigning additional personnel as security lookouts</td>
<td>maximising the length of time such surveillance equipment can continue to record</td>
<td></td>
</tr>
<tr>
<td>coverage should facilitate personnel identification at access points</td>
<td>ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided</td>
<td>preparation for underwater inspection of the hull of the ship</td>
<td></td>
</tr>
<tr>
<td>coverage may be provided through coordination with the port facility</td>
<td></td>
<td>initiation of measures, including the slow revolution of the ship’s propellers, if practicable, to deter underwater access to the hull of the ship</td>
<td></td>
</tr>
</tbody>
</table>

- **Information structure requirements:**

<table>
<thead>
<tr>
<th>Delivery of ship’s stores</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>checking to ensure stores match the order prior to being loaded on board</td>
<td>exercising checks prior to receiving stores on board and intensifying inspections</td>
<td>subjecting ship’s stores to more extensive checking</td>
<td></td>
</tr>
<tr>
<td>ensuring immediate secure stowage of ship’s stores</td>
<td></td>
<td>preparation for restriction or suspension of handling of ship’s stores</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>refusal to accept ship’s stores on board the ship</td>
<td></td>
</tr>
</tbody>
</table>
### Manpower requirements:

<table>
<thead>
<tr>
<th>Access to the ship</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc</td>
<td>assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access</td>
<td>limiting access to a single, controlled, access point</td>
</tr>
<tr>
<td>in liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and carry on searching of persons, baggage (including items), personal effects, vehicles and their contents can take place</td>
<td>limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them</td>
<td>granting access only to those responding to the security incident or threat thereof</td>
</tr>
<tr>
<td>in liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP</td>
<td>deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols</td>
<td>directions of persons on board</td>
</tr>
<tr>
<td>segregating checked persons and their personal effects from unchecked persons and their personal effects</td>
<td>establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility</td>
<td>suspension of embarkation or disembarkation</td>
</tr>
<tr>
<td>segregating embarking from disembarking passengers</td>
<td>increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship</td>
<td>suspension of cargo handling operations, deliveries etc</td>
</tr>
<tr>
<td>identification of access points that should be secured or attended to prevent unauthorized access</td>
<td>escorting visitors on the ship</td>
<td>evacuation of the ship</td>
</tr>
<tr>
<td>securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects, or activities and the need for increased vigilance</td>
<td>providing additional specific security briefings to all ship personnel on any identified threats, re-emphasising the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance</td>
<td>movement of the ship</td>
</tr>
<tr>
<td></td>
<td>carrying out a full or partial search of the ship</td>
<td>preparing for a full or partial search of the ship</td>
</tr>
<tr>
<td>Restricted areas on the ship</td>
<td>Security Level A</td>
<td>Security Level B</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>locking or securing access points</td>
<td>establishing restricted areas adjacent to access points</td>
<td>setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied</td>
</tr>
<tr>
<td>using surveillance equipment to monitor the areas</td>
<td>continuously monitoring surveillance equipment</td>
<td>searching of restricted areas as part of a search of the ship</td>
</tr>
<tr>
<td>using guards or patrols</td>
<td>dedicating additional personnel to guard and patrol restricted areas</td>
<td></td>
</tr>
<tr>
<td>using automatic intrusion detection devices to alert the ship’s personnel of unauthorized access</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Freight requirements:

<table>
<thead>
<tr>
<th>Handling of cargo</th>
<th>Security Level A</th>
<th>Security Level B</th>
<th>Security Level C</th>
</tr>
</thead>
<tbody>
<tr>
<td>routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations</td>
<td>detailed checking of cargo, cargo transport units and cargo spaces</td>
<td>suspension of the loading or unloading of cargo</td>
<td></td>
</tr>
<tr>
<td>checks to ensure that cargo being loaded matches the cargo documentation</td>
<td>intensified checks to ensure that only the intended cargo is loaded on ships</td>
<td>verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location</td>
<td></td>
</tr>
<tr>
<td>ensuring, in liaison with the port facility, that vehicles to be loaded on board car carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP</td>
<td>intensified searching of vehicles to be loaded on car carriers, ro-ro and passenger</td>
<td></td>
<td></td>
</tr>
<tr>
<td>checking of seals or other methods used to prevent tampering</td>
<td>increased frequency and detail in checking of seals or other methods used to prevent tampering</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
References


3- Chelsea C., White, III, Alan L. Erera, Martin W.P. Savelsbergh, 2004, A research agenda for supply chain security and productivity, School of Industrial and Systems Engineering Georgia Institute of Technology

4- Dan Purtell and James B. Rice, Jr., 2007, Assessing Cargo Supply Risk, Corporate Risk International

5- Daniel Ekwall and Luca Urciuoli, 2009, Supply Chain Security Programs: Comparing authority and business certification, Swedish School of Textiles, University of Borås

6- Hau L. Lee and Seungjin Whang, 2003, Higher Supply Chain Security with Lower Cost: Lessons from Total Quality Management, Graduate School of Business, Stanford University, Stanford, CA 94305, USA


8- Peter Kennedy, Charles Perrottet and Charles Thomas, 2003, Scenario Planning after 9/11: Managing the impact of a catastrophic event, Strategy & Leadership, VOL. 31 NO. 1 2003, pp. 4-13


10- Yossi Sheffi, James B. Rice, Jr., Jonathan M. Fleck, Federico Caniato, 2003, Supply Chain Response to Global Terrorism: A Situation Scan, Center for Transportation and Logistics, Massachusetts Institute of Technology