Capabilities meet regulation:

The Compliance Processes of Mexican Food Supply Chains with United States Biosecurity Regulations

Yari Borbon-Galvez

Doctor of Philosophy in Science and Technology Policy Studies

SPRU-Science and Technology Policy Research

School of Business, Management and Economics

University of Sussex

Brighton, United Kingdom

Submission: May 2011

Acknowledgments

I would like to acknowledge many people and institutions that made this thesis a reality. First of all, the CEOs, Compliance Managers and Administrative Personnel of the firms who were the main source of information for this thesis.

I would like to acknowledge my father, Rafael Ruben Borbon Siqueiros, with whom I had many conversations about technological change and innovation, and to my mother, Maria Elena Galvez Esparza, with whom I had many conversations about law and regulation, both of whom are the foundations of the present work.

I would like to acknowledge my doctoral supervisors, Paul Nightingale who was always enthusiastic and innovating about the thesis, and William Eduard Steinmueller (and his father), who continuously challenged me with the phrase “there is always room for improvement”.

I would like to acknowledge the Mexican Science and Technology Council (CONACYT), whose grant covered most of the costs of my doctoral studies, without which this thesis would have not existed.

Various people and institutions supported this investigation. Dr Vidal Salazar-Solano, Dr Luis Nunez-Noriega and Dr Jorge Siller-Cepeda from Centro de Investigacion en Alimentacion y Desarrollo, AC; Alison Moore and Georgina Felix from Fresh Produce Association of the Americas; Evangelos Demerutis from Trocadero Confederacion de Asociaciones de Agricultores del Estado de Sinaloa; and many others.

My acknowledgment to Maria Del Sorbo with whom I spent most of my time discussing my thesis, and with whom I learnt the methodology used in this investigation, refined my interviewing techniques, and who helped me understand what capabilities are.

I acknowledge the feedback from faculty and colleagues such as: the yearly SPRU research committees, the SPRU DPhil Days, the Technology and Development Group at the Freeman Centre, the Latin American Affairs at the Freeman Centre, and the SPRU Peer2Peer, and many other colleagues and faculty from SPRU, Centrim and IDS. And with much appreciation to many SPRU friends that helped in the final stages of this research. All the mistakes and omissions are my own responsibility however.

Dedications

This work is dedicated to my parents, and to my sister and her off-springs. They nurtured and also suffered my desire to seek for intellectual and cultural challenges.

I would also like to dedicate this work to my wife to be; who became the reason for changing my view of the present work from a personal to a family achievement. With eternal love to my other self, Maria, Amor.

To all my family, and very especially to La Jose, who faithfully saw me leave to start this piece of work, and who is now waiting for it from up high in companion of Manina, Panino, Abuelita, Abuelito and more members of my family that were also called by The Lord.

Thanks be to God.

.

Abstract

This thesis explores how Mexican fresh produce supply chains have responded to US bio-security regulations designed to prevent the intentional and accidental contamination of imported food. It explores the compliance processes, which are theorised using a framework drawn from the Resource-Based View (RBV) and the Supply Chain Governance (SCG) literatures.

The constructs developed herein regarding capabilities and supply chain 'governance structures' complement previous Regulation Studies (RS) explaining compliance behaviour.

The thesis analysed 12 case studies, and tested causal conditions of compliance using a multi-value Qualitative Comparative Analysis (mvQCA) method. The main results show: 1) the pathways to meet the regulatory requirements; 2) the limited diversity of capabilities associated with higher levels of compliance; and 3) the importance of tight supply chain coordination to source and exchange knowledge for compliance, regardless of how or who governs the supply chain.

The thesis contributes to various academic debates. It removes the RVB assumptions that resources and capabilities are intrinsically valuable and complementary, and therefore contributes towards making the theory less tautological. It shows how SCG benefits when the effects of supply chain integration and coordination are examined independently. It differentiates between firms lacking willingness and firms lacking capabilities to comply, making it possible to define suitable regulatory strategies for each type of firm.

The thesis makes a methodological contribution as it is one of the first studies applying the mvQCA in Science, Technology and Innovations Studies (STIs). The new methodology is used here to test the causal conditions of compliance, but can also be applied to innovative performance more generally.

The thesis concludes by showing how US regulations were effective in achieving their regulatory aims without significant negative consequences, and suggesting that STI regulatory policies can be used to increase business engagement to prevent the intentional and accidental contamination of the food chain.

Table of Contents

1.	**CHAPTER 1 INTRODUCTION**	**1**
1.1.	United States' New Security Agenda in The 9/11 Aftermaths	2
1.2.	The US Regulatory Diffusion	10
1.3.	Thesis Structure	12
2.	**CHAPTER 2 THEORY AND FRAMEWORK: UNDERSTANDING COMPLIANCE**	**14**
2.1.	Regulations: Public, Private, and Public-Private Partnership	18
2.2.	A Resource-Based View of Compliance	25
2.3.	Supply Chain Governance Structures and Compliance	39
2.4.	Minding Some Gaps in the Literature	45
2.5.	Analytical Framework	48
3.	**CHAPTER 3 METHODOLOGY**	**53**
3.1.	Aim, Objective and Research Questions	53
3.2.	Research Questions and Hypotheses Testing Roadmaps	55
3.3.	Research Design	66
3.4.	Research Process	72
3.5.	Qualitative Comparative Analysis: Multi-Value and Crisp Sets	81
3.6.	Summary	85
4.	**CHAPTER 4 BACKGROUND**	**86**
4.1.	Supply Chains and Post 9/11 Security Regulation	86
5.	**CHAPTER 5 CASE STUDIES**	**103**
5.1.	Supply Chain 1 Distributor (SC1D)	106
5.2.	Supply Chain 1 Grower/Packer/Exporter (SC1E)	112
5.3.	Supply Chain 1 & 5 Transport Provider (SC1&5T)	121
5.4.	Supply Chain 2 Distributor (SC2D)	128
5.5.	Supply Chain 2 Grower/Packer & Transport Provider (SC2E&T)	134
5.6.	Supply Chain 3 Distributor (SC3D)	141
5.7.	Supply Chain 3 Packer/Exporter (SC3E)	148
5.8.	Supply Chain 3 Transport Provider (SC3T)	155
5.9.	Supply Chain 4 Distributor (SC4D)	162
5.10.	Supply Chain 4 Packer/Exporter & Transport Provider (SC4E&T)	170
5.11.	Supply Chain 5 Distributor (SC5D)	176
5.12.	Supply Chain 5 Packer/Exporter (SC5E)	184
5.13.	Brief Remarks on the Case Studies	194
6.	**CHAPTER 6 EMPIRICAL RESULTS**	**195**
6.1.	Regulatory Compliance Process	195
6.1.1.	Summary of Compliance Processes	195
6.1.2.	MVQCA of The Regulatory Compliance Process	212
6.2.	Capability Building	224
6.2.1.	Summary of Capabilities Building Processes	224
6.2.2.	MVQCA of The Compliance Capabilities Building	238
6.3.	Supply Chain Relationships	249
6.3.1.	Summary of Supply Chains Governance Structures	250
6.3.2.	MVQCA of The Supply Chains Governance Structures	256
7.	**CHAPTER 7 DISCUSSION OF RESULTS**	**274**
7.1.	Business Regulation and The Compliance Process	274
7.2.	Leveraging Value from Compliance Capabilities	280
7.3.	Supply Chain Relationships for Capability Building	286
7.4.	Compliance Capability Building's Governance Structures	294
8.	**CHAPTER 8 CONCLUSIONS**	**297**
8.1.	Answering the Research Questions	297
8.2.	Theoretical Contributions and Implications	300
8.3.	Methodological Contributions, Limitations and Implications	305
8.4.	Regulatory Implications	307
8.5.	STI Security Regulation and Policy Implications	309
9.	**APPENDICES**	**315**
9.1.	Appendix A: Cover Letter	315

9.2.	Appendix B: Interview COMCAP 2007-2008	316
9.3.	Appendix C: Questionnaire COMCAP 2007-2008	318
9.4.	Appendix D: Guide to Read Tosmana Reports	324
10.	**REFERENCES**	**328**

List of Tables

Table 1.2.1: US CBP mutual recognition agreements with foreign governments related to CTPAT.......10

Table 2.1: Selected Federal Regulations in the United States 1887-2006...15

Table 2.5.1: Compliance capabilities: an organising framework 52

Table 3.2.1: Classification of capabilities by sophistication level 59

Table 3.2.2: Illustrative example of capabilities upgrading by compliance levels (no real data) 60

Table 3.2.3: Illustrative example of capabilities configurations causing compliance (no real data) 60

Table 3.2.4: Supply chains governance structures: constructs and definitions 64

Table 3.2.5:Illustrative example (no real data): firms' governance structures 65

Table 3.2.6. Illustrative example (no real data): Governance structures for capabilities sophistication65

Table 3.3.1: Case study outline/template...70

Table 3.4.1: Validating the instruments 74

Table 3.4.2: Content-Analytical Matrix (Compliance Process by Security Capabilities Matrix)..............80

Table 3.5.1: Illustrative example of the Boolean logic 82

Table 4.1.1: CTPAT Security criteria/guidelines sections 100

Table 4.1.2: CTPAT Statistics (April 2005) 102

Table 5.1: Case study outline 103

Table 5.2: Classification of variables from case studies 104

Table 5.1.1: SC1D Security resources and compliance capabilities sophistication 111

Table 5.2.1: SC1E Security resources and compliance capabilities sophistication 120

Table 5.3.1: SC1&5T Security resources and compliance capabilities sophistication 127

Table 5.4.1: SC2D Security resources and compliance capabilities sophistication 133

Table 5.5.1: SC2E&T Security resources and compliance capabilities sophistication 140

Table 5.6.1: SC3D Security resources and compliance capabilities sophistication 147

Table 5.7.1: Compliance enforcement team and roles SC3E 149

Table 5.7.2: SC3E Security resources and compliance capabilities sophistication 154

Table 5.8.1: SC3T Security resources and compliance capabilities sophistication 161

Table 5.9.1: SC4D Security resources and compliance capabilities sophistication 169

Table 5.10.1: SC4E&T Security resources and compliance capabilities sophistication.........................175

Table 5.11.1: SC5D Security resources and compliance capabilities sophistication............................183

Table 5.12.1: SC5E Capability building and resource development..193

Table 6.1.1.1. Sources of regulatory information 196

Table 6.1.1.2: Regulatory regimes and communication systems 203

Table 6.1.1.3: Regulatory regimes, conformance, and implementation strategies 204

Table 6.1.1.4: Participation in the evaluation of the development of security resources 206

Table 6.1.1.5: Speed and intensity of the conformance process 208

Table 6.1.1.6: Summary of the conformance processes (Selected firms: SC3T and SC5E) 211
Table 6.1.2.1: Causal configurations of regulatory process for Middle-High Compliance * 215
Table 6.2.1.1: Compliance and conformance levels 225
Table 6.2.1.2: Summary of capabilities building 227
Table 6.2.1.3: CTPAT Security Resources Development 228
Table 6.2.1.4: Compliance levels and capabilities sophistication 229
Table 6.2.1.5: Inventory of intermediate capabilities by low compliant firms 233
Table 6.2.1.6: Inventory of intermediate capabilities by middle compliant firms 234
Table 6.2.1.7: Inventory of advanced capabilities (Vertical alignment) by middle and high compliant firms 236
Table 6.2.2.1: Causal configurations of the compliance capability building* 240
Table 6.3.1.1: Supply chain governance structures...251
Table 6.3.1.2: Summary of supply chain governance structure 253
Table 6.3.2.1. Causal conditions, thresholds, and interpretations of governance structures 260
Table 6.3.2.2: Governance and structure configurations of capability building* 262

List of Figures

Figure 1: Snowball technique (Firms undisclosed by request) 77
Figure 2: CANAMEX Corridor 91
Figure 3: The Basic Fresh Produce Supply Chain from Mexico to United States 95
Figure 4: Summary of the compliance process by SC1D 108
Figure 5: Summary of the compliance process by SC1E 114
Figure 6: Compliance process SC1&5T 124
Figure 7: Compliance process SC2D 130
Figure 8: Compliance process SC2E&T 137
Figure 9: Supply chains reorganisation by lost certification by SC3D 142
Figure 10: Compliance process SC3D 144
Figure 11: Compliance process SC3E 151
Figure 12: Compliance process SC3T 157
Figure 13: Supply chains effects of lost certification by SC4D 163
Figure 14: Compliance process SC4D 166
Figure 15: Compliance process SC4E&T 171
Figure 16: Compliance process SC5D 178
Figure 17: Compliance process SC5E 187
Figure 18: CTPAT related security resources 192
Figure 19: Regulatory awareness diffusion 197
Figure 20: Compliance decision making 199
Figure 21: Negative feedback loops in the compliance decision-making 202
Figure 22: mvQCA of regulatory awareness as causes of middle-high compliance 217
Figure 23: Compliance decision and conformance decision as drivers of compliance 219
Figure 24: Communication mechanisms for compliance 220
Figure 25: Monitoring and evaluation for compliance 222
Figure 26: Capability building by compliance level 230
Figure 27: Capability building in low compliance 242
Figure 28: Capability building for middle compliance 243
Figure 29: Capability building for high compliance 245
Figure 30: Compliance capability building 247
Figure 31: Evolutionary compliance capability building 248
Figure 32: Visual representation of the governance structures 254
Figure 33: Governance structures for security-based managerial systems 263
Figure 34: Governance structures for security-based desorptive capacity 265

Figure 35: Governance structures for security-based vertical alignments..267
Figure 36: Governance conditions for security-based compliance capabilities 269
Figure 37: Structural conditions for security-based compliance capabilities......................................270
Figure 38: Governance structures for security-based compliance capabilities...................................271

List of Charts

Chart 1: United States imports of produce from Mexico from 1991-1993 to 2006-2008........................87

Chart 2: Fruit and vegetable consumption by selected regions. 88

Chart 3: Import Value (Million US dollars)...88

Chart 4: Share of autumn-winter production value of main Mexican States 90

Chart 5. Threshold setting for power asymmetry..258

Chart 6. Threshold setting for Asset specificity...259

List of Images

Image 1: Screening and controlling the access to the packaging facilities 115

Image 2: Access control to packaging and greenhouses (biometrics) 116

Image 3: Banners, Sensor-activated hands sanitizer, and GMP no contact with the produce 118

Abbreviations

9/11	Terrorists attacks of September 11, 2001
ACI	Advanced Commercial Information
ACR SmartButton	ACR systems - miniature-sized temperature logger
AD	Administrative Detention of Cargo
ADOT	Arizona Department of Transportation
AEO	Authorized Economic Operator
ALIGN	Vertical alignment
BioShield	Project BioShield Act
CAADES	Confederacion de Asociaciones Agricolas del Estado de Sinaloa
CBP	Customs Border Protection Agency
CCM	Cold Chain Monitoring
CCTV	Closed-Circuit Television
CEO	Chief Executive Officer
CIAD	Centro de Investigacion en Alimentacion y Desarrollo Alimentacion
CIDH	Comision para la Investigacion y Defensa de las Hortalizas
CM	Compliance Manager
CO	Compliance Officer
COAC	Advisory Committee on Commercial Operations
COMCAP 2007-2008	Research on Compliance Capabilities 2007-2008
Consul	Consultant
COOLTRAX	Cold Chain Monitoring and Tracking Temperature
CoordActivities	Supply Chain Activities Coordination
CoorInverst	Supply Chain Investment Coordination
CSI	Container Security Initiative
csQCA	Crisp Sets Qualitative comparative analysis
CTPAT	Customs-Trade Partnership Against Terrorism
D	Distributor
DHS	Department of Homeland Security
ECPR	European Consortium for Political Research
EM	Electronic Manifest
EU	European Union
Exp	Exporter
FAO	United Nations Food and Agriculture Organisation
FAST	Fast and Secure Trade Lanes
FBI	United States Federal Bureau of Investigation
FDA	Food and Drug Administration
FPAA	Fresh Produce Association of the Americas
FSC	Food Safety Certifiers
fsQCA	Fuzzy sets Qualitative Comparative Analysis
GAP	Good Agricultural Practices
GHP	Good Handling Practices
GM-Free	Generically Modified Free
GMP	Good Manufacturing Practices
GPS	Global Positioning System
HACCP	Hazard Analysis and Critical Control Point
HAZMAT	Hazardous Materials
Homeland Act	Homeland Security Act 2002
IA	Industry association
ID	Digital Identification
IN	Industry Network
INTCOORD	Internal coordination
IS	Invoicing System
ISO	International Standard Organisation
ITS	Information and Communication Systems
L-M	Low-Medium

MANSYS	Managerial systems
Mex	Mexican government
M-H	Medium-High
MR	Maintenance and Inspections of Records of Food
mvQCA	multi-value Qualitative Comparative Analysis
MX	Mexico
NAFTA	North American Free Trade Agreement
NGO	Non-Governmental Organisations
OECD	Organisation for Economic Co-operation and Development
ORGCAP	Organisational competencies
OSHA	United States Occupational Safety and Health Administration
PEP	Policia Estatal Preventiva
PN	Prior Notice of Imported Food Shipments
POE	Mariposa Port of Entry
PPP	Public-Private Partnership Regulation
QCA	Qualitative comparative analysis
RBV	Resource-Based View
RF	Registration of Food Facility
RFID	Radio frequency identification
SAGARPA	Secretaria de Agricultura, Ganaderia, Desarrollo Rural, Pesca y
SC	Supply Chain
SEDENA	Secretaria de la Defensa Nacional
SENASICA	Mexican Ministry of Agriculture
SIAP	Sistema de Informacion Agroalimentaria y Pesquera
Small-N	Small sample size
SPPA	Strategic Partnership Program Agroterrorism Initiative
SPS	Microbiological controls
STAH	Stakeholders support
STI	Science, Technology and Innovation
SUPDEV	Suppliers development
TAPA	Transported Asset Protection Association
TBA	2,4,6-tribromoanisole
TOSMANA	Tool for Small-N Analysis
TPC	Third party certifiers
UK	United Kingdom
US BioAct 2002	Public Health Security and Bioterrorism Preparedness and Response Act of 2002
US EPA	United States Environment Protection Agency
US	United States of America
USD	United States Dollars
USDA	United States Department of Agriculture
USDOT	United States Department of Transportation
USSG	United States Sentencing Commission, Guidelines Manual
VACIS	Gamma ray inspection machines
VCG	Value Chain Governance
WCO	World Customs Organisation
WTO	World Trade Organization

1. CHAPTER 1 Introduction

In 2004, Tommy G. Thompson, the then United States Health and Human Services Secretary, expressed major security concerns about food poisoning, and stated "I, for the life of me, cannot understand why the terrorists have not, you know, attacked our food supply because it is so easy to do" (Branigin, Allen, & Mintz, 2004). This thesis addresses these concerns and analyses how agri-businesses become compliant with regulations intended to prevent the accidental and intentional contamination of food in the supply chain. The investigation explores how firms' ability to prevent regulatory disruptions, and in some instances to potentially gain advantage from them, relates to their supply chain's relationships, with a particular focus on how knowledge is sourced.

Specifically, the main research questions in this thesis are: To meet regulations for the prevention of accidental and intentional contamination of food: 1) what compliance processes do firms follow, 2) what capabilities do firms build up, and 3) what governance structures enable firms to build up their capabilities?

These questions are important because one of the key roles of the modern regulatory state is to harness private capacity to secure compliance with regulatory goals (Parker, 2000, p. 542). In other words, if regulators are interested in knowing how firms' capabilities (with human intervention) may produce resources that are compliant with regulations, then it may be worth paying attention to how can those capabilities be produced, what impact will those regulations have on international supply chain relationships, and what programmes should be designed to enhance private compliance capacity.

The thesis identifies the factors that may influence the effectiveness of different compliance processes in a variety of supply chain contexts. This research could not identify a single model of compliance for firms and supply chains.

In other words, although there are a number of options related to regulatory awareness, assessment, implementation, and evaluation, there are only limited choices conducive to compliance. Hence, many capabilities could be built to enhance the security of firms and supply chains, but only a limited number of them are conducive to compliance; and although there are multiple types of supply chain relationships under which firms may build up capabilities, again only a limited number of these relationships are conducive to compliance.

These results were found using an innovative analytical methodology, the qualitative comparative analysis (QCA) (Kogut & Ragin, 2006; Ragin, 1989). This methodology is suitable for comparative case studies, and especially for studies with sample sizes that are insufficient for statistical generalisations, but too large for complex and time consuming single case study analysis.

The contributions of this thesis focus on two main areas. First, it suggests that including compliance and capabilities building processes in the analysis of compliance in a regulatory studies framework, may improve understanding of the relationship between regulators and regulated firms. This helps move analyses beyond the commonly held idea that compliance is just a matter of incentives, sanctions and willingness. Second, it suggests that combining the Resource-Based View (RBV) with this new methodological approach allows us to drop some of the core assumptions in the RBV that knowledge, capabilities, and resources are complementary and heterogeneous, by offering another way of assessing when complementarities are valuable. This suggests that heterogeneity may not be enough for competitive advantage.

The policy recommendations, directed at policy makers in government bodies such as the Department of Homeland Security, suggest that security policy focused on improving infrastructure may discourage supply chain participation in CTPAT/FAST, the flagship Public-Private Partnership programme against terrorism.

1.1. United States' new security agenda in the 9/11 aftermaths

Most countries have public and private regulations to prevent accidental contamination of food; however, regulations to prevent intentional contamination are a later development. Preventing life-threatening intentional contamination involving humans, plants and animals are now covered by counter-terrorism initiatives. This has been a United States (US) concern since before the 9/11 attacks and was, for example, suggested in 1999 when the

US Government Accounting Office recommended developing a risk assessment method (Cordesman & Burke, 2001, p. 2; Zilinskas, 2003, p. 2).

After 9/11, however, the US worked on a new biosecurity system that included the prevention of intentional contaminations. This new US biosecurity system was prioritised within public policy, as shown by the budget for the Department of Homeland Security, which, together with project BioShield, grew more than the total US budget from 2004 to 2005, 12.4% and 7.8% respectively (Homeland Security, 2006, p. 5; Office of Management and Budget, 2006b, p. 22).

According to Haftendorn (1991) such 'security systems' presuppose the existence of institutions to regulate interactions between units (states) and enforce rules and norms, with such interaction being influenced by the internal capabilities of the units (Haftendorn, 1991, p. 11). Buzan, Waever and de Wilde (1998) enhanced the previous notion of units and included actors within and across nations such as firms (Buzan, Wæver, & de Wilde, 1998, p. 6). Based on the previous definitions, we understand that the new US biosecurity system may be a conglomerate of governmental agencies, firms and related organisations interacting and enforcing rules and norms; such interactions and enforcements depend on their own capabilities to lower the risk of disruptive activities in the food supply.

The Department of Homeland Security (DHS) leads the new US biosecurity system. The DHS reorganised and created new public resources for security and public safety. It was developed from the merger of 22 different former agencies, and its general purpose was to coordinate all their non-defense related activities (Office of Management and Budget, 2006a, p. 131).

Also under the leadership of the DHS, the biosecurity system for the prevention of contamination of the food supply, seeks to engage (regulate) the private sector (food supply chains included) with programmes such as the Customs-Trade Partnership Against Terrorism (CTPAT), CSI-Container Security Initiative, and SPPA-Strategic Partnership Program Agroterrorism Initiative[1]. Each one of these has its own guidelines, certification

and enforcement mechanisms.

[1] The US DHS gets investigative support from institutions like the National Center for Food Protection and Defense and the National Center for Foreign Animal and Zoonotic Disease Defense. The full list of centres can be found at http://www.dhs.gov/xres/programs/editorial_0498.shtm

The engagement of the private sector (food supply chains included) in the biosecurity system was one of the functions given to the US Department of Homeland Security (DHS) by the Homeland Security Act 2002 (Homeland Act). The Homeland Act mandated the inclusion of a special assistant to the Secretary of the DHS in charge of communicating, interfacing, partnering and assisting in the development and promotion of best practices with the private sector, as well as advising the Secretary on the development of regulatory policies to address homeland security challenges ("Homeland Act," 2002, pp. 2143-2144).

The regulatory arms of the biosecurity system

Of three the main regulations included in the biosecurity system, one was compulsory and two were 'voluntary', reflecting State Regulations, Public-Private Partnership, and Self-Regulations respectively.

The State (compulsory) regulations with direct implications for food supply chains came from the *Public Health Security and Bioterrorism Preparedness and Response Act* of 2002[2]. The US BioAct 2002 gave regulatory powers to the Food and Drug Administration (FDA), whilst monitoring and enforcement powers were held by the Customs Border Protection Agency (CBP), one of the largest and most complex components of the Department of Homeland Security (DHS). The FDA ruled that along international food supply chains, administrative procedures, office, and business operations for security have to be developed and deployed (US BioAct 2002), thus non-compliance by the food and its supply chain would lead to foreign firms being denied the opportunity to trade with the US.

The public-private partnership (voluntary) regulation, Customs-Trade Partnership Against Terrorism (CTPAT), is also important for foreign firms. It would prevent CTPAT certified firms from being forbidden access to the US in the event of another terrorist attack. Based on regulatory understanding that they had the capabilities needed to prevent their facilities or products being used to harm the US population, such firms would be seen as 'low risk'. Furthermore, even when the US is not being attacked, these regulations allow CTPAT

[2] (US BioAct 2002), and specifically from section 303, *Administrative Detention of cargo (AD) in case of suspicious cargo/driver*; section 305, *Registration of Food Facility (RF)*; section 306, *Maintenance and Inspections of Records of Food (MR)*; and section 307, *Prior Notice of Imported Food Shipments (PN)*

certified firms to have preferential access, releasing cargo from the border faster and with fewer security inspections. This would give them an economic advantage over non-compliant firms. The programme is administered by the Customs Border Protection (CBP)[3] (C-TPAT/CBP, 2004).

On the other hand, self-regulations are those elicited and enforced by industry associations, international organisations, and/or firms themselves. These regulations have been a way of responding to consumer concerns about product quality, safety, environment and social issues. For the prevention of contaminations by the food industry there are regulations such as the International Standard Organisation-22000 (ISO-22000), Hazard Analysis Critical Control Point (HACCAP), Organic, Generically Modified Free (GM-Free) products, labelling, and other good agricultural and handling regulations to increase food safety. The transport industry adheres to regulations such as the Transported Asset Protection Association (TAPA) and the International Standard Organization (ISO-28000).

Furthermore, it is expected that even firms without security certifications may still have security measures in place, because a consequence of reputational damage following a security failure may be for buyers to terminate their relationships with the firm (Meidinger, 2006, p. 76; Raynaud, Sauvee, & Valceschini, 2005, p. 50); assuming that buyers are able to find firms as substitutes for the previous suppliers. Also, firms may introduce security measures because they may want to build up reputational capital to access better business deals (Klein, 1996, pp.454-455; Lafontaine & Slade, 2010 Forthcoming; Raynaud et al., 2005, p.56), to correct market failures, or to follow interest groups (Bartle & Vass, 2005, p. 46). For instance, in 1994 Wal-Mart conducted a four month exercise in Jacksonville, Texas, to protect what it considers their most valuable resources, 650,000 associates and 60 million weekly customers, putting in place safety and security measures that drove up sales by 13% by the end of the exercise (Gorman, 1996, pp. 56-57)[4].

All three regulatory regimes (i.e. Public Regulations, Public-Private Partnership Regulation, and Self-Regulation) may contribute to biosecurity and help prevent accidental and

[3] For all business except transport providers, the certification is called Customs-Trade Partnership Against Terrorism (CTPAT); while for transport providers the certification is called Fast and Secure Trade Lanes (FAST).

[4] Also Safeway removes unsafe or hazardous products from their stores as a food safety measure. See for instance the Safeway product recalls webpage for the latest recalls, http://www.safeway.com/IFL/Grocery/Product-Recalls

intentional contaminations of the food supply. However, an important question remains: which forms of regulation best achieve the purposes of the biosecurity system?

A study suggested that implementing FDA compulsory biosecurity regulations in the US milk supply chain is less cost effective than the use of real-time tracking with smart seals and voluntary biosecurity regulations (Nganje, Bier, Han, & Zack, 2008, p. 1271), which are part of the best practices guidelines of CTPAT (C-TPAT/CBP, 2010, pp. 14,18).

These results, combined with the fact that firms' capabilities determine whether and how biosecurity regulations are applied to prevent contaminations, suggest that, in some instances, CTPAT may be a more cost effective way of enhancing supply chain biosecurity capabilities than the FDA Public regulations (taking self-regulation as a baseline). This raises the question of what the food supply chain biosecurity baseline was before the FDA and CTPAT regulations.

Food supply chain system

The traditional concern of the international food supply chains had been to increase their efficiency in order to reach markets faster, at less cost, with greater accuracy, and often "just-in-time" (Swafford, Ghosh, & Murthy, 2006; Walters, 2006). More recently, issues related to food safety (preventing accidental contamination) and quality have also gained importance (Bollen, Riden, & Opara, 2006; Frearne, Hornibrook, & Dedman, 2001; Hobbs, Fearne, & Spriggs, 2002; Opara, 2003; Pimentel, Borin, & Claro, 2004; Sohal, Millen, Maggard, & Moss, 1999).

The main actors associated with Mexico-US fresh produce supply chains who traditionally deal with food safety and quality issues are the Food and Drug Administration (FDA), the United States Department of Agriculture (USDA), the Mexican Ministry of Agriculture (SENASICA), industry associations (e.g. CAADES-Confederacion de Asociaciones Agricolas del Estado de Sinaloa, FPAA-Fresh Produce Association of the Americas), third party certifiers (e.g. PrimusLabs, Scientific Certifications Systems, Mexico Calidad Suprema), and the firms themselves (Iizuka & Borbon-Galvez, 2009, pp. 16-17).

The biosecurity baseline for US and Mexican fresh produce growers, processors and distributors before the FDA and CTPAT regulations seemed to be mainly complying with food safety regulations, such as the Good Manufacturing Practices (GMP), Good Agricultural Practices (GAP), Hazard Analysis and Critical Control Point (HACCP), Microbiological controls (SPS), and so on (Iizuka & Borbon-Galvez, 2009, pp. 16-17).

Studies have shown that supply chain measures based on CTPAT biosecurity voluntary regulations (e.g. monitoring and tracking systems) are more cost efficient than FDA compulsory regulations (Nganje et al., 2008, p. 1271) and increase supply chain efficiency (Willis & Ortiz, 2004, p. 22). Yet another study argues that firms weakens their supply chain collaboration when they try to comply with CTPAT biosecurity voluntary regulations, which suggests that firms mostly build up capabilities for FDA biosecurity compulsory regulations (Agiwal, Mohtadi, & Kinsey, 2008, p. 10) are not willing to give up collaboration for cost efficiency of their supply chain.

Moreover, if a firm that previously used food safety measures to prevent contamination shifts to (voluntary) CTPAT biosecurity regulations it may be better off, compared to it moving to (compulsory) FDA biosecurity regulations, in which case the new biosecurity system may be clashing with the food supply chain system.

The clash of the systems: trade-offs between costs and risks

One explanation of the clash of the systems is the trade-offs between implementation costs and risk reduction. According to Bongers (2004), security regulations increase the long term costs of doing business all over the world, but particularly in North America, where the estimated cost of compliance in 2003 was USD $11,810 for a facility[5] to develop security policies, training and initial physical assessments (Bongers, 2004, p. 35). In the same line of argument, a study commissioned by the US Department of Homeland Security, surveying 29% of the CTPAT certified companies, out of which 16% said costs

---

[5] "The term 'facility' includes any factory, warehouse, or establishment (including a factory, warehouse, or establishment of an importer) that manufactures, processes, packs, or holds food. Such term does not include farms; restaurants; other retail food establishments; nonprofit food establishments in which food is prepared for or served directly to the consumer; or fishing vessels (except such vessels engaged in processing as defined in section 123.3(k) of title 21, Code of Federal Regulations)" (US BioAct 2002, p. 116 STAT. 668).

outweigh the benefits, and 24% said cost and benefits are about the same (C-TPAT/CBP, 2007, p. 58), with an estimated average potential implementation costs of CTPAT of USD $187,480 per facility in nine security resources: business partners, physical security, access controls, personnel control, procedural security, information and communication technologies, container and trailer security, conveyance security, and threat awareness. The CTPAT programme annual maintenance costs were USD $118,244, which resulted in firms almost doubling their annual expenditure on supply chain security (C-TPAT/CBP, 2007, pp. 41-45).

Firms therefore face trade-offs between the increased business costs of regulatory compliance and the risks and consequences of non-compliance. This has organisational implications, as firms with Mexico-US supply chains have a choice of either adapting their technological capabilities for compliance or running the risk that they may be displaced by firms or entire supply chains that already have security capabilities[6].

An example of what might happen to a non-compliant firm can be seen in the Tylenol case in 1982. On that occasion, seven people died after taking Extra-Strength Tylenol that had been laced with cyanide and placed on Chicago-area pharmacy shelves. Tylenol manufacturer Johnson & Johnson initiated one of the largest drug recalls in US history, which cost them more than $100 million. The company replaced capsules for caplets and unveiled new tamper-resistant packaging, which has now become the industry norm. Later the US Congress made drug tampering a federal offence (Fintor, 2002) allowing the use of national police resources (the FBI) to become involved.

A more recent recall of Johnson & Johnson products was prompted by '2,4,6-tribromoanisole' (TBA) applied to wooden pallets used to transport and store packaging materials (Kavilanz, 2010). Johnson & Johnson recalled over 40 medications for approximately six million bottles, and in May 2010 shut down the manufacturing facility in Fort Washington, PA responsible for repeated contaminations of drugs[7]. This caused a 13.6% reduction in over-the-counter pharmaceutical and nutritional products sales in the

[6] Although security capabilities are defined in different ways (Closs, 2005), based on the definitions of resources and capabilities in the theoretical chapter, we understand security capabilities as "ways of acquiring, researching, experimenting, planning, designing, preventing, developing, coordinating, learning, predicting, or reconfiguring, security resources".
[7] http://www.fda.gov/Safety/Recalls/ucm210443.htm

second fiscal quarter, causing an approximately USD $176 million loss of sales, and damaging the company brand (Wernau, 2010).

Another recent case involved poultry and hogs tainted by dioxin is being investigated by the German government to see if it has criminal origins, on the grounds that some firms had been aware of the contamination since March 2010. At the moment 4,700 farms in Germany have been closed[8].

Not only producers, but any stage in the supply chain (i.e. material and input providers, exporters, transporters, distributors, wholesalers, retainers, food chains, consumers) may be at risk. An investigation about fatalities and injuries due to intentional contamination shows various stages of the supply chain, water supply, pre-harvest, post-harvest, retail and food service, may be at risk. Although these acts are not very likely to be from terrorists inspired by ideological motives[9], they are certainly cases of intentional contamination; and although the US has the most cases, such attacks have also been seen in the rest of the world (Dalziel, 2009, p. 24)[10].

In summary, there is an open question of how firms may deal with new US biosecurity regulations? How they build up their supply chain biosecurity capabilities (if at all)? Although these questions are relevant for the Mexico-United States food supply, they may also capture the attention of business and regulators from other parts of the world, as shown in the following section.

Of the three types of regulations, the empirical focus of this thesis is on the effect of Public-Private-Partnership Regulation (PPP) on the capabilities building of the firm, i.e. how the Mexico-US fresh produce supply chain build up their capabilities to comply with the Customs-Trade Partnership Against Terrorism (CTPAT) guidelines. A reason for selecting this regulation, as will be shown in the background (i.e. Chapter 4), is that efforts

---

8 http://www.euractiv.com/en/print/cap/germany-investigates-criminal-origin-dioxin-contamination-news-501084, accessed on 11 January 2011. In the presentation of the case studies (SC2D) capability [18] shows the importance of preventing potential cross-contamination.

9 The author would argue that terrorism may include efforts to create terror simply due to misanthropy or malice as well as ideologically (e.g. Islamist extremism) efforts.

10 It is thought that Dalziel makes the most comprehensive account of intentional contaminations of the food supply chain, by injuries, fatalities, contaminants, segment of the supply chain where the contamination occurred, country and year, from 1950 to 2008.

to comply with the public and private regulations overlap to great extent with the Public-Private Partnership Regulation.

1.2. The US regulatory diffusion

Although CTPAT was designed for North Americans (Canada, US, and Mexico), a number of firms importing from the rest of the world into the US were invited by the CBP to voluntarily join CTPAT/FAST, including exporters and logistics providers.

Later, other initiatives around the world followed the US security systems. The European Union (EU) initiated similar regulations, including the Authorized Economic Operator Program (European Commission, 2005). The EU, US, and other countries are also pursuing mutual recognition of their supply chain security programmes (CBP, 2010). Following such initiatives, the World Customs Organisation (WCO) have invited all customs offices around the world to partner with business in increasing security to prevent any kind of terrorism activities throughout global supply chains (World Customs Organizations, 2007). Singapore, which is considered the most efficient port in the world in facilitating transit of goods (InSYNC, 2007), launched a similar security programme (Singapore Customs, 2007). As of January 2010, the CBP had signed four mutual recognition agreements like CTPAT, and was working on three more.

Table 1.2.1: US CBP mutual recognition agreements with foreign governments related to CTPAT

Signed	In negotiations
June 2007 – New Zealand Customs Service's Secure Export Scheme Program June 2007 – Jordan Customs Department's Golden List Program June 2008 – Canada Border Services Agency's Partners in Protection Program June 2009 – Japan Customs and Tariff Bureau's Authorized Economic Operator Program	Korean Customs – Authorized Economic Operator Program Singapore Customs – Secure Trade Partnership Plus Program European Union – Authorized Economic Operator Program

Source: www.CBP.gov

One interesting feature of this set of regulations is the focus on international supply chains rather than just single business units. This gives these regulations an inherently transnational flavour, as they impose a *de facto* responsibility on foreign nations to assist their businesses to develop the capacity to respond to the new security systems. Even though foreign national governments are not supposed to harmonise their regulatory regimes to those of the US, Mexican exporters sometimes request the State to support them to meet their regulatory commitments. An example of this will be shown in Section 5.5 of Chapter 5, the empirical chapter, which describes how one of the Mexican cases that was struggling with its capability building responded.

On the other hand, as of 2005, 18% of the firms applying for CTPAT certification had their application rejected. This suggests that they did not have, or were perceived not to have, the capabilities needed to secure their international supply chain. Furthermore, while the overall certified/rejected ratio in the programme was 3.8, this ratio was only 0.95 for Mexican organisations, which shows that more than half of the firms that applied were perceived to lack the capability to secure their supply chain (Rojas, 2005).

In light of the global diffusion of security regulations, questions arise about what has been the case for firms and supply chains in other developing countries that have been subject to the compliance requirements of the evolving global security regulatory regimes. The question has yet to be investigated. However, in this thesis a slightly different question is addressed: whether and how compliance capabilities are built.

Thus, the key issue in this dissertation is to understand how firms build up their capabilities, if at all, in order to meet the new biosecurity regulations. Equally important is to investigate the role played by the international supply chains in these processes, given the new scope of the regulation, CTPAT, which includes various stages of the supply chain, some of which may be located in different countries.

From the Mexico-US case, this investigation attempts to contribute to the Resource-Based View by incorporating compliance capabilities as another cause of competitive advantage.

1.3. Thesis structure

To reach that aim, this dissertation is structured as follows. After this introduction chapter, a second literature and theory chapter explores how various streams of literature have contributed to the understanding of the State's rationale and mechanisms to regulate businesses. It explores the ways businesses react to regulatory interventions, specifically in terms of developing and acquiring the resources and capabilities for compliance from the perspective of the Resource-Based View (RBV). Similarly, it explores the role international supply chains play in capability building from a Value Chain Governance (VCG) perspective. The chapter also briefly highlights the problems of previous contributions to the literature and attempts to disentangle the relationship between business regulation, compliance, and the role of supply chains. The chapter ends by putting forward a framework that integrates business regulation, capability building, and supply chain relationships, to contribute to better theoretical understanding of compliance-capability building.

The third, methodology, chapter formalises the questions and hypothesis driving the empirical investigation and describes the methodology and research design. The fourth, background, chapter describes the Mexico-US fresh produce supply chains and their evolution, highlighting the contribution made to the Mexican economy by international trade. It also describes the multiple stages of the Mexico-US supply chains and their operations, and the complexities of what the new security systems is attempting to regulate. The chapter concludes with a more detailed account of the characteristics of the BioAct 2002 and CTPAT/FAST.

The fifth chapter describes the 12 cases that comprise this comparative research. The comparative approach of the research design of the thesis means that all the case studies are structured in the same way. They first present the regulatory compliance processes: this is followed by the resources and capabilities developed by each firm, and finally the role of internal and external sources of knowledge for capability building (i.e. other stakeholders and supply chain partners).

The sixth chapter summarises all the cases, and provides an overview of the regulatory compliance processes, the resources and capabilities developed, and the supply chain relationships evolution during compliance. This chapter is intended to discover whether there was a 'model' for compliance or a diverse set of pathways that firms followed when they attempted to build up their compliance capabilities.

Based upon this qualitative comparative analysis, the thesis continues in Chapter 7 with the specific compliance processes, capability building and supply chain relationships that led towards compliance. Chapter 8 discusses the results. The main argument of the thesis is that firms overcoming the biosecurity and supply chain systems clash based on PPP regulation (i.e. CTPAT guidelines), do not follow a single compliance model. Instead, CTPAT compliant firms may follow a 'limited diversity of patterns' of compliance capability building processes. The chapter discusses previous contributions, and the extent to which the questions and hypotheses in the thesis were covered. To conclude, the thesis summarises the results and the discussion, and explores how the contributions of this dissertation helped to reach the aim of the investigation. The thesis ends with some policy and methodological recommendations for investigating the supply chain security.

2. CHAPTER 2 Theory and Framework: Understanding Compliance

This chapter summarises scholarly interpretations of the State's rationale to regulate businesses, why and how businesses comply, and the relationships that enable or constrain firms' collaboration with the State to achieve regulatory aims. It begins with a brief introduction to the history of Federal regulation in the United States, and a brief explanation of the theoretical models used to understand businesses compliance behaviour.

Although public and private sectors co-exist in the regulation, Braithwaite and Drahos (2000) have argued that global business regulation has been characterised by major shifts in who 'dominated' the regulation of the firms; in the 1800s-1930s it was business, in the 1940s-1970s, the State, and from the 1980s they have shared the responsibility, with steering in the hands of States, and rowing undertaken by businesses (Braithwaite & Drahos, 2000).

According to Rabin (1986), in the US social and economic concerns have changed over time, and this can be seen by the enactment of the main federal regulations. The first US Federal regulations were concerned with economic, industrial organisation and market conditions. For instance, the first US Federal regulation was in 1887, concerned with railway discriminatory market access. In the early 1900s a couple of unusual but very important regulations related to food safety were introduced. Transportation issues re-gained importance in the 1920s and in the 1930s economic recovery and market stability were very important. The social regulations related to safety again became important after the 1950s; and environmental concerns became the new agenda for the US in the 1970s. At the same time consumer safety regulations increased, all under a wave of economic, industry, and market deregulation (Rabin, 1986). In the 1980s, concerns related to terrorism and crime were expressed in the enactment of several Acts (HeinOnline, 2011; McLeish & Nightingale, 2007), some of which are listed below (see Table 2.1 below).

Business compliance and compliance behaviour studies have followed many approaches. Among others, key approaches are rule-based, regulatory studies, economic, sociological, institutional, evolutionary, organisation, and resource-based. According to Kingsbury (1997), approach is important because "compliance is not a free-standing concept, but derives meaning and utility from theories, so that different theories lead to significantly different notions of what is meant by compliance" (Kingsbury, 1997, p. 346).

Table 2.1: Selected Federal Regulations in the United States 1887-2006

Year	*Regulation – purpose*
1887	Interstate Commerce Act. Addressing issues of railroad abuse and discrimination
1889	Administrative Regulation (Alliance plan) - registration of public cooperatives
1890	Sherman Antitrust Act
1906	Pure Food and Drugs Act – Meat Inspection Act
1920	Transportation Act
1933	National Industry Recovery Act
1933-34	Security and Exchange Act (Stock issuances and transactions)
1935	Social Security Act; National Labor Relations Act
1938	Agricultural Adjustment Act
1946-50	Administrative procedure Act
1966	Automobile Safety Act
1967	Wholesome Meat Act
1970	Clean Air Act and Federal Water Pollution Control Act, National Environmental Policy Act, Endangered Species Act, Occupational Health and Safety Act; Crime control Act
1972	Consumer Product Safety Act (Trade and Consumer Safety)
1978	Airline Deregulation Act
1980	Motor Carrier Reform Act, Staggers Rail Act, Depository Institutions Deregulation and Monetary Control Act
1984	Act to combat terrorism; Cigarette Safety Act; Comprehensive Crime Control Act
1987	Water Quality Act; Medicare and Medicaid Patient and Program Protection Act
1988	Medical Waste Tracking Act; US - Canada Free-Trade Agreement Implementation Act
1990	Clean Air Act Amendments; Oil Pollution Act; Safe Medical Devices Act; Americans with Disabilities Act; Fire Safe Cigarette Act; Immigration Act
1991	Civil Rights Act; Solid Waste Disposal Act (amended)
1992	Energy Policy Act of 1992
1994	International Antitrust Enforcement Assistance Act; Marine Mammal Protection Act (Amendments); Violent Crime Control and Law Enforcement Act
1996	Iran and Libya Sanctions Act; Prison Litigation Reform Act; Antiterrorism and Effective Death Penalty Act; Illegal Immigration Reform and Immigrant Responsibility Act
2001	Uniting and Strengthening of America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
2002	Sarbanes-Oxley Act (Corporate Fraud Responsibility); Technology, Education and Copyright Harmonization Act; Homeland Security Act; Public Health Security and Bioterrorism Preparedness and Response Act
2005	Energy Policy Act
2006	Military Commissions Act

Source: Based on (HeinOnline, 2011; McLeish & Nightingale, 2007; Rabin, 1986)

Rule-based approaches, for example, do not lend themselves to our analyses because they focus on how legal rules and sanctions are set, and the assessment of compliance as the outcome (Kingsbury, 1997, p. 349). In spite of the importance of rules and their compliance outcomes, the rule-based approached do not explore how such outcomes are reached, i.e. the compliance processes. Moreover, rule-based approaches pay comparatively less attention to the relationship between the regulator and the regulated parties in a wider processes of compliance (Kingsbury, 1997, p. 349). In particular, studies in this field often assume that the firm will be able to comply, once it decides to do so. Although this is an incomplete perspective[11] it may offer some of the information needed to explain what happens within the firm in their consideration of compliance and attempts to comply.

The economics, psychological and sociological perspectives of compliance behaviour include analyses of the economics of detection and sanction (e.g. cost-benefit analysis) (Sutinen & Gauvin, 1989, p. 417). The economics perspectives suggest an increase in the size of a penalty to promote compliance; the psychological and sociological perspectives suggest that compliance is associated to the level of the individual's moral development and social influence on individual, which might be achieved through fair regulatory procedures and effective regulatory programmes (Kuperan & Sutinen, 1998, p. 325; Tyler, 2006, p. 165). Even though those elements may relate to conformity to norms, those contributions have been focused on analysing criminal deterrence rather than compliance; in other words deterring the terrorist rather than analysing how can firms prevent terrorist from using the firms' supply chain to make an attack.

The institutional approaches are interested in the arrangements of inspections to identify non-compliance, setting up liabilities, regulation by insurance, disclosures of activities of the regulated firm; public status to organised interest groups which serve as monitors, private party enforcers, incentives, contracting out regulatory functions, interests, commitment, coherence (Grabosky, 1995). However, these approaches mostly focus on institutional actors or instruments to promote compliance, rather than the internal processes by which firms and their supply chains might acquire the knowledge to comply. Although, disclosure may actually lead to self-awareness, learning and self-correction for compliance, it had not been analysed from the firms' side.

The evolutionary approach is appealing for this thesis. It focuses on units of selection (e.g. capabilities), selection mechanisms (e.g. regulations and markets), adaptation (e.g. capabilities transformation) and variation (e.g. innovation) (Dosi & Nelson, 1994, p. 155). Although it will be useful to describe how each firm responded to regulations, as will be shown in thesis, for the regulations we are analysing, there is no change in the selection

[11] The gap between theory and practice here may reflect the common assumption in economics of 'perfect information' in which all techniques that might be employed by the firm are readily available although they may differ in cost. That a firm would choose not to comply is therefore implicitly a conclusion that non-compliance is less expensive than compliance. If, however, it is recognised that firms may require time and investment to gather and co-ordinate the skills and tools needed for compliance, immediate compliance cannot be seen as possible nor can non-compliance be seen as a choice.

mechanisms, they will be given. Therefore, there is not much methodological ground to assess a co-evolution between the biosecurity regulations and capabilities building.

Thus, the two main approaches used in this thesis to understand compliance from the point of view of the firm are organisation theories (e.g. French, Neighbors, Carswell, Williams, & Bush, 1992; Henson & Heasman, 1998; Sproull, 1981) and the resource-based view RBV (e.g. Hart, 1995; Penrose, 1955; Rugman & Verbeke, 1998; Teece & Pisano, 1994; von Tunzelmann & Wang, 2003; Wernerfelt, 1984). These approaches aid our understanding of the processes by which firms reach compliance, and the capabilities required to do so, thus, being able to give insights to regulatory scholars on the importance of understanding the firms behaviour. The RBV is also taken to understand whether firms are able to gain competitive advantage out of compliance.

The chapter shows that although scholars from regulatory studies[12], innovation studies[13], and supply chain governance[14] have been interested in business compliance, individually they have been limited in explaining how firms manage comply, and even less on the role of their supply chain partners, taking into account that, as will be shown later, security regulations not only expect compliance from single firms, but also from their supply chains partners.

Therefore, this review focuses on understanding three elements: 1) the compliance processes, 2) the resources and capabilities of the firm for compliance, and 3) the supply chain partners' role for compliance. After exploring these elements, a framework integrating business regulation, capability building, and supply chain relationships[15] is presented.

[12] (Baldwin & Black, 2007; Braithwaite & Drahos, 2000; Christmann & Taylor, 2005; Parker, 2000; Viscusi, Vernon, & Harrignton, 1995; Yapp & Fairman, 2006).

[13] (Ashford, Heaton, & Priest, 1979; Buysse & Verbeke, 2003; Delmas, 1999; Delmas & Toffel, 2008; Porter & van der Linde, 1995; Rugman & Verbeke, 1998; Williams & Edge, 1996)

[14] (Cousins, Lamming, & Bowen, 2004; Delmas, 1999; Garcia-Martinez, Fearne, Caswell, & Henson, 2007; Gereffi, Humphrey, & Sturgeon, 2005; Henson & Heasman, 1998; Phillips, Lamming, Bessant, & Noke, 2006; Teece, 1986)

[15] Although related literatures such as transaction costs, governance structures, and value chain governance are included in the analysis, they are only used instrumentally for the understanding of the external sources of knowledge of the firm, and we are not expecting to make theoretical contributions in this area.

2.1. Regulations: public, private, and public-private partnership

Public and private regulations

Regulations allow society, in the form of the State and other stakeholders, to shape human behaviour to achieve social aims. This can involve preventing or correcting undesirable outcomes of social, economic and political processes using markets[16], contracts, rules, and so on (Baldwin, Schott, & Hood, 1998). According to Black (2010, p. 302), regulations are forms of managing risks (on life and health), and beyond the State (with organisations in general) managing risk has become a benchmark of good governance.

The ways regulations are enforced vary according to who sets them. Private regulations may be set up in business contracts requiring to related firms to acquire or work on acquiring certifiable standards issued by third party certifying agencies (Christmann & Taylor, 2005), however, standards need not to be necessarily certifiable. The case above, as well as regulations set for the firm itself, is a case of self-regulations. Public regulations set up laws requiring firms with given characteristics to acquire standards issued by the State, and usually verifiable by a public agency, and infringement may incur penalties (Kitching, 2006, p. 801). The case above is a case of command-control regulation.

To prevent or correct undesirable risks to life and health, the evidence suggests relying on free markets and deregulation as regulatory policy may lead to undesirable outcomes (Sunstein, 1997, p. 9). Scheppele (1988) explains that under free markets, *caveat emptor* generally applies, as sellers know little about the products that pass through their hands, and buyers have more opportunity to inspect products, and not taking advantage of this makes them liable, but when the seller and the buyer are equally ignorant, the loss stays where it finally fell (Scheppele, 1988, p. 283), presumably more often on the consumer or civil society. Hence free markets may give incentives to sellers to remain ignorant about the

[16] Markets depend on law for their existence, and the system of private property only exists with legal rules telling who owns what, penalties for trespassing, and saying who can do what to whom (Sunstein, 1997).

risks and defects of the products they are selling, lowering the possibilities of a law suit, and therefore not having the need to self-regulate[17].

Governments may try to mind such market failures with public regulations (Tran & Daim, 2008), forcing the development or implementation of the best available technologies – and specific capabilities – at rates or directions that were not expected to be initiated by firms otherwise (Schot & Rip, 1996, pp. 259-261). These regulations have been also called Constructive Technology Assessment (Schot & Rip, 1996; van Merkerk & Smits, 2008), Technology Assessment (Guston & Sarewitz, 2002), Anticipatory Governance (Philbrick, 2010), Social Shaping and Construction of Technology (Pinch & Bijker, 1984; Williams & Edge, 1996), and they are applied to areas such as environmental protection (Kemp, 2000, p. 35), auto safety and systems (Fleischman, 2001; M. Lee, T., 1998; Schot, Hoogman, & Elzen, 1994), occupational health and safety (Parashes, 1978, p. 55), and so on.

There are criticisms to public regulations on various grounds. First, technology forcing relies on a strong sense of technological determinism/imperatives, as, for instance, assuming that the rate, nature and direction of technological change is not problematic, can be determined, and produces social and organisational change (Williams & Edge, 1996, p. 868); as if technology could be forecasted as a demonstrated fact, rather than as a speculative possibility. Second, public regulations may lack enforcement capacity in geographically dispersed firms (Bednar, 2006, pp. 368-369; Boyd, 1998, pp. 2, 31-32). Thirdly, they tend to limit pro-active compliance by driving firms to not doing more than what is being dictated. This seems to be a reason behind environmentalists' pressuring businesses to adopt and implement environmental practices going beyond the dictates of statues and regulations (Stenzel, 2000, p. 243). Fourth, public agencies may lack the knowledge of the technological capabilities, options, and availabilities to be implemented by the industry, at the time they are setting up regulatory standards (Majone, 2002, p. 89). And fifth, precautionary principles applied to risk management in public regulations may be misused to justify protectionist measures, with undesirable distributive consequences (Majone, 2002, p. 89). Although, according to Kaufman (2007), security policies inheritably

---

[17] See for instance a case of health care services, where the consumers preferred to remain in a state of ignorance, and not devote efforts to actively seeking out information about their doctor or evaluating his or her services (Lupton, Donaldson, & Lloyd, 1991, p. 567).

create trade obstacles, the concern is how international trade can be enhanced given the new security policies (Kaufman, 2007, p. 641).

Yet, as in the case of the regulations for preventing the depletion of the ozone layer (Andersen, Sarma, & Sinclair, 2002, p. 265), unclear final consumer messages for security and uncoordinated efforts by suppliers to engage in biosecurity self-regulations, gives importance to comprehensive and universal regulation to avoid coordination and market failures.

There are instances actually in which firms and their associations try to control their own behaviour with private regulations. For instance in Mexico and the US, supermarkets define quality and food safety standards for their food suppliers (Calvin & Barrios, 1999; Dolan & Humphrey, 2000; Reardon, 2006; Reardon, Henson, & Berdegue, 2007).

Criticisms on private regulations focus on the effectiveness to achieve desirable social aims (Garcia-Martinez, Fearne, Caswell, & Henson, 2007, p. 300), to ensure public accountability (Bartle & Vass, 2007, p. 897), and the issue of the capacity and incentives to identify and control risks, because this requires the knowledge not only of the costs of reducing the risks, but of the probability and severity of them (Shavell, 1983, p. 359). Although private parties may know more than regulators about the costs of specific activities in their firms to reduce risks, it is unlikely that the fresh produce industry know more about the probability and severity of the risks of bioterrorism than regulators.

Although regulations exist, one should not expect perfect compliance. Compliance can be costly for the firm (Froud & Ogus, 1996), and monitoring and enforcement may neither be easy nor cheap (Parker, 2000, p. 560). Regulatory enforcement of any type (public or private) tends to be imperfect (Farina, Gutman, Lavarello, Nunes, & Reardon, 2005, p.306; North, 1995, p.95; Viscusi, Vernon, & Harrignton, 1995, p.819), making perfect compliance unlikely.

A wrong-doing firms, is one lacking the efforts to continuously enhance compliance rather than one not eliminating risks. Stuart (2008) argues that total control over food safety may be just an illusion, despite the new technologies and the war against nature (Stuart, 2008), or despite measures to prevent human frustrations vented over food. But, firms should be monitored and given penalties to discourage non-compliance and rewards to incentivise voluntary compliance (OECD, 2000, pp. 55-56).

From the point of view of the firm, some of the benefits of private regulation are: 1) it limits competition and promotes sectoral interests, 2) it helps to pre-empt public regulation, and 3) it informs consumers of the quality (and safety and security) provisions of the suppliers; but 4) it mostly involves gaining reputational capital or reducing the risk of reputational damage (Nunez, 2007, pp. 211-212) by means of terminating business relations with non-compliant firms (Meidinger, 2006, p. 75; Raynaud et al., 2005, p. 50).

Private regulations are useful instruments when formal obligations and public regulations are absent or ineffectively enforced (Busch, Jorgens, & Tews, 2005, p. 147). Furthermore, even when compulsory statutory regulations are present and effectively enforced, they may still not be sufficient to achieve social aims (OECD, 2000, pp. 7, 11). So, what are the alternatives?

Public-Private Partnership Regulations

Although the traditional view of regulation is that the State should legislate, execute, and enforce compliance[18], in the food industry at least, many roles are actually shared between the State and the private sector (Iizuka & Borbon-Galvez, 2009; Meidinger, 2009), and this is the main idea behind a Public-Private Partnership Regulation.

Public-private partnership regulations (PPPs) have been set up to cover aspects not considered individually by private and public regulations. Achieving regulatory aims, responding to consumer needs, assuring non-discriminatory conditions, effectively achieving social aims with fewer burdens are some of those aspects (Garcia-Martinez et al., 2007, pp. 301, 312), allowing for some form of accountability, and preventing rent-seeking behaviours (Ogus, 1995, p. 98). Yet, Baldwin and Black (2008) warn that complex and uncertain regulations may hinder compliance (Baldwin & Black, 2008, p. 63), which may be the case of PPPs.

[18] The private sector may face severe challenges of impartiality when enforcing locally and legitimating internationally their own developed regulations and certifications (C-TPAT/CBP, 2010, p. 6).

PPPs evolved on the one hand by handing public regulatory functions over private sectors, for instance the regulatory enforcement functions (Wigger & Nolke, 2007, p. 488). In the agri-food supply chain chains some of the reasons behind such substitutions had been: 1) lack of direct State supervision in supplying countries, 2) increasing use of private standards as tools to coordinate internationally dispersed suppliers, 3) to manage risk (Berdegue, Balsevich, Flores, & Reardon, 2005, p. 259; Reardon, 2006; Tallontire, 2007, p. 776), 4) better monitoring systems that reduce the overall chains' transactions costs (Delmas & Toffel, 2008, p. 1035; Muradian & Pelupessy, 2005, p. 2032), and 5) due to the rapid obsolescence of public regulations after industry transformations (McInerney, 2007, p. 183).

PPPs also evolved by taking private regulations as the model for setting up public regulations, but with private standards setting organisations remaining private. States' reasons behind may this may include: 1) the need for universal compliance, 2) need of governmental accountability, 3) need to adhere to international trade rules (Aruoma, 2006, p. 123), need to comply with international agreements and control regimes (Smith & Crotty, 2008, p. 343). There are examples of this in the agrifood sector (Hutter, 1993, p. 238; Iizuka & Borbon-Galvez, 2009, pp. 12-13).

PPPs had also emerged by means of States mandating the creation of standards by the private sector. The UK 1990 Food Safety Act mandated operators in the food industry to exercise 'due diligence' over supply chains delivering to ensure safe food, which has driven firms to develop a series of food safety measures along their global supply chains (Henson & Humphrey, 2009, p. 11), which indicates the case of command-control regulations with private standards with presence of both private and public enforcement mechanisms, the former by firms' due diligence, and the second by governments' public enforcement.

A comprehensive literature survey by Henson and Humphrey (2009) concludes that the difference between public and private regulations may be explained by the fact that governments are interested in meeting public expectations, while the private sector may be interested in meeting customer needs, or reacting to public interventions that affect the competitive advantage of the firm[19] (Henson & Humphrey, 2009). This would have not

---

[19] Henson and Humphrey (2009) present a comprehensive debate and discussion of the increasing importance of private regulations in preventing the contamination of the food supply chain (food safety

been a problem if the private as much as the public regulation was accountable not only to the buyers, but to all the population in terms of human protection and fair trade, or as Yapp and Fairman (2006) argue, if there was not regulatory competition; because to meet regulatory aims, firms require resources and capabilities that adhere to the norms (Yapp & Fairman, 2006, p. 44).

Thus, under the risk of 1) negative effects on economic growth as a direct consequence of public regulations set by unknowledgeable public agencies, and 2) business discrimination as a consequence of self-regulation that are set by opportunistic and rent-seeking private parties, public rule-making with informal discussion, negotiation, consensus, and with multiple institutions involvement appears to be more effective (Braun & Wield, 1994, p. 270; Stewart, 1981, pp. 1346-1347; Viscusi, 1988, p. 304). This, of course, assumes that the private sector is represented among the institutions involved in the regulatory design and standards setting, which then would mean that such regulations are Public-Private Partnerships Regulations (PPPs).

The Customs-Trade Partnership Against Terrorism (CTPAT) is a PPP, which combines public and private regulatory characteristics such as: a) duty payments and electronic transmission of cargo before importing through the Advanced Commercial Information-ACI (non-compulsory features are administered by the US Customs Border Protection-CBP); the system is managed by Prior Notice of Food Import Shipments (which has command-control features and is administered by the US Food and Drug Administration-FDA); and b) reduced cargo inspections as incentives for good security records in cross-border operations (a non-compulsory feature of CTPAT that is administered by CBP) (C-TPAT/CBP, 2006, p. 7; FDA/HHS, 2009, p. 4). Furthermore, it was designed by public (i.e. Customs Border Protection) and private organisations (i.e. 50 international trade experts) representing most stages of the supply chains (Laden, 2007, p. 76)[20].

standards), and its use as a Non-Tariff Barrier to trade, the argument is that it is not completely clear whether private regulations distort trade, and public regulation should find the ways to adapt to the sector and local conditions of the food supply chain (Iizuka & Borbon-Galvez, 2009).

[20] CTPAT requires that firms adopt, adapt or develop resources that prevent terrorism such as safe firm relationships, physical security, access control, personnel security, procedural security, information systems, trailers and containers security, conveyance security, security training and awareness (Henson & Humphrey, 2009).

Yet, since the question is whether firms are able to comply with CTPAT, it is necessary to explore the other side of the regulatory story: the firms' compliance processes.

Regulatory Compliance

Regulatory scholars generally consider that "non-compliance is, first of all, a violation of the law" (Lai, Yung, Li, & Ho, 2007, p. 539). Such violations may be due to lack of: 1) enforcement capacity, 2) rewards systems, 3) organisational expectations of regulatory benefits, or 4) adequate institutional arrangements, or management tactics opening up planning legislation to the public and stakeholders.

There are however regulatory scholars interested from the 'responsive regulations' strand that have transcended the above view, acknowledging the importance of resources, competencies, capabilities, operational and cognitive frameworks of the firms such as Parker (2006), Nielsen & Parker (2008), and Baldwin and Black (2008).

According to Yapp and Fairman (2006), compliance with a regulation requires technologies, procedures, systems and capabilities that enable the firm to adhere to the regulation's norms (Yapp & Fairman, 2006, p. 44), and they need to be available at the precise moment they are required (Williams & Edge, 1996, p. 873). Moreover, it is possible for early movers in allocating resources to gain advantage for achieving compliance, according to Ashford et al., (1979) and Porter and van der Linde (1995), raising resource barriers (Wernerfelt, 1984), i.e. the limited resources already allocated (e.g. specialised human resources already hired exclusively to manage compliance in a given firm).

Yet again, responsive regulation scholars believe that allocating resources for compliance will depend mainly on the hegemony, power, and legitimacy of the regulation (Braithwaite & Drahos, 2000, p. 398; Scott, 1987, p. 451), and of a clear understanding by the regulated of 'who' is ruling 'what' (Baldwin & Black, 2008, p. 63).

This suggests that regulatory compliance depends on the regulatory design, which drives the allocation of resources and capabilities for compliance. It is then necessary understanding what had scholars discussed about how capabilities and resources can contribute to the firm to become compliant. For this enterprise we mainly rely on the Resource-Based View scholars.

2.2. A Resource-Based View of Compliance

The introduction chapter discussed that security often requires the 'engagement' of the private sector. But understanding how firms can engage (comply), requires as suggested by 'responsive regulation' scholars, understanding the role of capabilities, resources, and organisational processes to become compliant. And first of all, to clarify how capabilities and resources relate to compliance, we need to understand what are they, how are they built, and how can they meet regulations?

Compliance capabilities

The Resource-Based View (RBV) scholars have spent a long time around what capabilities are, how they are built, and how they can sustain the competitive advantage of the firms (Barney, 1991; Hart, 1995; Helfat & Peteraf, 2003; Penrose, 1955; Rugman & Verbeke, 1998; Teece & Pisano, 1994; von Tunzelmann & Wang, 2003; Wernerfelt, 1984; Winter, 2000).

A capability is "a high-level routine (or collection of routines) that, together with its implementing input flows, confers upon an organization's management a set of decision options for producing significant outputs of a particular type ... 'routine' is a behaviour that is learned, highly patterned, repetitious, or quasi-repetitious, founded in part in tacit knowledge ... and in the specificity of objectives" (Winter, 2000, p. 983). Competitive advantage is defined as "implementing a value creating strategy not simultaneously being implemented by any current or potential competitor. It is sustained ... when other firms are unable to duplicate the benefits of this strategy" (Barney, 1991, p. 102).

Delmas and Toffel (2008) have shown that nonmarket pressures – i.e. regulations – are usually channelled throughout firm's legal departments, which later may influence other firm managers, taking the form of direct control over the decision making, or indirectly through information sharing and training; later with the help of marketing – and other managers – firms may be able to convey such nonmarket management decisions into firm's competitiveness (Delmas & Toffel, 2008, pp. 1032-1033). However, turning external pressures into internal decision making processes, learning, innovating, and conveying those by managers into the firm's competitiveness, may require skills, experience, knowledge, technologies and systems; or what had been broadly called capabilities (Langlois & Robertson, 1993, p. 35; Nightingale, 2004, p. 1273; Song, Droge, Hanvanich, & Calantone, 2005, pp. 260-261). When these capabilities respond to external pressures of regulatory nature, they should be called **compliance capabilities** hereafter.

In this line of argument, Fermeth (2009) showed how the decision to comply by US electric utilities exposed to environmental regulations depends on the capabilities and their redeployment or development to meet externally established objectives – i.e. Regulations (Fremeth, 2009, p. 90).

To comply with safety and traceability regulations, firms complemented new radio frequency identification (RFID) technologies with operations optimisation of all stages of the their supply chains (Jones, Clarke-Hill, Comfort, Hillier, & Shears, 2005).

New organisational (Johannessen, 2008, p. 409) and administrative capabilities (Yamin, Mavondo, Gunasekaran, & Sarros, 1997, p. 166) have been complemented with technologies and systems for compliance. For instance, as the US Environment Protection Agency (US EPA) banned the ethylene dibromide and approved the hot water treatment for fruit flies in mangos, new and complex organisational capabilities such as engineering protocols, machinery and plant designs, logistical operations, and coordination between public agencies and Mexican mango exporters, were integrated with information and communication technologies, and biotechnologies (biological analysis and control technologies), etc. These organisational capabilities, together with the new technologies, have liberalised Mexican mango exporters and other fruit exporters from intra-regional trade, and allowed them to exploit global markets (Alvarez, 2001, p. 125).

According to Fremeth, when compliance capabilities are similar to those existing within the firm, firms may only need to be redeployed capabilities from previous uses to compliance (Fremeth, 2009, p. 91). This implies that when capabilities for compliance are dissimilar to the existing within the firm, it might be necessary to develop them or, if possible, source them from outside the firm.

External compliance capabilities

According to Lamm (1997), it is not uncommon that small firms have difficulties to comply. In the United Kingdom such firms required compliance expertise on occupational health and safety, which was usually sourced from outside non-governmental actors and organisations (Lamm, 1997, p. 156). According to Drew (2007) not only small but any firms may need external expertise (experience) to assess and approach risks and compliance (Drew, 2007, p. 23). For instance, SMEs with environmental problems, and without sufficient internal capabilities to comply with regulations, have used external expertise to refocus existing capacity to environmental compliance, adapting existing organisational structures, procedures and recording systems (Perez Sanchez, Barton, & Bower, 2003, p. 74).

Furthermore, even though firms could develop capabilities internally, it is not rare for their development costs, i.e. search, planning, negotiating, monitoring, and enforcement, to be too high. When they are able to have control over capabilities developed externally, it is more economical to outsource their development and merge internal capabilities of the firm with the outsourced skills, routines and capabilities (Blomqvist, Kyläheiko, & Virolainen, 2002, pp. 7-8). However, to reduce the risks of control loss and knowledge spillovers to competitors (Premus & Sanders, 2003, p. 53), in-site outsourcing (transfer of property without relocation of operations) is usually preferred over near-site (transfer of property with relocation of operations to near sites) or off-shore outsourcing (transfer of property with off-shore relocation of operations). Overall, outsourcing happens because suppliers are able to provide products or services at lower cost than the firm is able internally (Strange, 2009).

Carlson and Fernandes (2006) suggest that large firms also need a great deal of external support for their capabilities to comply with regulations. They have had to increase considerably the share of outside resources in the overall compliance efforts, because of the difficulties in expanding internal compliance support fast enough, to be able to initiate activities not related to compliance, e.g. developing new products and services, to acquire IT systems, new personnel and other compliance activities: in some instances they are not even suitable to the compliance activities. The opportunity costs of these compliance trends included shifted management focus, disrupted provision of products and services, and waiting times (Carlson & Fernandez, 2006, p. 8).

Hence, it is still not clear whether firm size correlates with compliance capabilities (Aragón-Correa, Hurtado-Torres, Sharma, & García-Morales, 2008, p. 93), regardless of what some scholars may argue (Lynch-Wood & Williamson, 2010).

Compliance capabilities and firm performance

Compliance capabilities may have positive effects on various areas of firm performance. Chinander et al. (1998) regulations trigger R&D activities, human resources development, and organisational transformations for the execution of compliance activities; later, the assessment of compliance drove changes in the development strategy of the firm, by modifying product, processes and market strategies (Chinander, Kleindorfer, & Kunreuther, 1998, p. 137).

In response to regulations, when required changes are identified, Hart (1995) showed that compliance drove drive firms to either introduce end-of-pipe technologies or processes and organisational changes. To various degrees, these capabilities influenced the productive capacity and technologies and systems of the firm, eliminating unnecessary and simplifying steps in the production operation. Firms, after compliance saw positive revenues, profits, business relations, and markets of the firms (Hart, 1995, pp. 992-998).

Similarly, Ashford, Heaton and Priest (1979) showed how although building up technological capabilities for compliance represents a burden for the firm, those capabilities may help offset the burden. Based on a case study of vinyl chloride "regulations" enforced by the United States Occupational Safety and Health Administration (OSHA), they showed a series of innovations following compliance capabilities, including improved product developments exceeding the long run costs of compliance for the industry (Ashford et al., 1979, p. 180).

Porter and van der Linde (1995) described cases of organisational innovations that would have not existed without compliance to regulatory pressures. One was the Molten Metal Technology which developed a process (organisational capability) for hazardous waste that reduced the cost of compliance. Another case was the Robbins Company, which developed a new handling and purification system of water used for plating, with results over 40 times cleaner than the city water, increasing the competitiveness of the firm (Porter & van der Linde, 1995, p. 101).

Dewick and Miozzo in 2002 showed that building regulations in Sweden, the Netherlands and Germany were stricter than in the UK, contributing to higher material and labour costs. However, the technologies and economies of learning derived from compliance with stricter regulations contributed to making the total building costs lower than those in UK (Dewick & Miozzo, 2002, p. 826).

To sum up, although compliance may be a burden for firms, compliance leadership in some instance may lead to better firm performance. The question is how are capabilities for compliance built?

Compliance capability building process

As noticed earlier, firm' compliance had been subject of regulatory studies (Aruoma, 2006; Crotty, 2006; Froud & Ogus, 1996; Grabowski, Viscusi, & Evans, 1989; James, Johnstone, Quinlan, & Walters, 2007; Millstone, 1994; Nicholas Hughes, 2006; Parker, 2000; Smith & Crotty, 2008; Viscusi, 1979). However, they mostly focused on the regulation as a cause and the firm's output (innovation, increased efficiency, market exit, so on) as an effect, leaving the middle-ground unstudied. Hence, the processes by which firms achieved or not compliance have typically remained "black boxed".

The following sections review the key contributions on compliance capability building, like Ashford, Heaton and Priest (1979) from a technological change point of view, Scott (1981) from an institutional perspective, and Henson and Heasman (1998) from an organisational perspective have advanced understanding of firm's compliance. Later, based upon the RBV contributions, the review explores how the skills and capabilities required for compliance, if innovative, may be difficult to acquire, develop, or mobilise (Porter & van der Linde, 1995). This can be a criticism to Ashford et al. (1979) Scott (1981) and Henson and Heasman (1998) who assume the availability and readiness of resources and capabilities at each stage of a compliance process.

The RBV touches upon issues of compliance, assembled into a framework that tries to clarify the relationships between regulations, compliance, and intra and inter firm learning (Buysse & Verbeke, 2003; Delmas, 1999; Delmas & Toffel, 2008; Pilkington, 1998; Rugman & Verbeke, 1998; Williams & Edge, 1996). The next sections are organised as follows, 1) compliance processes, 2) capability building, and 3) supply chain relationships, and finish by presenting the analytical framework connecting the three elements with the regulatory regimes.

The compliance process

Ashford, Heaton and Priest (1979) show that the first activity of the firm for compliance is allocating resources, initially diverting them from other business and R&D activities to create compliance departments, involving dedicated personnel, financial resources and time. The allocation of resources increases according to the desired level of **compliance leadership**.

Later, Sproull (1981) proposed so analyse compliance as an organisational process, consisting of the following stages: 1) identify regulations, 2) perceive and interpret regulations, 3) investigate the internal organisational context looking for plausible responses (ability to comply), 4) decide to comply[21], 5) communicate compliance strategies, and, finally, 6) assess conformance to the regulatory requirements (Sproull, 1981).

Like Ashford, she stressed the internal struggles for attracting the resources and capabilities for each stage of the compliance process. She however, did not question whether: 1) resources and capabilities were unavailable, and 2) deployment of resources and capabilities across the organisation in some and not all instances meet the regulatory requirements.

---

[21] Internal organisation competition for resources and whether to avoiding certain resources from the repertoire, adding resources from the repertoire, or resources from the repertoire to the pre-existing business operations).

Scott (1987) acknowledged that resources and capabilities – as roles and functions within the firm – may not be available nor meet the regulatory requirements. For him, organisations need to create structures according to their complex environments, adapting, creating and embedding functions and roles in their structures as their environments change. Eventually, the whole organisational structure of the firm reflects the patterns of the strategic contingencies to meet the regulatory changes (Scott, 1987).

The problems with such view are: 1) the an assumption that regulations are fully met, implying that organisational structures and activities are fully developed by the time another regulatory change appears; 2) the little consideration given to the fact that firms may pre-empt their regulatory environment change, hence their organisational structure may not fully reflect or meet regulatory changes[22]; and 3) there is limited insight of how resources and capabilities get developed and deployed across organisations, mainly due to the contingent approach, it would not make sense identifying patterns of development.

French *et al.* (1992) and Henson and Heasman (1998) refined Sproull's compliance process and applied it to the food industry in response to food safety and labelling regulations. The general compliance model follows the following stages (French et al., 1992; Henson & Heasman, 1998):

1. Identifying the regulation, awareness;
2. Interpreting the regulation;
3. Identify the degree of compliance prior to implementation to estimate required changes;
4. Deciding the desired level of compliance (exit to partial to full compliance) in the function of the apparent direct compliance costs;
5. Search of the methods or alternatives for compliance and allocation of resources for assessment and implementation;
6. Communicating the compliance decision, strategies, and implications it has for the whole organisation;
7. Implementation of changes at technological and organisational level;

[22] For instance, from a survey of C-TPAT members ordered by CBP, only 4.7% of the businesses had not had any of the security criteria, while the rest of the businesses have implemented at least to some extent the security criteria (CTPAT/CBP, 2006).

8. Allocation of resources for monitoring and evaluation of the compliance process.

This approach acknowledges feedback loops to each of the stages of the process. However, the fundamental difference of Henson and Heasman's model compared to previous ones is the role of resources availability – financial and human – in their analysis. Their study concluded that the main factor contributing to compliance was firm size, rooted in the economies of scale that financial resources and staff time has over the compliance processes; and nothing can be said regarding the organisational compliance processes, or whether differences in those had an impact on compliance. They added that regardless of their technological and organisational capabilities, smaller firms tend to follow partial or non-compliance strategies, while larger firms follow full compliance strategies (Henson & Heasman, 1998, p. 20).

Similarly, the US federal government, through the Sentencing Commission, Guidelines Manual §3E1.1 (November 2009) ruled that *all firms* must exercise due diligence and promote an organisational culture of prevention and detection of crime. However, a compliance programme may vary according to the size of the firm. Large organisations should have more formal operations and greater resources than small organisations. Large organisations should also encourage small organisations (those related or seeking to have business relations with large organisations) to implement effective compliance programmes (USSG, nov. 2009, p. 506). The elements of a compliance model for all firms in the US are (USSG, nov. 2009, p. 503):

1. Standards and procedures to prevent and detect criminal conduct;
2. Knowledge from the organisation's governing authority about the compliance programme, and top level personnel engaged in it;
3. No responsibility given to high-risk persons;
4. Effective communication of standards and procedures: training programmes and/or disseminating information;
5. Monitoring and auditing, evaluating, and publicising systems of the programme;
6. Compliance programme shall include incentives and disciplinary measures;
7. Detection should be followed by response, and corrections of the compliance programmes.

Thus, based on Henson and Heasman (1998) and the US Federal Sentencing Commission Guidelines Manual §3E1.1 (November 2009), it seems that compliance requires only a great deal of resources; hence large firms with more financial and human resources tend to comply whereas small firms, lacking those resources, will comply much less often or effectively. However, in one of the cases in Henson and Heasman's study, a multiple retailer (presumably a large firm), who declared, after trying to pre-empt a UK food safety regulation, it lost millions when the state modified the rules and resulted in the firm being non-compliant (Henson & Heasman, 1998, p. 19). Even large firms may not be able to comply, adding to the open debate of the relationship between firm size and compliance; hence. Hence, it seems that it has to do with accumulation of resources and capabilities. The question then is, how those capabilities and resources are build?

The resource and capability building

> *"Scholars who identify themselves with the "Resource-Based View" examine the question of what sort of resources confer lasting competitive advantages, how these advantages can be extended, and what considerations prevent the elimination of the gap between the costs of the resources and the market value of the output produced" (Dosi, Faillo, & Marengo, 2008, p. 19).*

To understand what resources and capabilities are required for compliance, it is necessary to know how they are built and their relationship with firm performance. This takes us back to Penrose (1955).

Penrose was concerned with the limits on the growth of firms in the 1950s. She suggested that these limits were given by the firm's internal resources: experiences, skills, and technological know-how related to internal operations (Penrose, 1956, p. 225). These resources may be combined to form capabilities, and the most important capabilities are research and planning, managerial services, and the ability to re-interpret and understand their own resources. Resources and capabilities are not homogeneous (e.g. fixed and variable capital and assets), instead they are heterogeneous (e.g. skills, technologies, knowledge, managerial services, etc.), yet valuable and conducive of unlimited growth, as long as the span of control allows it (Penrose, 1955, pp. 532-533, 537, 540, 1960, p. 19). Hence, if resources and capabilities are available a firm will be able to comply.

Later, Wernerfelt (1984) contested Penrose's view on the limits of growth of the firm, because, even if available, resources were not easy to acquire in the marketplace, they may be difficult to imitate, substitute, or move: this means that there are resource barriers (Wernerfelt, 1984, p. 173).

Yet, Wernerfelt (1984) it also goes down to availability of resources and capabilities, developed or acquired. Then, we wonder if upon availability of capabilities and resources, a firm will be always able to comply. If not, then what else apart from resources and capabilities availability is needed?

Wernerfelt however, did mentioned that firms may follow acquisition strategies to get resources that 'combines effectively' with those of the firm (Wernerfelt, 1984, p. 175). Similarly, Pilkington (1998) argued that radical regulations, those that require technologies that are beyond the operating region of the firm, may drive them into joint-ventures or take-overs (Pilkington, 1998, p. 213) to acquire the necessary resources to combine and combine them with the existing ones. This implies the risk of vertical integration to after regulatory pressures.

However, Wernerfelt (1984) and Pilkington (1998) did not explain how those internal and external resources were developed or how they may be combined to achieve compliance. For instance, at this point it is unclear why, by 2005, 18.5% of the firms that developed resources and built up capabilities to comply with CTPAT had their applications rejected (Rojas, 2005), and why by the end of 2008, 7.4% of the applications were rejected (COAC/CBP, 2008).

Resources and capabilities

According to Dosi, Faillo and Marengo (2008) resources are 'things' while capabilities are 'ways of doing' things (Dosi et al., 2008, p. 11). Further, "capabilities fill the gap between intention and outcome, and they fill it in such a way that the outcome bears a definite resemblance to what was intended" (Dosi, Nelson, & Winter, 2000, p. 2).

Resources (things) constitute brand names, skilled personnel, physical technologies, assets, inputs to production, institutional structures and institutional linkages, etc. (Bell & Pavitt, 1995; Eisenhardt & Martin, 2000; Helfat & Peteraf, 2003; Maijoor & Van Witteloostuijn, 1996; Nightingale, 2004; Prieto & Easterby-Smith, 2006; Wernerfelt, 1984).

Capabilities (ways of doing) on the other hand constitute acquisitions, researching, experimentation, planning, designing, preventing, developing, coordinating, learning by doing, predicting, reconfiguring, etc., of resources (things) (Hart, 1995; Kogut & Zander, 1996; Nightingale, 2004; Penrose, 1955, 1956, 1960; Zhou, Zhang, & Liu, 2005; Zollo & Winter, 2002).

In other words, firms' intention to comply may trigger the collection of *input resources* (such as skilled personnel, physical technologies, inputs to production, assets, software, and so on), to build up *capabilities* (such as researching, learning by doing, coordinating, reconfiguring, etc.), which in turn sets the options and implements the creation of *output resources and products*, such as new security systems and technologies. These output resources and products should resemble the firm's intention to comply.

Capability building

According to Hoopes and Madsen (2008), there are broadly four areas related to how capabilities are built up, or what input resources are collected for:

1) Intra-firm capability replication, i.e. **managerial systems**[23] (internal capability building), and intra-firm capability imitation, i.e. **organisational competencies and capabilities** (internal capability building) (Hoopes & Madsen, 2008, p. 400; Pettus, Kor, & Mahoney, 2009, p. 189; Winter & Szulanski, 2001, pp. 733-734);

2) Capability integration, i.e. **internal coordination** (internal capability building) (Hoopes & Madsen, 2008, p. 403; Kogut & Zander, 1992, p. 388; McInerney, 2004, p. 193);

3) Capability creation. Intra-firm capability creation based upon leadership, organisational culture, information technology, social networks, skills, know-how, etc., i.e. **organisational competencies and capabilities** (internal capability

[23] The bold text represents the classification of capabilities that are included in the analytical framework.

building) (Hoopes & Madsen, 2008, p. 407; Montealegre, 2002, p. 522), or based upon organisational coordination mechanisms and cross-functional teams, i.e. **internal coordination** (internal capability building) (Henderson, 1994, p. 617; Hoopes & Madsen, 2008, p. 408).

4) Inter-firm creation is based upon interaction to combine knowledge and capabilities of the science base, i.e. **stakeholders support** (external capability building), or with suppliers, i.e. **supplier development or desorptive capacity** (external capability building), and **vertical alignment** (external capability building) (Halldorsson, Kotzab, Mikkola, & Skjøtt-Larsen, 2007, p. 290; Hoopes & Madsen, 2008, pp. 408-409; Lichtenthaler & Lichtenthaler, 2009, p. 1325; Romijn, 1997, p. 367; Romijn & Albaladejo, 2002, p. 1062; von Tunzelmann & Wang, 2003, pp. 39, 47).

The difference between building up capabilities based upon stakeholders support and vertical alignment, is that the former follows the traditional absorptive capacity argument where the firm builds up capabilities to innovate, based on communication between the external environment and internal subunits, distributing expertise within the organisation (Cohen & Levinthal, 1990, p. 131). Vertical alignment is where a firm's internal capabilities align to the evolving capabilities of the clients/suppliers (von Tunzelmann & Wang, 2007, p. 202). Desorptive capacity on the other hand, is the ability of the firm to identify external opportunities, transfer knowledge to external organisations and exploit it, even without internal application (Lichtenthaler & Lichtenthaler, 2009, p. 1322).

Other contributions have also made distinctions between static and dynamic capabilities, where the static capabilities are organisational processes designed for conventional products/services and unsuitable for new product/processes, whilst dynamic capabilities are coordinative management processes for interorganisational learning to find solutions to introduce new products/services (Teece, Pisano, & Shuen, 1997, p. 518). Static capabilities may be more suitable for stable markets where there is limited or no technical change, and for conditions which approximate perfect knowledge (Nightingale, 2008, p. 559). Hence static regulations, or those suffering little change over time, or that are fully understood may be approached by building up static capabilities. On the other hand, regulations that change continuously, or change significantly, or are uncertain or not fully understood, may drive firms to respond by building up dynamic capabilities.

Overall, dynamic capabilities consist of changing capabilities to sustain competition (Hoopes & Madsen, 2008, p. 413; Winter, 2003, p. 992). From an evolutionary view point however, it has been suggested that, if a capability changes in order to remain competitive, it should be in light of the capability changes of the firm's suppliers and clients, i.e. **vertical alignment**; dynamic capabilities should be accumulated within the firm based on external interaction with a network of suppliers (Del Sorbo, 2010, p. 33; Lamming, 2000, p. 771; von Tunzelmann & Wang, 2003, pp. 39, 47, 2007, p. 203). Hence, radical changes in regulations may drive firms towards collaborative interaction with their stakeholders and suppliers.

To sum up, there are broadly three internal and three external mechanisms to build up capabilities. The *internal capability buildings* are: 1) organisational competencies and capabilities, leading to capabilities creation and imitation; 2) managerial systems, leading to capabilities replication; and 3) internal coordination, leading to capabilities creation, integration and coordination across functional teams. The *external capability build ups* are: 1) stakeholders' support, which lead to exert the firm's absorptive capacity; 2) supplier development, based on developing the firm's desorptive capacity (a definition is given below); and 3) vertical alignment, which leads to the adapting of internal firm's capabilities in function of the capabilities of the supply chain partners. In theory, each one of the mechanisms to build up capabilities may be used accordingly by firms to respond to their regulatory environment.

Assuming that building up internal capabilities may require less input resources than external capabilities, and that absorptive and desorptive capacity may require less input resources than vertical alignment, because the later requires both of the interacting firms building up capabilities, rather than only one of the two interacting; later in the discussion and analysis the internal capability building will be classified as basic, the external with one firm building up capabilities will be classified as intermediate, and the external with the two interacting firms building up capabilities will be classified as advanced.

According to Carmeli (2001), and Lechner and Gudmundsson (2008) it is not given that resources and capabilities have value on their own. It is more important the 'way' resources and capabilities are 'combined' to create value (Carmeli, 2001, p. 665). It is the resources and capabilities 'bundle', the interactive or simultaneous effects that may have an effect on firm performance (Lechner & Gudmundsson, 2008, p. 3). This implies that attempting to add up the individual values of resources and capabilities to estimate total value or performance of a firm may render incorrect interpretations.

In relation to the need at instances of external sources of knowledge to combine or bundle resources and capabilities form different firms, the question is whether accessibility, development and exploitation may be conditioned to the governance and structures of the organisations pulling resources and capabilities together. The assumption of this thesis is yes.

External knowledge sourcing

The RBV literature about supply chain and client/supplier relationships (Bessant, Kaplinsky, & Lamming, 2003; Bowen, Cousins, Lamming, & Faruk, 2001; Buysse & Verbeke, 2003; Crotty, 2006; Lamming, 1992; von Tunzelmann & Wang, 2003) has only a limited number of contributions that explicitly analyse how relationships are governed and structured so that resource- and capability-building across organisational boundaries can be understood (Delmas, 1999; Dosi et al., 2008, p. 23), with Delmas (1999) apparently having the only empirical study that considers such issues.

Hence, there is need to empirical investigations that explore and validate explanations of how supply chain partners relate one another (i.e. ownership, power distribution, coordination, etc.) to building up input resources and capabilities, appropriate and exploit output resources and capabilities, to reach compliance and gain competitive advantage.

What is more, the RBV have largely considered that capabilities are complementary (Lichtenthaler & Lichtenthaler, 2009, p. 1318) but omitted testing whether the complemented resources and capabilities had in fact been valuable (Fiss, 2007, p. 1192).

Ghoshal, Hanh and Moran (1999) argue that there are reasons for the possibility of non-complementarity of capabilities. First, just as in the division of labour, different specialised bodies of knowledge may not necessarily complement each other. As a result, bodies of knowledge may become substitutes and drive firms, for instance, into vertical disintegration. Second, when two bodies of knowledge are complementary, the transformation of one of them may not sustain their complementary status (Ghoshal, Hahn, & Moran, 1999, pp. 133-134). Recently Nooteboom (2009) also noticed that accumulating dissimilar and non-complementary capabilities, increases the complexity of cognitive coordination required to exploit their combinations, and argues that it limits the size of a firm (Nooteboom, 2009, pp. 121-122).

Thus, if understanding compliance requires knowledge of the regulatory aim (Buysse & Verbeke, 2003, pp. 458,460-461,464-465), how firms respond to regulations (Delmas, 1999, p. 645), and industrial performance (Boyd, 1998, p. 42; Viscusi, 1979, p. 125), i.e. better or longer supply chain relationships, then it is important to understand whether capabilities turn out to be complementary, and the role in these complementarities played by the supply chain relationships.

2.3. Supply Chain Governance Structures and Compliance

An international fresh produce supply chain moves produce from the growing areas through packing facilities, warehouses for transportation, the containers and trucks for transportation, distribution facilities, and the supermarket warehouses (Closs & McGarrel, 2004, p. 8; US BioAct 2002), and includes all the logistics activities taking place in each one of the mentioned stages of the supply chain[24].

Value chains are series of activities that adds value to the produce (Gereffi, Humphrey, & Sturgeon, 2005; Kaplinsky & Morris, 2001). For instance, modifying the packing materials or the brands the customers' perceptions of the value of the product can change, whilst it is very unlikely for a change in transport or warehousing to change the customers' perceptions of the value product. On the other hand, faster transport or better cooled or controlled atmosphere containers and warehousing may sustain the quality of fresh produce for a longer time, hence, influencing the customers' perceptions of the value of the produce, in which the value adding activity is not the change of transport, or warehousing, but the incorporation of more efficient systems or technologies.

[24] For the purpose of this study, transportation (logistics) from and to different supply chain stages, is also part of the supply chain, hence it represents another stage. See the background chapter, section on Mexico-US fresh produce supply chains.

The supply chain literature has been mainly concerned with setting performance measures of how supply chain parties act and react according to other parties actions and reactions (Beamon, 1999; Bullinger, Kühner, & Van Hoof, 2002; Chan & Qi, 2003) as well as of how they cooperate or coordinate their activities (Griffith & Myers, 2005; Hewitt-Dundas, Andreosso-O'Callaghan, Crone, & Roper, 2005; Lawson, Tyler, & Cousins, 2008; Reeves, 2007).

In the study of the impact of regulations on the interrelationships between firms, studies from value chain perspective and supply chain management perspective have a common interest which is understanding what happens at the level of governance and the structure of the relationships between chain partners (Bitran, Gurumurthi, & Sam, 2007; Gyau & Spiller, 2008; Macdonald, 2007; Nadvi, 2008; Raynaud et al., 2005; Squire, Cousins, & Brown, 2009).

Briefly, as described in the next subsection, governance structures, these may be understood as types of markets (e.g. open markets, relational, hierarchies) and relationships (e.g. power distribution, inter-firm coordination) contexts in which business transactions occur.

Surprisingly, in the literature about firms' capabilities, understanding the building, development and sharing of governance structures have not been much of a concern. Although for some scholars capabilities are important for governance structures, they do not explain the how capabilities may evolve to influence the governance structures (Dosi et al., 2008; Gereffi et al., 2005; Reeves, 2007).

Fortunately, Delmas (1999), Delmas and Toffel (2008), and Lamming, Bessant and Noke (2006) have provided insights on how to understand the relationships between governance structures and capability building. Delmas (1999) initially focused on the waste management industry, and voluntary environmental regulations. She predicted that alliances are chosen over vertical integration to complement competencies to develop tacit knowledge and re-deployable technologies in contexts of high technological and regulatory uncertainty (Delmas, 1999, p. 662).

One of the difficulties in Delma's study (1999) was explaining the presence of 'highly specific investments' under 'contractual arrangements', which contradicts the theory, because 'high asset specificity' should, in theory, correspond to 'vertically integrated structures' (Delmas, 1999, p. 659). This means that European and North American waste management companies subject to regulatory changes opted for deploying specific assets with technology that had been already developed outside the firm, rather than by developing the assets by themselves within vertically integrated governance structures (as the transaction costs theory would suggest). Delmas' explanation is that the assets, although specific to the transactions, are actually meant to be redeployable (for the introduction of other technologies and products) (Delmas, 1999, p. 660).

However, there is a problem of not distinguishing between coordination and integration in the analysis of the governance structures. By making such distinctions, one could argue that, although the specific assets have been developed and acquired outside the boundaries of the firm, it may have happened under a coordinated governance structure, resembling dynamic capabilities, i.e. vertical alignments, because specific assets may not need vertical integration but may occur under contractual arrangements. Some of the reasons for this are, for instance, presence of strong appropriability regimes, non-critical assets, a weak financial situation, and presence of imitators/strong competitors (Teece, 1986, p. 296).

Hence, developing and incrementally improving biosecurity of the firm and their supply chains may require important collaborative efforts with clients and suppliers, which in turn may lead to important investments in highly specific assets, driving higher vertical coordination but not necessarily integration of the supply chain.

Similarly, it was shown that in the transport service sector, access to knowledge may happen on a short-term basis with not much commitment among businesses, reducing the need for mergers and acquisitions or in-house capability development (Phillips, Lamming, Bessant, & Noke, 2006, p. 455). However, it contradicts a more recent argument by Delmas and Toffel (2008) about heavy polluting industrial sectors, where there is a positive role of buyers' and suppliers' (receptivity to market pressure) engagement in local firms' compliance (Delmas & Toffel, 2008, p. 1045), which implies a sustained relationship to meet regulatory requirements. So, since knowledge transfers are facilitated by firms' relationships, that in service sectors seem to be short-term and non-committing while in heavy polluting industries seem to be committing and long lasting, the question is what about the fresh produce industry?

Thus, the question is how governance structures mediated the ways firms in the food supply chain build up their capabilities to comply with biosecurity regulations. However, it is still to be explored how governance and structure influence the way capabilities are built for compliance. If governance structures are relevant for the capabilities building, and consequently for the firm and its supply chain's biosecurity resources, then governance structures may indirectly influence the valuation that CTPAT regulators make of those capabilities, even when such valuations are contextual.

Governance Structures

Governance structures, heavily based on transaction costs and the value chain governance literatures, have been classified as market, modular, relational, captive and hierarchical (Dosi et al., 2008; Gereffi et al., 2005; O'Toole & Donaldson, 2000; Williamson, 1981). Each one of them differs to some extent in four fundamental aspects: power asymmetry, dependency, integration and coordination (Bowen et al., 2001; Cousins, 2002; Dahlstrom, McNeilly, & Speh, 1996; Delmas, 1999; Delmas & Toffel, 2008; Jaspers & van den Ende, 2006; Pietrobelli & Saliola, 2008; Robertson & Langlois, 1995; Squire et al., 2009; Teece, 1986).

The ***power asymmetry*** in the supply chain means that the decision to mobilise capabilities along the chain is concentrated in a lead firm, and the concentration of decision making powers is more likely to happen in hierarchies than in markets because hierarchies tend to be vertically integrated firms and markets are at the opposite spectrum of hierarchies (Gereffi et al., 2005, p. 88; Monteverde & Teece, 1982, p. 324), thus hierarchy transactions are coordinated under unified directions, whilst market transactions are not coordinated under unified directions. Supply chain power refers to who enforces standards/norms/regulations in the chain (Pietrobelli & Saliola, 2008, p. 953), as well as whether there are firms concentrating the supply chain roles, activities and responsibilities[25] (Dahlstrom et al., 1996, p. 120).

---

[25] Although Dahlstrom, McNeilly and Speh (1996:120-122) consider definition of roles and responsibilities from a formal or informal control mechanism, we considered it more relevant to capture changes in responsibilities along the chain, as well as roles and activities accumulated by each partner of the chain,

Compliance may also be influenced by various degrees of ***dependency*** of the firms' assets to its clients/suppliers. These degrees may be null (no dependency among firms), unilateral (one firm depends on the other, but not the other way around) and bilateral (both firms are interdependent) (Teece, 1986, p. 289). Dependency increases when: 1) the switching costs of doing business with other firms increases (Cousins, 2002, p. 79; Monteverde & Teece, 1982, p. 324; Strange, 2009; Teece, 1986, p. 289), 2) the share of sales to a given supply chain partner increases (Delmas, 1999, p. 635), 3) the asset specificity of the firm to the transaction increases (Dahlstrom et al., 1996, pp. 120-122; Patnayakuni, Rai, & Seth, 2006, p. 21), and 4) the relationship length of the supply chain partners increases. Dependency is associated with embedded relationships to acquire routines and norms that become the stable expectations of both parties, facilitating the collaborations and mutuality of the dependency between supply chain partners throughout time (Cousins, 2002, p. 81; Squire et al., 2009, p. 466). Hence, the extent that a firm requires its suppliers' and clients' capabilities for its own compliance, it can be said to have deeper dependency on those partners.

The dominant view is that governance structures relate to degrees of vertical integration as suggested by the Transactions Costs and the Value Chain Governance literatures (Gereffi et al., 2005; Williamson, 1971). However, governance structures also relate to coordination or interaction routines, because there are alternative forms of vertical relationships (Raynaud, Sauvee, & Valceschini, 2009, p. 18).

Vertical coordination and vertical integration differ in that the first are vertical interactions and information flows (Jaspers & van den Ende, 2006, p. 819; Patnayakuni et al., 2006, p. 15), while the second are controlled and owned or holding shares of their suppliers/clients (Jaspers & van den Ende, 2006, p. 821; Robertson & Langlois, 1995, p. 547).

More specifically, ***vertical integration*** refers to the ownership of the different stages of the supply chain, and the more stages are owned by one firm, the more integrated the supply chain is. However, it is not given that these firms are managed by a central office (hierarchical control). In fact when Williamson discussed the differential control properties of firms in comparison to markets (Delmas, 1999, p. 663; Williamson, 1971, p. 113), he referred to different types of governance structures exerting control over firms, the

---

modifying the sense of the measurement from formal control mechanisms to accumulation of power, giving the possibility to capture how asymmetric if distributed along the supply chain.

underlying assumption was the possibility of hierarchical inter-firm controls. Further, he explicitly mentioned that activities within each section of the firm can be run independently from one another (Williamson, 1971, p. 113).

The view of regulatory studies is that if compliance requires increasing divisional coordination, and if such divisions are located in different supply chain stages (e.g. exporter and transporter), then vertical integration will occur, especially if the knowledge that supply chain partners are sharing is tacit (Gorga & Halberstam, 2007, p. 1203; McInerney, 2004, p. 194). On the other hand, there are studies that challenge that view, arguing that disintegrated structures rely more on tacit knowledge (van den Berg, 2008, p. 192). Hence, the relationship between knowledge exchange, capability building and supply chains' degrees of integration remains ambiguous in the literature.

Vertical coordination refers to integrating capabilities in efficient configurations, provision of technical expertise, and loans to supply chain partners (Arshinder, Kanda, & Deshmukh, 2008, p. 318; Frank & Henderson, 1992, p. 942; Jaspers & van den Ende, 2006, p. 819; Patnayakuni et al., 2006, p. 15; Sirmon, Hitt, & Ireland, 2007, p. 277).

Integration and coordination are neither mutually exclusive nor inclusive; it may be possible to find *vertically integrated and uncoordinated firms*, when owned and managed by the same company but each party in the chain may not coordinate or share activities (Raynaud et al., 2009, p. 18), such as the case of Agrilink Foods Inc. (Chaddad & Cook, 2004, p. 356). V*ertically disintegrated and uncoordinated firms* have separated ownership and control, and their activities are not shared or coordinated between them, what is commonly known as market transactions. *Vertically integrated and coordinated firms* share ownership and managerial control, as well as coordinating and sharing activities across parties in the chain (Chaddad & Cook, 2004, p. 352; Sporleder, 1994, p. 537), such as the case of American Apparel (American Apparel, 2009, p. 5). *Vertically disintegrated and coordinated firms* have different ownerships and control, yet they share activities and systems, coordinate processes and management across parties in the chain. This is what Teece (1986) called specialised and co-specialised complementary assets. Examples of this type are repair facilities for rotary engines by Mazda (Teece, 1986, p. 289), also exclusive and specialised warehousing, for instance, in the construction industry (Bayazit, Karpak, & Yagci, 2006), Toyota's suppliers' exclusive warehousing supporting Toyota's just-in-time systems (Kalwani & Narayandas, 1995, p. 5), or the distribution centre for exports of Supply Chain 1 (p.106).

To sum up, coordinative or integrative governance structures relate to various degrees of assets complementarities, and various degrees of dependency and power relations between firms (Teece, 1986, p. 289). Surprisingly, the analysis of the interfaces between firms' internal and external relationships remains under-investigated (Peck & Juttner, 2000, p. 42), and empirical contributions are still scarce (Matopoulos, Vlachopoulou, Manthou, & Manos, 2007, p. 177).

The following sections specify the areas of concern in the previous literature, and present the main theoretical question driving the empirical investigation for this thesis.

2.4. Minding some gaps in the Literature

To understand how business regulation may drive organisations towards or away from desirable or undesirable social, economic, environmental, or security consequences, it is necessary to understand compliance processes and firms' capability building. However, both the regulatory studies and the Resource-Based View miss important elements to advance such an understanding.

The regulatory studies:

1) Assumed that business compliance is a matter of 'willingness' or financial resources to meet a regulatory aim; hence the regulators would just need to force or tactfully motivate the firms to comply, omitting, at least empirically, the capability building and compliance processes.
2) Focus on the cost and negative effects of regulations, with limited contributions about how firms might engage in innovative compliance to regulatory commitments and the role of regulatory structures in allowing the flexibility to undertake such innovation.

3) Have not sufficiently investigated the impact of regulations in the context of inter-firm relationships, even though regulations are explicitly engaging the focal firm and their clients and suppliers.

4) Because public-private partnership regulations (PPPs) are recently being suggested as a model for regulatory policy (Garcia-Martinez et al., 2007) scholars have focused much on the regulatory standard setting, rather than in their impacts in international supply chains' governance structures.

5) Not investigating the impacts of PPPs on international supply chain governance structures, implies uncritically accepting the world-wide diffusion of the potential shortcoming so the PPPs, which may include their potentially, can be used as Non-Tariff Measures in the global trade.

6) And, although there are compliance models, they have not yet been sufficiently empirically tested to validate them[26].

The Resource-Based View scholars, on the other hand:

1) Have not yet systematically studied the organisational capabilities building processes that are not driven by the need to capture market-value, but by regulations. In other words, the RBV remains narrowed in its investigations by focusing on productive capabilities, whereas not enough attention has been paid to understand the roles of facilitative, enabling, supportive capabilities, such as compliance capabilities. As a result, they have been unable to capture non-market-based sources of competitive advantage and any unforeseen long term ancillary benefits of organisational innovations from compliance.
2) Have assumed that capabilities have intrinsic value and they are complementary, rather than testing whether such value exists and whether they are complementary.
3) Have not assessed transformations of governance structures in the context of capabilities building along supply chains.
4) Have paid limited attention to innovation processes in 'low tech' sectors, such as the agri-food business.

[26] For instance, the US federal sentencing commission publishes information about compliance programmes only from organisations accused of infringements (See http://www.ussc.gov/annrpts.htm).

All in all, there are gaps in the supply chain relationships literature, in the resource-based view, and the regulatory studies that make it difficult to connect the impact of regulations on firms' compliance. For instance, it is unknown whether the potential shortcomings of the PPPs – ineffectiveness or illegitimate - distort the ways firms' capabilities are evaluated by the regulators. There is still need to understand how supply chain governance structures relate to compliance capabilities building, so that issues of dependency and power asymmetries are at least acknowledged, and issues of integration and coordination are envisaged in international trade policies. It is necessary to understand the relationship between regulation and capabilities in the processes of compliance, should regulators want to design smarter or more responsive regulations to promote compliance.

Hence, this thesis offers a framework and tests it with an empirical investigation that allows communicating better between regulatory scholars, RBV scholars, and supply chain governance scholars.

Theoretical question

The theoretical question is according to the RBV which capabilities are best for regulatory compliance? The answer to this question expects to clarify and differentiate the processes to acquired knowledge –intra-firm and inter-firm- to build up capabilities, the capabilities built at each compliance level, and resources developed by the capabilities and which are finally evaluated by regulators to determine whether a firm is complying or not with the regulations.

In addition, the theoretical question allows to identifying suitability (value), persistency, and complementarity of capabilities at each compliance level. This contributes to removing a common assumption that knowledge, capabilities and assets are complementary. Moving forward from only analysing variety, heterogeneity, and bundle of capabilities and resources, to analysing whether they are complementary.

For instance, assuming that a variety of capabilities and resources are not necessary enough for compliance with CTPAT, but it is necessary to identify the most suitable capabilities at each compliance level, then, CTPAT Regulators and firms may want to know which and under what conditions capabilities lead firms to compliance. Perhaps CTPAT seminars (capacity building) would transcend from informing the guidelines with the bunch of resources needed for compliance, to facilitating the learning processes of the firms to identify their own ways to build and complement capabilities to secure their supply chains. This may in turn help achieve the social aim of the regulation, reducing the risk of biosecurity threats.

To address such question and concerns, the following analytical framework was devised integrating regulatory, capability building, and governance structures contributions.

2.5. Analytical framework

Regulatory studies have stressed the need to regulate businesses, and particularly the food industry. Regulations may vary in their degrees of constraints according to industry types (Ashford et al., 1979, p. 161; Baldwin et al., 1998; Braun & Wield, 1994, p. 261; Delmas & Toffel, 2008, p. 1035; Henson & Humphrey, 2009, p. 11; Muradian & Pelupessy, 2005, p. 2032). To build up reputational capital (Rivera, 2002, p. 338), reduce the risk of the negative consequences of reputational damage (Meidinger, 2006, p. 75; Pfarrer, Smith, Bartol, Khanin, & Zhang, 2008, p. 388; Raynaud et al., 2005, p. 50), or to be allowed to remain in business firms follow **compliance processes** (Identification, Interpretation, Identifying requirements, Compliance decision, Compliance method, Communication, Implementation (routines), and Evaluation and monitoring) (French et al., 1992; Henson & Heasman, 1998, p. 20; Sproull, 1981, p. 454)[27]. The degree of success in meeting regulatory requirements-i.e. **compliance leadership (low, medium, high compliance)**- may vary according to the types of capabilities and resources that the firms have or can build (Buysse & Verbeke, 2003, pp. 458,460-461,464-465; Delmas, 1999; Delmas & Toffel, 2008; McGee, 1998; Rugman & Verbeke, 1998, pp. 371-372)[28].

Given that, 1) the agricultural and food sectors tend to concentrate efforts in technological and organisational forms of innovations (Pavitt, 1984, p. 354, 1998, p. 434), and 2) the

[27] See page 30, Table 2.5.1, p.52.
[28] See pages 28 to 30, and Table 2.5.1, p. 52.

security resources required for compliance, i.e. business partnership, physical, access controls, personnel, information technology, procedural, trailer and conveyance, training and threat awareness (C-TPAT/CBP, 2006, p. iii, 2007, p. 3), indicate organisational routines, the analysis in this thesis focuses on organisational forms of innovation for the development of biosecurity resources for compliance[29].

Since resources are 'things' and capabilities are 'ways of doing things' (Dosi et al., 2008, p. 11), in other words, capabilities are a 'collection of routines' for the 'production of significant outputs' (Hoopes & Madsen, 2008, p. 397), the focus in this framework is on how firms build up capabilities to develop resources, or how intra-firm and inter-firm routines are collected to produce security-based systems and technologies (resources).

This framework focuses attention on how organisational routines contribute to build up the following **capabilities**: managerial systems and organisational competencies (Montealegre, 2002, p. 522; Winter & Szulanski, 2001, pp. 733-734), internal coordination mechanisms (Henderson, 1994, p. 617; Kogut & Zander, 1992, p. 388; McInerney, 2004, p. 194), interaction with external organisations, suppliers, and clients (e.g. stakeholders support, supplier development, vertical alignment) (Buysse & Verbeke, 2003, p. 465; Del Sorbo, 2010, p. 33; Hart, 1995, p. 1001; Lamming, 2000, p. 771; Lichtenthaler & Lichtenthaler, 2009, p. 1321; Romijn, 1997, p. 367; Romijn & Albaladejo, 2002, p. 1062; Sako, 2004, p. 281; von Tunzelmann & Wang, 2003, pp. 39, 47, 2007, p. 203)[30].

Also, given that interactions with external organisations for capability building require some form of **governance structures** (Delmas, 1999, p. 663; Williamson, 1971, p. 113)[31], in this framework we analyse how the firms are governed and structured in their supply chains (Arshinder et al., 2008, p. 318; Frank & Henderson, 1992, p. 942; Jaspers & van den Ende, 2006, p. 819; Patnayakuni et al., 2006, p. 15; Sirmon et al., 2007, p. 277)[32].

The firms' interactions are structured by degrees of integration (Jaspers & van den Ende, 2006, p. 821; Robertson & Langlois, 1995, p. 547; Williamson, 2002, p. 180) and coordination (Jaspers & van den Ende, 2006, p. 819; Patnayakuni et al., 2006, p. 15;

[29] See page 8, and Table 2.5.1, p. 52.
[30] See pages 34 to 39, and Table 2.5.1, p. 52.
[31] Governance structures are forms of inter-firm controls in Delmas and Williamson.
[32] See pages 42 to 45, and Table 2.5.1, p. 52

Williamson, 1991, p. 279). These are neither mutually exclusive nor inclusive and may interact.

The firms' interactions are governed by degrees of dependency and power asymmetry between firms. Dependency of the firm increases when the switching costs of doing business with other firms increase (Cousins, 2002, p. 79; Monteverde & Teece, 1982, p. 324; Strange, 2009; Teece, 1986, p. 289). Switching costs are assumed to be related to the degree of asset specificity (Dahlstrom et al., 1996, pp. 120-122; Patnayakuni et al., 2006, p. 21; Williamson, 1991, p. 281), market concentration of the firm in the supply chain (Delmas, 1999, p. 635; Pietrobelli & Saliola, 2008, p. 955), and the length of the relationship (Cousins, 2002, p. 81; Squire et al., 2009, p. 466; Williamson, 1991, p. 280).

Power asymmetry increases with the concentration of the decision making powers in a lead firm (Gereffi et al., 2005, p. 88; Monteverde & Teece, 1982, p. 324). The power is assumed to be located in the firm that decides and enforces standards/norms/regulations to the supply chain partners (Pietrobelli & Saliola, 2008, p. 953).

In this analytical framework the regulations, standards, and norms are exogenous. This helps to identify various regulations and make it easier to compare the resources and capabilities building by regulation. Although regulations drive the resources and capabilities building processes and compliance, and vice versa (Paraskevopoulou, 2008), this thesis centres on the first part of the analysis, regulations driving capabilities.

However, the capacity of the firm to build up capabilities to meet regulations may also be constrained or enhanced by their supply chain governance structures. Some governance structures may favour building certain capabilities configurations; moreover if such configurations require capabilities located in different firms along the supply chain.

Altogether, when a regulation is set and a firm identifies the regulation, the compliance process starts. The firm evaluates the potential benefits of complying with the new regulation in terms of benefits of reputational capital or reduced risk of reputational damage, and they may or may not decide to comply. If the firm decides to comply, it needs to go further in the compliance process, for which capabilities are required. There are three types of capabilities: basic, intermediate and advanced. These capabilities will be used mainly in the implementation process, in order to develop security resources. There are nine types of security resources: business partners, physical security, access controls, personnel control, procedural security, information and communication technologies, container and trailer security, conveyance security, and threat awareness.

The ways knowledge is sourced and resources deployed depend on the firm's supply chain governance structures. The governance structure indicates degrees of integration, coordination, dependency, and power asymmetry in the supply chain.

The framework is thought to assess the firms' compliance levels against the processes followed by firms in their attempts to achieve compliance, from which we identify the compliance processes. It is also thought to assess the compliance levels against capabilities, from which we identify the compliance capabilities, and it is also thought to assess compliance capabilities, against governance structures, from which we identify the valuable governance structures.

Although further assessment may be run, such as compliance levels with governance structures, or compliance levels and security resources, or security resources and governance structures, the assessments will limit to the necessary for answering the research questions and test the hypothesis, which will be described in the next section.

Table 2.5.1: Compliance capabilities: an organising framework

Regulatory compliance		Resource and Capability Building		Supply chain relationships
Compliance leadership	Processes	Capabilities	Security Resources	Governance structures
Low Middle High	Identification Interpretation Identifying requirements Compliance decision Compliance method Communication Implementation (routines) Merge routines/resources Add routines/resources Avoid routines/resources Evaluation and monitoring	<u>Basic capabilities</u> Organisational competencies Management systems Internal coordination <u>Intermediate capabilities</u> Strategies (with stakeholder) Supplier development <u>Advance capabilities</u> Vertical alignment	Business partners Physical security Access controls Personnel security Procedural security Information systems security Container security Conveyance security Training and threat awareness	<u>Structure</u> Integration vs disintegration Coordination vs. un-coordination <u>Dependency</u> Asset specificity Market concentration Relationship length <u>Power Asymmetry</u> Symmetric Asymmetric
(Buysse & Verbeke, 2003, pp. 458,460-461,464-465; Delmas, 1999; Delmas & Toffel, 2008; McGee, 1998; Rugman & Verbeke, 1998, pp. 371-372)	(French et al., 1992; Henson & Heasman, 1998, p. 20; Sproull, 1981, p. 452)	(Buysse & Verbeke, 2003, p. 465; Del Sorbo, 2010, p. 33; Dosi et al., 2008, p. 11; Henderson, 1994, p. 617; Hoopes & Madsen, 2008, p. 400; Kogut & Zander, 1992, p. 388; Lamming, 2000, p. 771; Lichtenthaler & Lichtenthaler, 2009, p. 1321; Montealegre, 2002, p. 522; Romijn, 1997, p. 367; Romijn & Albaladejo, 2002, p. 1062; von Tunzelmann & Wang, 2003, pp. 39, 47, 2007, p. 203; Winter & Szulanski, 2001, pp. 733-734)	(C-TPAT/CBP, 2004, p. 7, 2006, pp. 1, 7; Closs, 2005; Erera, 2005; FDA/HHS, 2009, p. 4; Manning, Baines, & Chadd, 2005; Rice & Spayd, 2005; Sarathy, 2006; Sheu, Lee, & Niehoff, 2006)	(Arshinder et al., 2008, p. 318; Bowen et al., 2001; Cousins, 2002; Dahlstrom et al., 1996; Delmas, 1999; Delmas & Toffel, 2008; Frank & Henderson, 1992, p. 942; Gereffi et al., 2005; Jaspers & van den Ende, 2006; Monteverde & Teece, 1982, p. 324; Patnayakuni et al., 2006, p. 15; Pietrobelli & Saliola, 2008; Robertson & Langlois, 1995; Sirmon et al., 2007, p. 277; Squire et al., 2009; Teece, 1986; Williamson, 1971, 1991, 2002)

3. CHAPTER 3 Methodology

The methodological chapter is divided into three sections. The first section presents the aim of the present investigation and the research questions. The second section sets the hypotheses and the way these are tested; it also describes how it is expected to answer the research questions. Thirdly, it shows how the traditional comparative case studies research design is complemented with a novel approach for the science, technology and innovation studies for case comparisons, the Qualitative Comparative Analysis.

3.1. Aim, objective and research questions

Aim

In the previous discussion about the role of technology forcing and constructive technology assessment was said that regulation needed to drive firms to develop new technologies and capabilities to achieve social aims, when on their own they were not able to solve the coordination problems and in case of market failures (Schot & Rip, 1996; Williams & Edge, 1996). But the question is, given that firms may knowingly limit their knowledge to self-regulate, *caveat emptor* (Scheppele, 1988, p. 283), would firms in the fresh produce supply chains have secured themselves against being used by terrorists without the 'push' of regulation, and if so, to what extent? Yet, because it is unlikely to get all supply chains partners in a coordinated effort, the risk of terrorism throughout the fresh produce supply chain is still 'arguably high', hence the necessity of regulation to solve coordination failures.

Having decided that a comprehensive or universal regulation is necessary, it then becomes important to assess the regulatory burden on different forms of implementation. Previously it was said that Public-Private Partnerships are the least burdensome methods (Garcia-Martinez et al., 2007). The arguments were based on the following assumptions:

1) governments are not sufficiently knowledgeable to choose the best means of implementation; they are not able to assess relative costs of implementing

different types of regulation, and hence cannot choose the best type of technologies from a compliance costs viewpoint; and

2) governments search for means of reducing costs of enforcement, and one way of doing this is to set standards that make it possible to audit compliance. However these standards are best set in collaboration with industry because industry is better informed about the relative cost of monitoring/audit schemes.

Both the coordination efforts of the supply chains partners for biosecurity, and the knowledge of technologies (and capabilities) to meet the regulatory requirements, led to a consideration of the value of the compliance capabilities, the principle domain of this thesis research.

Hence, the aim of this thesis is to add to the RBV the 'compliance capabilities' as another factor explaining competitive advantage, given that firms may be subject to any form of regulatory pressure (public, private or PPP).

Objective

Based upon assessment of Mexico-US supply chains partners attempting to comply with the Customs-Trade Partnership Against Terrorism (CTPAT), the objective of this investigation is developing an analytical framework capable of analysing firms' compliance processes with social regulations in the context of their supply chains relationships.

Research questions

To meet the aim and objective, this investigation will address the following research questions:

1. What compliance processes do firms follow to meet regulations for the prevention of accidental and intentional contamination of food?
    a. Do differences in the compliance processes across firms explain the differences in their compliance levels with CTPAT?

2. What capabilities do firms build up to meet regulations for the prevention of accidental and intentional contamination of food? And how?
    a. Do differences in the capabilities building across firms explain the differences in their compliance levels with CTPAT?
3. What governance structures enable firms to build up their capabilities to meet regulations for the prevention of accidental and intentional contamination of food?
    a. Do differences in the governance structures across firms explain the difference in their compliance capabilities built for CTPAT?

3.2. Research questions and hypotheses testing roadmaps

By answering the research questions and the following hypotheses, we try to identify the relationships between: 1) compliance processes and compliance; 2) capability building and compliance; and, 3) governance structure and capability building.

On the other hand, the **aim** of the thesis will be met to the extent that three aspects are covered. First, given that firms are in the same marketplace (fresh produce industry), by showing how firms follow different capability building patterns according to whether they seek compliance or not. Second, by showing how firms configure their capabilities is as important as the capabilities themselves (or their bundles) to receive a certification. And third, showing how firms' capability building relates to their supply chains governance structures.

Finally, note that the research questions 1, 2 and 3, are more explorative and have no hypothesis testing associated, however, research questions 2a, and 3a try to perform assessments, comparisons and/or evaluations, which is why they have hypothesis testing associated. For research question 1a, although is comparative, there are not previous theoretical insights, which is why it is left to the conclusions.

Questions and hypotheses 1: The compliance processes

1. What compliance processes do firms follow to meet regulations for the prevention of accidental and intentional contamination of food?
    a. Do the differences in the compliance processes across firms explain the differences in compliance levels with CTPAT?

These questions try to capture the correlation compliance processes and compliance levels with CTPAT.

However, because other regulatory regimes overlap with the CTPAT regulatory requirements, we expect that the answers to these questions have also implications for other regulatory regimes. Nganje *et al.* (2004) have shown that the United States Food Safety and Public Act 2002 (US BioAct 2002) overlaps with CTPAT regulatory aims (Nganje, Wilson, & Nolan, 2004, p. 149), and self-regulatory regimes also may overlap, such as Food safety Standards[33].

The US BioAct 2002 requires procedures in three main aspects: 1) prior notification of imports, 2) electronic manifest, and 3) records keeping (US BioAct, 2002:670-671). The CTPAT requires procedures in several aspects: 1) partners' involvement in implementation of security measures, 2) physical security, 3) access controls, 4) personnel security, 5) procedural (e.g. documentation, traceability, discrepancies, shipping, manifesting, etc.), 6) information technology security, 7) container and trailer security, 8) conveyance, 9) training and threat awareness (C-TPAT/CBP, 2006). Finally, there are Food Safety Standards and other preventive measures developed by firms themselves will be described in more detail in the background chapter.

Question 1 does not require hypotheses because it is a description and story-telling of the organisational compliance processes model explained based upon the analytical framework (Table 2.5.1, page 52). It also paves the ways for questions 1a and 1b, which are more about comparisons and evaluations of organisational compliance processes.

Although **Questions 1a** could have a hypothesis, there are not enough insights from previous studies on whether different compliance processes may explain differences in

[33] The CTPAT is a Public-Private Partnership regulatory regime; the US BioAct 2002 is a public regulatory regime; and Food Safety Standards and other voluntary measures are self-regulatory regimes.

compliance levels. Hence, we have left the hypothesis for the conclusions of this investigation.

Therefore, these research questions drive the description and comparative analysis of the pathways that each of the firms followed for compliance. The discovery of variations and similarities in those processes will yield theoretical and policy insights about organisational compliance process models.

Questions and hypotheses 2: The compliance capability building

2. What capabilities do firms build up to meet regulations for the prevention of accidental and intentional contamination of food? And how?
    a. Do differences in the capabilities building across firms explain the differences in their compliance levels with CTPAT?

The second pair of questions explores the correlations between capability building and compliance levels. Research question 2 requires a description and story-telling of the capability building by the firms, including the inter-firm resources and capabilities exchanges.

Thus, the firms were asked to describe whether and how they built up the following security-related capabilities, which were identified with the literature review (Barratt & Oke, 2007; Boske, 2006; Closs, 2005; Closs & McGarrel, 2004; Erera, 2005; Goddard, 2005; Kinser, Seltzer, & Friddle, 2005; H. L. Lee, 2004; LLTRM, 2004; Manning et al., 2005; Petersen, Handfield, & Ragatz, 2003; Rice & Spayd, 2005; Sarathy, 2006; Shannon, Lee, & Stephenson, 2006; Sheu et al., 2006; Suarez-Bello, 2003):

1) Assessment capacity;
2) Visibility and monitoring capacity;
3) Supply chain coordination and integration;
4) Vulnerability reduction capacity;
5) Operations agility capacity;
6) Learning and knowledge capabilities.

This set of capabilities tries to be comprehensive including the necessary for CTPAT, US BioAct 2002, and any self-regulatory regimes. It gives the flexibility to regroup capabilities by the RBV classification, as well as to regroup resources by CTPAT requirements. The 6 capabilities listed above were the basis of the interview guidelines (see appendix 9.2) and used for the classification of the interview data (see Table 3.4.2, p.80). Later, capabilities were regrouped to match the RBV literature classification of capabilities, which were the basis for the summary of capabilities and resources built by each firm, presented at the end of each case study: they became the primary data for the analyses to answer the following research questions.

Q**uestion 2a** compares the types of capabilities built by firms to meet the regulatory requirements according to each compliance level to CTPAT, i.e. low, intermediate, and high compliance levels. The hypothesis for this question is:

Hypothesis 2a: the higher the CTPAT compliance level of the firm, the more predominant will be the presence of intermediate and advanced capabilities built for compliance, consequently, less predominant will be the presence of basic capabilities built for compliance.

Assessments

Compliance level

The compliance level is measured by the security certification status to CTPAT held by the firms. There are three ordinal levels by which firms may be classified: **low** in those cases where there is no implementation of CTPAT/FAST guidelines; **middle** in those cases where there is implementation of the guidelines and the application for certification had been filled, but these have not yet been validated (certified); and **high** in those cases where the firm holds a CTPAT/FAST certification.

Capabilities sophistication

After grouping the types of capabilities that firms built up for compliance with security regulations, capabilities may be grouped into three levels of sophistication. The **basic capabilities** of the firm are organisational competencies, managerial systems, and internal coordination mechanisms; these represent basic capabilities used to develop security-based resources. The **intermediate capabilities** of the firm are unidirectional knowledge transfers with stakeholders, i.e. absorptive capacity and desorptive capacity (as explained in the section on capability building in the theory chapter, p.35); and these represent dynamic capabilities used to develop security-based resources. The **advanced capabilities** of the firms are bidirectional knowledge transfers with the supply chain partners; and these represent dynamic interactive capabilities used to develop security-based resources.

Table 3.2.1: Classification of capabilities by sophistication level

Qualitative	Capabilities	Ordinal	Code
Basic capabilities	Organisational competencies Management systems Internal coordination	Basic	BCs
Dynamic capabilities	Strategy design feedbacks from stakeholders Supplier development	Intermediate	ICs
Dynamic interactive capabilities	Vertical alignment with the supply chain	Advanced	ACs

For each of the cases, there will be an assessment of the capabilities built up and resources developed. This allows counting the capabilities in each firm by sophistication level, i.e. basic, intermediate, and advanced capabilities counts[34].

[34] These counts must be taken with care, since there it represents stacking up qualitatively different capabilities. This is story of counting apples and oranges together. The assumption is that each sophistication level will group capabilities with shared characteristics.

Relationship between capabilities upgrading and compliance levels

By classifying the firms in low, middle and high compliance categories, it will be possible to identify the share of each level of capability sophistication in the total count of capabilities by compliance level (see Table 3.2.2 for an illustrative example).

Table 3.2.2: Illustrative example of capabilities upgrading by compliance levels (no real data)

Compliance	Capabilities			
	Basic	Intermediate	Advanced	Total
Low	**5**	2	1	8
Middle	3	**4**	2	9
High	2	2	**4**	8
Total	10	8	6	25

A Qualitative Comparative Analysis of all cases will complement the previous relationship allowing the identification of the set of capabilities behind each compliance level (see Table 3.2.3 for an illustrative example).

Table 3.2.3: Illustrative example of capabilities configurations causing compliance (no real data)

Compliance level	Capabilities configurations
0. Low compliance	Organisational competencies and stakeholder support
1. Middle compliance	Supplier development and stakeholder support
2. High compliance	Vertical alignment and stakeholder support

The previous illustrative example (Table 3.2.3, above) may indicate that organisational competencies, supplier development, and vertical alignment have only relational value; furthermore, they are only valuable at a given compliance level. On the other hand, stakeholder support has not only relational but also intrinsic value. This is because the capability retains value at any compliance level, which would indicate that a firm may want to build up that capability with some certainty that it will be required at any stage of their compliance journey, not only for a given level.

This exercise may address not only the research question but also contributes to the achievement of the aim, by showing how compliance capabilities may be a source of competitive advantage, from the RBV.

Questions and hypotheses 3: The governance structures

3. What governance structures enabled firms to build up their capabilities to meet regulations for the prevention of accidental and intentional contamination of food?
    a. Do differences in the governance structures across firms explain the difference in their compliance capabilities built for CTPAT?

The third set of questions tries to identify the enabling conditions for capability building conducive to compliance. **Question 3 examines what type of governance structure was present at the time when firms built their capabilities for compliance, and how those governance structures may have facilitated or inhibited capability building.**

Thus, each case includes a story-telling and description of the role that knowledge exchange and capability building played while interacting with external organisations, i.e. supply chain partners and stakeholders.

Based on the analytical framework, the firms were asked in a questionnaire (Appendix C: Questionnaire COMCAP 2007-2008) to describe their supply chain governance and structure (see Table 3.2.4, p.64). Due to the descriptive and explorative nature of the question, there are no hypotheses associated with this question.

The results of each firms' constructs from the questionnaire will be compared against the rest of the firms. For each firm we may be able to say if it had decision making powers, if it was dependent on or independent from its supply chain, if it was coordinated or not, and whether it was integrated or not, compared with the rest of the firms (for an illustrative example see Table 3.2.5).

Q**uestion 3a** on the other hand, does allow hypothesis testing. Williamson (1991, p.279, and 2002, p.180) stated that tighter governance structures in terms of control and hierarchies are required when the firm needs to build up specific assets, when the complexity of the adaptations between firms increases, when the length of the relationships between firms increases, and when bilateral dependency increases.

However, Delmas (1999) found that specific investments (usually associated to vertical integration) were present under contractual arrangements (markets) (Delmas, 1999, p. 645). This seems to be a contradiction that implies that there is more than a straight path between markets and hierarchies; this is because vertical coordination and vertical integration should be taken separately, rather than considering that coordination is directly related to integration.

Thus, given that learning and knowledge exchange with supply chain partners to build up capabilities to meet regulatory compliance with CTPAT may be related to tighter governance structures, this investigation will test the following hypothesis:

Hypothesis 3a: the transition from basic to sophisticated capabilities is associated to changes in governance structures, this is: 1) increased controls or asymmetric power, 2) increased bilateral dependency, 3) increased coordination, and 4) increased integration.

Assessment

Governance structures

To assess governance structures it was necessary to follow the analytical framework (Table 2.5.1, p.52). Thus the questionnaire (COMCAP 2007-2008) was created and validated to capture the four components of Hypothesis 3a into their corresponding constructs (see Table 3.2.4, p.64).

The descriptions and explorative analysis of **question 3**, allows us to move forward to test Hypothesis 3a stated before.

For that, the qualitative comparative analysis will be applied, this time to identify the governance structures that are common across firms with capabilities associated to each compliance level. This is possible by analysing the results of **question 3** in light of the results of research **question 2a**.

After establishing such analyses and relationships we will be in position to discuss more specifically how governance structures enabled capabilities building, as well as the differences between governance structures associated to advanced capabilities built to meet the CTPAT requirements (see below an illustrative example of the type of relationships between capabilities sophistication and governance structures).

All in all, understanding the compliance process, capabilities building analysed, and the role of governance structures clarified, we will show from the RBV what and how capabilities are built, and how they leverage value, even though the process is not market driven, but regulatory driven. With this, we expect to say how compliance capabilities contribute to the competitive advantage of the firm, the aim of the thesis.

Finally, we expect to depict some regulatory policy implications related to compliance, and policy recommendations related to corporate strategy in a supply chain context.

Table 3.2.4: Supply chains governance structures: constructs and definitions

	Constructs	Variables	Scales	Definitions
Governance	Power Asymmetry[35]	Decision making	1 to 10	1 means that decisions are made by the supply chain partners, 10 means that decisions are made by the firm; and 5 means that decision are jointly made between the firm and its supply chain partners.
	Dependency[36]	Asset specificity	-6 to 6	-6 denotes that assets are not specific and 6 means that assets are highly specific. 6 types of assets were evaluated: 1) Geographic location, 2) infrastructure, 3) human capital, 4) brand, 5) technology and processes, and 6) marketing windows.
		Relationship length	0 to 30	0 means that the firm does not expect to complete even 1 year in relationship with its supply chain partners, whilst 30 means that the firm expects to complete 30 years of relationship with the partners.
		Market Concentration	0 to 100	0 represents the 0% of production volume is distributed throughout distributor X or 0% of production volume distributed for exporter X. 100 represents the 100% of production volume is distributed throughout distributor X or 100% of production volume is distributed for exporter X.
Structures	Coordination[37]	Activities	0 to 5	0 represents no coordination of skills and capability building activities with the supply chain partners and 5 represents complete coordination. 5 activities were evaluated: 1) systems (synergies between projects), 2) roadmaps (information sharing), 3) joint development planning, 4) exchange (temporal) of human resources, and 5) shared teams (continuous)
		Investments	0 to 4	0 implies that there were no efforts to coordinate investments in assets between the firm and supply chain partners, whilst 4 means maximum coordination. 4 Investment types were evaluated: 1) systems (synergies between projects), 2) roadmaps, 3) parallel and interacting investments among firms (synergies between units), and 4) loans and financing the client/supplier.
	Integration[38]	Hierarchies	0 to 2	0 indicates that the firm manages the skills formation and capability building activities only within its boundaries; 1 indicates that the firm also manages the skills formation of other stages of the supply chain; and, 2 indicates that the firm also manages the entire capability building activities of other stages of the supply chain.
		Ownership	0 to 3	0 means separate ownership between the firm and other supply chain partners; 1 means the presence of minority shares of the firm in their supply chain partners' business; 2 means the presence of joint ventures (resulting in creation of new entities) between the firm and the supply chain partners; and 3 means that the firm is under unified ownership (acquisition/merger) with other supply chain partners.

[35] COMCAP 2007-2008, question 18
[36] COMCAP 2007-2008, questions 9, 11, 13, 14, 15, 16,
[37] COMCAP 2007-2008, question 8b
[38] COMCAP 2007-2008, question 8a

Table 3.2.5:Illustrative example (no real data): firms' governance structures

Firm	Power asymmetry	Dependency	Coordination	Integration
A	Symmetric (Decision making power 5)	Independent (Asset spec. -3, relationship length 10, market share 30%)	Uncoordinated (Activities 0, Investments 0)	Disintegrated (Hierarchies 0, Ownership 0)
B	Partners (Decision making power 1)	Independent (Asset spec. 0, relationship length 5, market share 30%)	Coordinated (Activities 5, Investments 4)	Integrated (Hierarchies 2, Ownership 3)
C	Firm (Decision making power 10)	Dependent (Asset spec. 6, relationship length 25, market share 80%)	Coordinated (Activities 3, Investments 3)	Disintegrated (Hierarchies 1, Ownership 1)

Table 3.2.6. Illustrative example (no real data):
Governance structures for capabilities sophistication

Capabilities	Commonalities across firms
Organisational competencies	Symmetric power and lack of coordinated investments
Stakeholder support	Specific assets and coordinated activities
Vertical alignment and stakeholder support	Power asymmetry, long term relationships, specific assets, and coordinated activities

3.3. Research design

Methods of data collection

The information for the investigation is mainly primary data, collected through interviews and questionnaires. The information and data were processed, structured, and entered in a database, and later analysed using a comparative case study approach. Also secondary data was used to complement the background chapter and gather regulatory information.

Sources of information and bias

The information was gathered *in situ* from the firm responsible for security implementations' general managers or CEOs. However, direct observation was not always possible due to restricted access to the work floor. Secondary data was also gathered from governmental and official online sources to collect information regarding CTPAT and BioAct 2002.

To address researcher bias and errors, the summary reports of the information provided by each firm were submitted to each interviewee (as well as to other researchers and/or practitioners) for revision and correction. So far there have been no responses with corrections.

Internal validity of the information increases to the extent that the researcher is able to refute invalid information, use comparative methods, treat the data comprehensively, consider deviant cases, and use appropriate tabulations (Silverman, 2005, p. 212). The following strategies were followed in this research. To be able to refute the information, the researcher complemented the interview with an *in situ* observation of the facilities. The comparative method and deviant cases are part of the research design, by contrasting (comparative) the information between low, medium and high compliant firms (deviant cases). It was shown how the data was as exhaustive (comprehensive) as possible capturing the compliance process, resources development and supply chain relationships, by implementing not only qualitative, but also quantitative data collection methods. Moreover, considerable care was given to the data management, classification and analysis (data treatment).

Furthermore, external validity was achieved by cross-referencing information among supply chain partners.

The reliability of the research was assured by keeping a case database and the research protocols (Richards, 2005, p. 55). While some interviewees agreed to the disclosure of their identity and position in their organisation, for practical reasons the identity of the interviewee and organisation is not disclosed.

Comparative case studies

Understanding complex relationships between compliance, capability building, and governance structures requires attention to the firms' internal and external contexts; consequently, the research is based upon explanatory case study methods (Gyau & Spiller, 2008; O'Toole & Donaldson, 2000). This is particularly important in the compliance capability building process because multiple cases add analytical power by comparing them and picking up common patterns across the cases; furthermore, process related changes are more easily picked up by case study methods, which traditional statistical methods hardly do (Ragin, 1989).

A previous study analysing CTPAT (Sheu et al., 2006) used similar research methods, complemented with secondary data. Secondary data is necessary for comparative case analyses (Gimenez, 2006, p. 318; McCarthy & Golicic, 2002, p. 436; Seuring, 2006, p. 248). Sheu et al. (2006) analysed five cases (one custom broker, three importers and one transport provider) to understand three elements: 1) their certification processes, 2) whether and how collaboration along the international supply chain takes place, and 3) the benefits and impacts of certifications. However, in their study no reference to different compliance levels was made, or to how capabilities and resources were built. Sheu et al's study used within-case and cross-case analysis, with the former used to identify unique patterns while the later method was used to establish the relationships between independent and dependent variables (Sheu et al., 2006, p. 368). Our investigation modifies their approach, by including the identification of common patterns based on cross-case comparisons.

The relationships and common patterns will be undertaken by comparing firms by compliance levels. According to Yin's case comparisons strategies (Yin, 2003, p. 40), to refine findings at least one case per compliance level should be included.

Case study template

A reliable comparison across cases in this study required structuring the cases for easy identification of the themes. Case study templates have been used in different social sciences and engineering disciplines to facilitate comparability of co-variation patterns across cases (Aiken, Kock, & Mandviwalla, 2000; Cashore, Gale, Meidinger, & Newson, 2006; Gerring & McDermott, 2007).

Each case adhered as much as possible to a case study template. The sections of the cases include: 1) the compliance processes, 2) the security resources developed, as well as the capabilities used by firms for that purpose, and 3) the knowledge and learning mechanisms to indicate whether the firms built up capabilities based on its internal efforts or external support (supply chain or stakeholders) (see Table 3.3.1).

The first sections of the case studies present the compliance processes, as the basis for the assessment of research question 1, and which is based upon the compliance process model displayed in the analytical framework (Table 2.5.1, p.52) and explained in the compliance process section of the theory chapter (pp. 37-41). From the description of the ways firms built up capabilities and developed security resources, an identification and coding (Table 5.2, p.104) was performed to have the information for the descriptions of the compliance processes of the firms. At the end of the description a figure is displayed as a way of visual summary of the compliance processes.

After the compliance process, the case study describes the capability building and resources development processes. These sections contain the information and data required for the assessment of the research question and hypothesis 2, which, again, is based on the capability building and resource development displayed in the analytical framework and explained in the resources and capability building section of the theory chapter (p.33), and the background section (Table 4.1.1, p.100).

An additional and complementary section on internal and external sources of knowledge and learning was added to capture information related to the influence of external actors in the compliance processes, as well as in the resources and capability building processes. Each case study finalises with a table of the relationship between resources development and capability building which contains the count value of compliance capabilities built to be able to develop security resources (e.g. Table 5.1.1, p.111). After identifying the compliance level of each firm, the table feeds the database for the summary of results (statistical) and the multi value qualitative comparative analysis-mvQCA- (chapter 6, empirical).

Table 3.3.1: Case study outline/template

Themes		Description
The process		Story telling of the compliance process
Process stages	Regulatory identification	The role of stakeholders and supply chain partners for regulatory awareness
	Regulatory interpretation	Firms assessment of the regulations (public, private, and PPP) based on perception of the benefits of compliance
	Assessment of change	Firm's evaluations of the required changes and of their capacity to change.
	Compliance options and levels	Security regulations firms decided to comply with (Public, Private, and PPPs), as well as their expected degree of compliance (full, partial, delay/exit).
	Communication systems	Formal and informal communication systems
	Implementation	Describing the mechanisms for security resource development (trial and error, design and implementation, outsourced, or combinations); and the strategies to prevent interference with normal business operations.
	Evaluation and Monitoring	Actors and mechanisms for assessing the overall compliance process
	Feedback loops	Iterative connection between regulatory process stages
Summary of the compliance process (Figure)		
Security resources and capability building		Descriptions of the resources that firms argued were needed to enhance their firm and supply chain security; and descriptions their related capabilities building processes.
Resources	Business partners	Selection and screening of main business partners
	Physical security	Alarm systems, building structure, fencing, lighting, locking devises, and key controls, and so on.
	Access control	Employees, visitors, removal of unauthorised persons, and so on.
	Personnel security	Personnel backgrounds, verification and termination procedures, and so on.
	Procedural security	Manifesting, shipping, receiving, and cargo procedures and analysis, and so on.
	Information Technology Security	Identification, accountability, controls, password protection, and so on.
	Container and Trailer security	Container inspection, trailer inspection, container and trailer seals, container and trailer storage, and so on.
	Conveyance Security	Container security (in transit), conveyance inspection procedures, conveyance tracking and monitoring procedures, and so on.
	Threat awareness	Training and threat awareness for countering terrorism and smuggling
Capabilities	Organisational competencies	Internal individual and functional competencies coordination mechanisms
	Management systems	Structures and administrative control systems
	Internal coordination	Coordination across interfaces, functions and organisational divisions
	Stakeholder support	Involvement of stakeholders in the firm's strategic planning of resources development
	Supplier development	Commitments to enhance the suppliers capability building
	Vertical alignment	Bilateral support between supply chain partners
Temporal dimension		When it was available, the date of each event was included
Summary of internal and external sources of knowledge and learning for capability building		
Summary of relationship between resources development and capabilities building (Table)		

Critical point of view on the research method

The first critical point relates to **the firm as the unit of analysis** in this investigation. We examine the firms' internal compliance and capability building processes, the firms' external compliance and capability building processes (with other supply chain partners and stakeholders), and the firms' supply chain's governance structures. The latter is critical because, as described in the question and hypothesis section, although two firms may belong to the same supply chain, they may not depend to the same extent on one another, they may not have the same decision making powers, they may not have the same expectations in terms of the length of their relationship, and so on. Thus, **governance structures are not supply chain but firm-specific.**

Secondly, the fact that the investigation is a small-N comparative case study implies that only limited generalisations may be possible. Aiming at **theoretical generalisations**, as suggested elsewhere (Sheu et al., 2006, p. 363), the supply chains and firms were chosen for their exemplary value rather than for their statistical representativeness. They fall within different compliance levels, i.e. low, middle and high. This approach is important to grant the researcher the advantage of the uniqueness of each case and the emergence of themes to improve findings, as suggested by methodological experts (Eisenhardt, 1989, p. 542; Koulikofff-Souviron & Harrison, 2006, p. 270) and applied by well-established political scientists (Kogut & Ragin, 2004; Levi-Faur, 2002). Yet, since it is the common features of the compliance processes of the three stages of the supply chains what the mvQCA will try to identify, the lack of significance and presence of theoretical significance of compliance call for further empirical investigations for theoretical validations. Further, there is no reason to believe that securing the standard facilities and supply chain operations of a tomatoes exporter would be too dissimilar to securing those of a cucumber exporter or of other fresh produce exporters; or to believe that securing the transport operations of the exporter would be too dissimilar if the transport had been outsourced.

Thirdly, as will be developed in Section 3.5 Qualitative Comparative Analysis: Multi-value and Crisp Sets (p.81), our approach is based on a logical inference, which is not to be confused with a statistical inference. This is important because given the complexity of the pathways and diversity of observations, from a statistical inference view one might conclude that further observations could be inconsistent with the observed patterns. Whilst a logical inference in comparative-case studies claims that depending on the context, in which our cases are embedded, a given condition may have a different effect on the outcome, hence acknowledging the possibility of different causal paths (Rihoux, 2003, p. 353), this means there is no definite and unquestionable causality.

Hence, rather than "trying to specify a single causal model that fits the data best" – as the statistical inference would do, with the help of logical inferences with QCA we would like to "determine the number and character of the different causal models that exist among comparable cases" (Ragin, 1987, p. 167). This implies that more cases, rather than contradicting previous results, would refine and enhance multiple causal conditions or pathways to regulatory compliance based on added characteristics of the new contexts where compliance may be occurring.

3.4. Research Process

In studying cause-effect relationships between compliance process and capability building, a five stage process was used to increase validity and reliability (Seuring, 2006, p. 246). The fifth stage is the dissemination of the results of the investigation; however, since the results of the present doctoral dissertation will be publicly available, the discussion of this stage will be omitted. Hence, this section contains only four stages.

First stage: research questions

The research was grounded on *a priori* identifying constructs from the literature review and setting an analytical framework. The literature review was narrowed down to three scholarly disciplines: the Resource-Based View of the Firm, Regulation Studies, and Supply Chain Relationships. For each of them, the literature search was based on three criteria: disciplinary early contributions (from the 1950s onwards), high citations and new contributions to the disciplines.

Second stage: instrument development and case selection

The access to firms derived from a snowballing technique. The technique consisted of contacting a focal firm (i.e. the US importer), requesting them to identify their main first-tier supplier (shipper/exporter from Mexico) and closest to them in terms of compliance to CTPAT. Later, the Mexican partner provided the contact and access to the main transport provider between the Mexican and US partner, just as suggested by supply chain study specialists (Stuart, McCutcheon, Handfield, McLachlin, & Samson, 2002, p. 420).

However, the case selection was based upon initial identification of distributors having supply chain partners with similar compliance levels. The initial identification was based on perception and recommendations of the Fresh Produce Association of the Americas (FPAA) to the author, taking into account that the FPAA experience had grown as a result of the continuous exchange of information with CTPAT officials regarding the compliance of US fresh produce distributors (members) and their supply chains[39]. The selection consisted of low compliant supply chains (SC1 and SC2), middle compliant supply chains (SC3 and SC4), and high compliant supply chains[40] (SC5). The production sites of the supply chains were not as important (as long as they were in Mexico) as the location of the distribution centre, which was Nogales, Arizona, US. Yet, most of the growers were located in the province Sinaloa, whilst one was in Nayarit, the neighbour province of Sinaloa.

The research involved conducting qualitative cross-cases and single-case analysis; thus the instruments included structured and unstructured questions for each of the three types of actor. To capture how compliance capabilities were developed, unstructured, standardised interview protocols were used. The use of the questionnaire was to capture issues related to governance structures. The instruments were validated by several experts during a pilot study conducted between summer 2006 and autumn 2007 (see Table 3.4.1, p.74).

As suggested earlier, the study planned to include three supply chains, each including at most three partners (distributor, grower/shipper and transporter), for a total of nine firms.

---

[39] In this selection process, the support of the Fresh Produce Association of the Americas (FPAA) was crucial for the identification of supply chains, and for the information regarding the perception that FPAA had about the overall security/conformance levels of the potential supply chains to be sampled.
[40] SC6 was another candidate for high compliant firm, however the supply chain did not provide sufficient information for a reliable analysis, hence this supply chain was dropped from the sample.

However, during field work it was possible to contact additional supply chains. This opportunity was not only relevant to enhance robustness, but also, as will be shown later, because 12 is the best number of cases to perform relevant Qualitative Comparative Analyses with reasonable control over the complexities associated with each case study.

Fortunately, the hazard of identifying like-minded people by snowball techniques was overcome by the fact that there is a good balance of low, middle and high compliant cases, as well as a great diversity of governance structures in the supply chain relationships, as will be shown in the empirical chapters. Perhaps this was also the result of explicitly asking the industry association, Fresh Produce Association of the Americas, to nominate distributors with different levels of compliance, taking into account that the association is . This is relevant to enhance the validity of the assessment of the relationships between capability building and compliance processes, as well as between capability building and governance structures.

Table 3.4.1: Validating the instruments

Expert Validations	Institution	Classification
CEO and compliance team (four quality and safety managers)	Ganfer Sociedad Agricola, SA de CV	Grower/Packer/Exporter
Dr Vidal Salazar Solano, Senior agricultural economist	Centro de Investigacion en Alimentacion y Desarrollo, AC.	Public Research Centre
Mr Evangelos Demerutis, CEO	Trocadero CAADES-Confederacion de Asociaciones de Agricultores del Estado de Sinaloa.	Growers Industry Association
Mrs Marcela Placencia, Manager	Pacific Brokerage	Customs Broker
Alison Moore (Communications director) and Georgina Felix (Industrial Engineer)	Fresh Produce Association of the Americas	Importers/Distributors Industry Association
Mr Jacobo Escobosa, Warehouse foreman	MG-Brothers/hired by Fresh Farms	Distributor

In fact, the intention was initially to select six supply chains (18 firms in total). However, one supply chain did not provide complete information and was eliminated from the analysis (15 firms in total), one transporter was fully integrated to the grower (14 firms in total), and one more was the main transport provider for two of the supply chains included in this study (13 firms in total); further, one transport provider, although not integrated, worked in full coordination with the exporter and they provided information as if they were one single case (12 cases in total). Hence, although there were 13 firms, only 12 case studies were reported.

Third stage: Data gathering

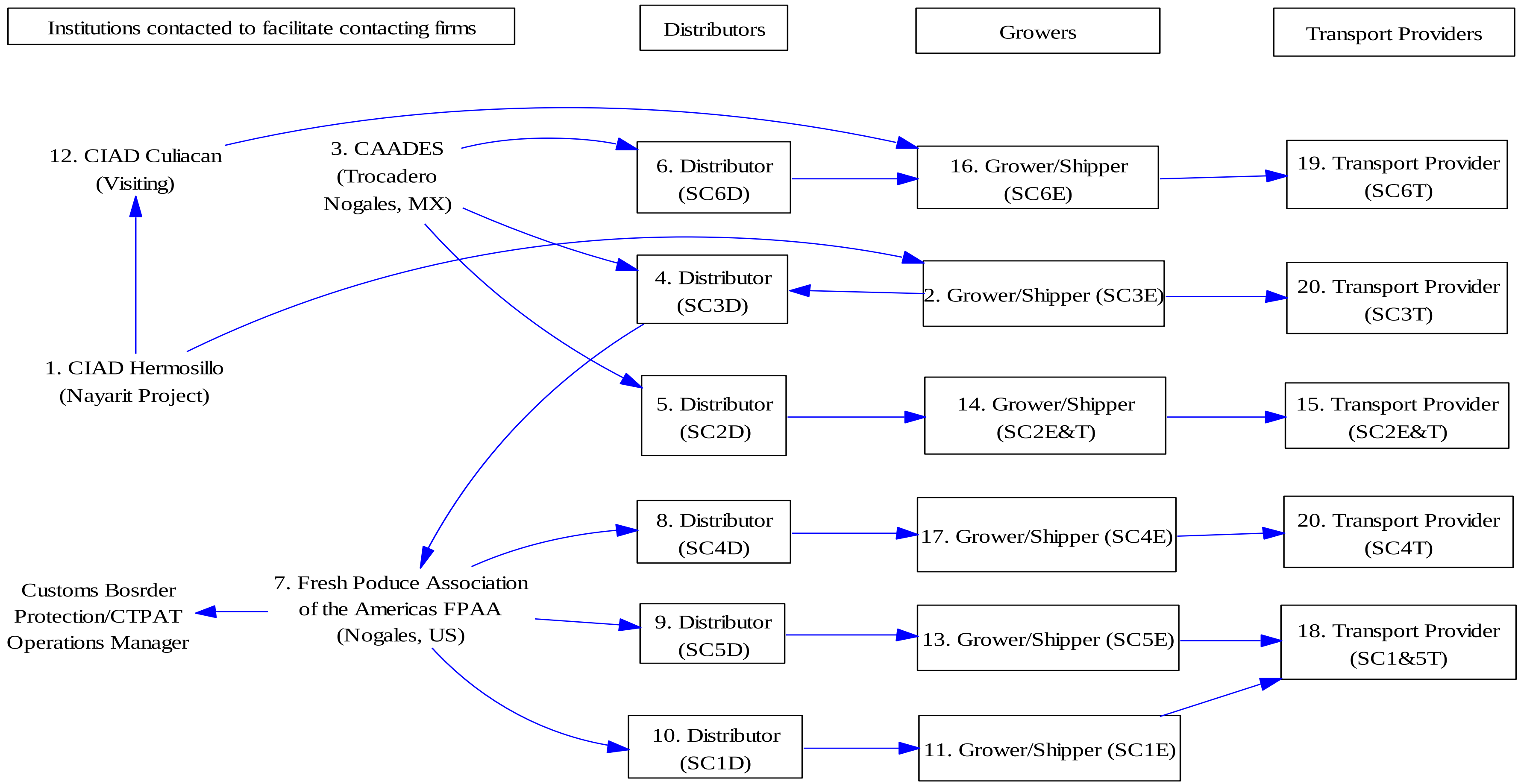
The third stage, as suggested elsewhere (Koulikofff-Souviron & Harrison, 2006, pp. 269-270; I. Stuart et al., 2002, p. 420), consisted of identifying the informants, functions, and hierarchy within the organisation. Thus, asking for the one officer in charge of implementing security-related measures in each firm, the result was that all the interviewees were either the chief executive officers (CEOs) or the compliance managers in security and safety.

Previously, the author was involved in a research project with CIAD (Food and Development Research Centre in Mexico) to investigate technology transfers and development needs in the food supply chains from Mexico (September to November 2007). It was discovered that one of the interviewees in that project was attempting to comply with CTPAT, which in turn opened up the door to the network of distributors and their supply chains (see Figure 1, p.77).

Once access was granted, the first fieldwork period started, and lasted from November 2007 to January 2008. The instrument for gathering data in the first period was an unstructured and standardised interview. The second fieldwork period was in March 2008, when the instrument for gathering data was a structured and standardised questionnaire. The first fieldwork period coincided with the beginning of the winter production and export season of fresh produce from Mexico to the United States, whilst the second fieldwork period occurred at the peak of the production and shipping season[41].

[41] During the second period the CEOs and security/compliance directors from SC6E and SC6T were too busy to provide information, which left Supply Chain 6 with incomplete information for the analysis. For that reason this supply chain was eliminated from the study.

Figure 1: Snowball technique (Firms undisclosed by request)



Fourth stage: Organising and developing the data[42]

Firstly, using field notes, reducing them to tables and coding them, the data was organised to facilitate the identification of similarities and differences across cases. As suggested elsewhere (Koulikofff-Souviron & Harrison, 2006, p. 271; Seuring, 2006, pp. 246-247; I. Stuart et al., 2002, p. 426), the strategy contributed to the identification of patterns by compliance levels, contexts, and time frames.

Fieldwork notes were directly transcribed into content-analytic matrixes, which are traditionally used for single cases (Miles & Huberman, 1994, p. 183). Each case study report summarises the content-analytical matrix, according to a case study template, thus facilitating the comparisons across cases.

The content-analytical matrix contains the information from the standardised semi-structured interviews. They reflect the development and building up of resources and capabilities. From the interviews, the first classification of information was based on the supply chain security capabilities literature (Barratt & Oke, 2007; Boske, 2006; Closs, 2005; Closs & McGarrel, 2004; Erera, 2005; Goddard, 2005; Kinser et al., 2005; H. L. Lee, 2004; LLTRM, 2004; Manning et al., 2005; Petersen et al., 2003; Rice & Spayd, 2005; Sarathy, 2006; Shannon et al., 2006; Sheu et al., 2006; Suarez-Bello, 2003), which is what structured the interviews in the first place (See appendix B), and which is reflected in the titles row of the content-analytical matrix. After the classification of interview information by supply chain security capabilities, the second classification was done according to the basic compliance process described by Henson (1998), and which is reflected in the titles column. Consequently, the content-analytic matrixes represent 'process-by-security capabilities' built by firms (see Table 3.4.2, p.80). The cells in the content-analytic matrixes contain the security resources and the capabilities built for their development. Expectedly, the resources and capabilities would be different according to the stage of the compliance process in turn. In detail, each cell contains:

- Challenges and experiences in the specific stage of the compliance process;
- Whether and how capabilities were built to meet the need of security resources; and
- Date of the events

[42] Although the fourth part should be organisation and analysis of the fieldwork data, the second part will be discussed in the next section.

The date of event is a useful variable to identify the timeframes of the compliance processes, which in turn measures the time required for compliance. The combination of this variable with the extent to which firms progress in compliance, contributed also to a variable capturing the intensity of the capability building processes.

The last capability in the content-analytic matrix is the learning and knowledge sources. This in turn, enhanced our understanding of the role of the supply chain partners and other stakeholders in the firm's capability building (see Table 3.4.2, p.80).

In addition to supporting the understanding of the capabilities and compliance processes, the matrixes served the purpose of exhaustive accounts of the resources and capabilities developed by the firms, as described by the interviewees. Hence, whenever the interviewee made reference to a capability built and the resources that such capability was trying to develop, it was numbered.

This was useful when the cases had to be revisited to verify the consistency of the analysis and the case study presentation. The numbering is similar to the coding suggested by qualitative researchers in the transcripts of data for initial analysis and to enhance the rigour of the qualitative research (Miles & Huberman, 1994, pp. 55-56; Poland, 1995). However, it was thought that the numbering may also be useful to the reader, hence its inclusion in the case studies writing up, and its summaries in the capabilities-resources matrixes at the end of each case study.

Table 3.4.2: Content-Analytical Matrix (Compliance Process by Security Capabilities Matrix)

(SC_Firm)	**Supply chain security capabilities**					
Supply chain Security Literature / **Compliance Process (Henson, 1998)**	Assessment	Visibility and monitoring	Coordination and integration	Vulnerability and risk reduction	Agility (Velocity, Variability, Predictability)	Learning and knowledge sources
Identifying regulation	1. Security resources required 2. Capabilities used 3. Time	1. Security resources required 2. Capabilities used 3. Time	1. 2. 3.	1. 2. 3.	1. Security resources required 2. Capabilities used 3. Time	1. Internal sources 2. External sources
Interpreting regulation	1. Security resources required 2. Capabilities used 3. Time	1. 2. 3.	…	…	1. 2. 3.	1. Internal sources 2. External sources
Loop to Interpret regulation: Attempt to influence regulation	…	…	…	…	…	…
Identify change (assessment of current and expected activities)	…	…	…	…	…	…
Compliance decisions: whether to comply or not (awareness of costs and benefits)	…	…	…	…	…	…
Specifying the method of compliance (Available options)	…	…	…	…	…	…
Communication	1. 2. 3.	…	…	…	…	1. 2.
Implementation	1. Security resources required 2. Capabilities used 3. Time	1. 2. 3.	…	…	1. 2. 3.	1. Internal sources 2. External sources
Evaluation and monitoring	1. Security resources required 2. Capabilities used 3. Time	1. Security resources required 2. Capabilities used 3. Time	1. 2. 3.	1. 2. 3.	1. Security resources required 2. Capabilities used 3. Time	1. Internal sources 2. External sources

Adapted from Miles and Huberman (1994, p.183)

3.5. Qualitative Comparative Analysis: Multi-value and Crisp Sets

After organising, summarising and coding, the research moved onto the analysis. In a previous section, it was noted that this is a small-N research design; therefore traditional parametric tests of statistical significances are unreliable (Field, 2009).

Other very powerful and novel options are the re-sampling methods, such as bootstrapping and permutation tests. However their assumptions include random sampling and independent variables (Good, 2006, p. 95). These assumptions do not adhere to the needs of the present investigation, which include systematic sample selection (i.e. by compliance levels) and testing whether the value of capabilities and resources are complementary or interdependent, rather than assuming independence between variables.

Thus, cross-case displays for ordering and explanations based on presence causal-effect and associative analysis was used (Miles & Huberman, 1994, p. 207; Ritchie & Lewis, 2003, p. 250; Silverman, 2005, p. 202), which is the basis of the comparative case study methods.

The analytical method in this investigation is the Qualitative Comparative Analysis (QCA). This, as with other comparative approaches, studies how different conditions combine in one setting and compare it with how they combine in another setting, to unveil the convergent causal conditions of a setting (Ragin, 1989, p. 13).

The Qualitative Comparative Analysis applies John Stuart Mill's (1867) method to assess causality (Vink & Van Vliet, 2009, p. 272). It helps to identify a cause even when it is small in relation to many changeable related causes that may be jointly causing a certain effect.

The advantage of this method is that is logical (Boolean), combinatorial, highlights irregularities for further investigation, does not require a representative sample of the population, and it is compatible with the vocabulary of necessary and sufficient causation; which is valuable for assessing the limits of social scientific generalisations (Kogut, MacDuffie, & Ragin, 2004; Kogut & Ragin, 2004, 2006, p. 46; Ragin, 1989, pp. 15,16, 101, 2000, pp. 5, 13, 88). All in all, it helps assess relationships for theoretical generalisations while exploring different configurations of explanatory variables with small sample sizes.

For instance, assume A, B and C, may be causal conditions of innovation (Y). Displaying all the possible combinations of A, B, and C, and the presence (Y) or not (y) of innovation, we have the following possible configurations (see Table 3.5.1).

Table 3.5.1: Illustrative example of the Boolean logic

Causal configurations			Effects
A	B	C	**Y**
A	B	c	y
A	B	C	**Y**
A	B	c	y
a	B	C	y
a	B	c	y
a	B	C	y
a	B	c	y
A		C	**Y**

In the illustrative example, innovation (Y) happens when both A and C are present. If one of those is not present, innovation does not happen.

In this investigation the multi-value Qualitative Comparative Analysis (mvQCA) was chosen to test the causal conditions of compliance, which is one of the three existing QCAs methods[43]. The mvQCA is a generalised method considered the best choice when investigations are of small to medium sample sizes, also when the richness of information to be handled is higher than in standard quantitative methods. It is perfect when the datasets include between 10 to 15 cases (Cronqvist, 2005; Ragin, 1989, 2000).

The disadvantage of the method is that the dependent variable can only take dichotomous values, which requires running more than one analysis when the dependent variable has more than three categories (Herrmann & Cronqvist, 2009; Rihoux, 2006, p. 686; Vink &

[43] The three methods are the Crisp Sets (csQCA), Multi-value (mvQCA) and the Fuzzy sets (fsQCA). The first method allows only dichotomic variables. The second method allows multiple values, yet, they are all categorical. The third method allows scale variables; however, the software available for this method is not as user friendly as the software for the mvQCA.

Van Vliet, 2009, p. 266). However, as the empirical analyses will show, it does not represent a problem.

Another potential issue with the mvQCA is that the variables denote only categories. Even if the variables are ordinal or scale, each one of the values of the variables will be taken as nominal (Vink & Van Vliet, 2009, p. 266). This may be a problem for investigations where there is need to quantify or establish marginal relationships. However, in this investigation the qualitative character of the variables is maintained; hence, the causal conditions are only categorical. Rather than unveiling a trajectory from low to high (i.e. compliance levels), the analysis identifies the causal conditions at each one of those levels.

In general the method for QCA consists of three phases:

1) cases selection (described in the second stage of the research process) and identifying causal conditions (using the Boolean logic);
2) testing the sufficiency and necessity of the causal conditions; and
3) evaluation and interpretation of results (Kogut & Ragin, 2006, p. 49).

In the first phase, the identification of causal conditions based on mvQCA requires three additional steps:

1) *Setting up a table that shows whether the causal conditions and the outputs are present or not*. Since the mvQCA allows for multi-values, the conditions (scale or ordinal variables) do not need to be dichotomous; however the output (dependent variable) needs to be dichotomous;
2) *Constructing a truth table listing all the possible logical combinations of causal conditions*. In this step, if the variables are multi-value, thresholds should be set, indicating when a range of the variable represents a different category from other ranges of the same variables (e.g. compliance may be broken down into two or three categories: low compliance, middle compliance and high compliance); and
3) *Applying the Boolean algebra to identify the causal conditions of the outputs* (i.e. in our examples of compliance: causal conditions of low compliance, causal conditions of middle compliance, and causal conditions of high compliance) (Mill, 1867, p. 318).

If the researcher finds contradictions (e.g. **Y** and y) in the outcome derived from the same causal configurations, Herrmann and Cronqvist (2009) suggest adding thresholds to the causal conditions, i.e. changing the variables from crisp to multi-values, but trying to keep a low number of categories in the variable to reduce complexity, which helps identify more parsimonious solutions (Herrmann & Cronqvist, 2009, pp. 35-38).

In the second phase, a cause is necessary and sufficient if it is the only cause producing an outcome; a cause is necessary but not sufficient when is present together with other causes, and they all produce the outcome; a cause is sufficient when it is able to produce the outcome, but it may be that it is missing and other causes can still produce the outcome; finally, the cause is neither necessary nor sufficient if it appears in various causal configurations, but not in all (Mill, 1867, p. 206).

Although the lexicon suggests that we are testing causality, it is not actually argued that the causal conditions are the reason for compliance to exist, but only that they **co-exist**. This is what statisticians call co-variance.

This thesis subscribes to the interpretation of 'cause-effect' as described by Mill (1867), which represents a 'relation of co-existence'. In other words, if compliance exists and underlying causal conditions are present, this is because they co-exist, not because the causal conditions originated or produced compliance.

The QCA have also been subject of various critiques. The most important are: there are limited number of causal conditions (variables) to be analysed, dichotomisation of variables obscures complexity; it is difficult to capture marginal and dynamic (temporal) effects (Caren & Panofsky, 2005, p. 147; Cortina, 1993, pp. 915-922; Lieberson, 2004, pp. 13-14). However, new methodological contributions try to take note of these limitations. For instance rather than including a quantitative variables in two points in time, a fixed time effect would be applied, to capture the total change in the dependent variable, and same for the independent variables, in a specified (fixed) time period, so to assess whether the change in the dependent variable was caused by changes in a variable, or by a combination of changes in of the a set of independent variables (Hino, 2009; Ragin & Strand, 2008). Further, the limited number of causal conditions for assessment in the QCA, is now limited to the computing capacity of the researcher's equipment, thanks to the development of the algorithms for STATA (Longest & Vaisey, 2008).

The analysis is run in the software TOSMANA-Tool for Small-N Analysis, which together with the Multi-Value Qualitative Comparative Analysis was developed by Cronqvist (Cronqvist, 2009). Furthermore, due to the prolific use of TOSMANA, an appendix was included with a guide to read the software reports (See Appendix D: Guide to Read TOSMANA Reports, p.324).

3.6. Summary

This chapter presented the methodology devised to address the thesis aim, objective, questions and the corresponding hypotheses. It presented the way the research was designed, yet because there is always room for improvement, it included a section with a critical view regarding the research method. Also we presented the actual process followed during the research as an attempt as a way to transparency and replicability of the research. Finally, the section presented the key concepts to use throughout the rest of the thesis, and a brief description of the qualitative comparative analysis, from which the hypotheses were tested. The next section, will present the background ad context information of the supply chains that were subject of study. Followed by the case studies, analysis and conclusions.

4. CHAPTER 4 Background

This chapter first contextualises the Mexican agri-business industry and its main fresh produce supply chains for exports to the United States. It describes the most relevant post 9/11 security regulations and details the Public Private Partnership regulation, which is the regulation whose effect is under investigation.

4.1. Supply Chains and Post 9/11 Security Regulation

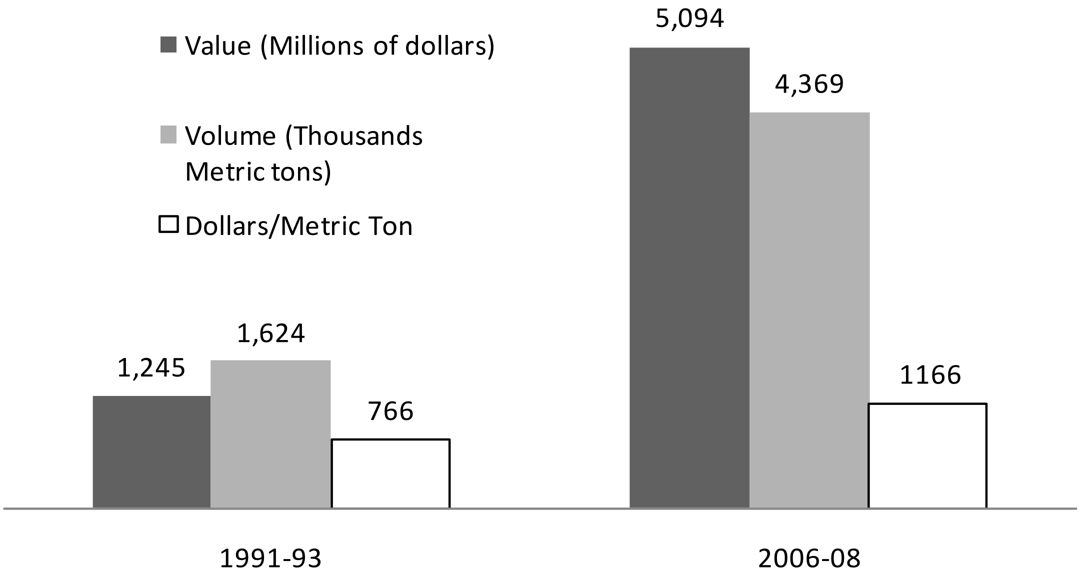
Mexico-US Agri-business[44]

The demand for fresh produce in the United States has changed over the last two decades. The consumption of fresh fruit increased from 88.7 pounds to 101.2 pounds per person between 1983-85 and 2003-05. The consumption of fresh vegetables rose from 123.2 pounds to 173.5 pounds per person in the same period. Not only US but also other international producers benefited from that trend in consumption. Imports accounted for 50% of the growth in fresh vegetable consumption and 25% of the growth of fresh fruit consumption (Huang & Huang, 2007, p. 10).

US imports of produce from Mexico also grew steadily. The movement of fruit and vegetables from Mexico to the US increased by 169% of the initial volume: from 1991-1993 to 2006-2008 it increased from 1.6 to 4.3 million metric tons. More notable is the size of the increase in the value of such exports, which was 309% of the initial level: in absolute terms this was an increase from US$1.2 to US$5 billion in the same period (see Chart 1, p.87).

[44] The supply chain and logistical description in this section is based on the present investigations as well as previous publications (Borbon-Galvez, 1998, 2000, 2001, 2004; Wong-Gonzalez, 2005).

Chart 1: United States imports of produce from Mexico from 1991-1993 to 2006-2008 (Thousands metric tons and millions of dollars)

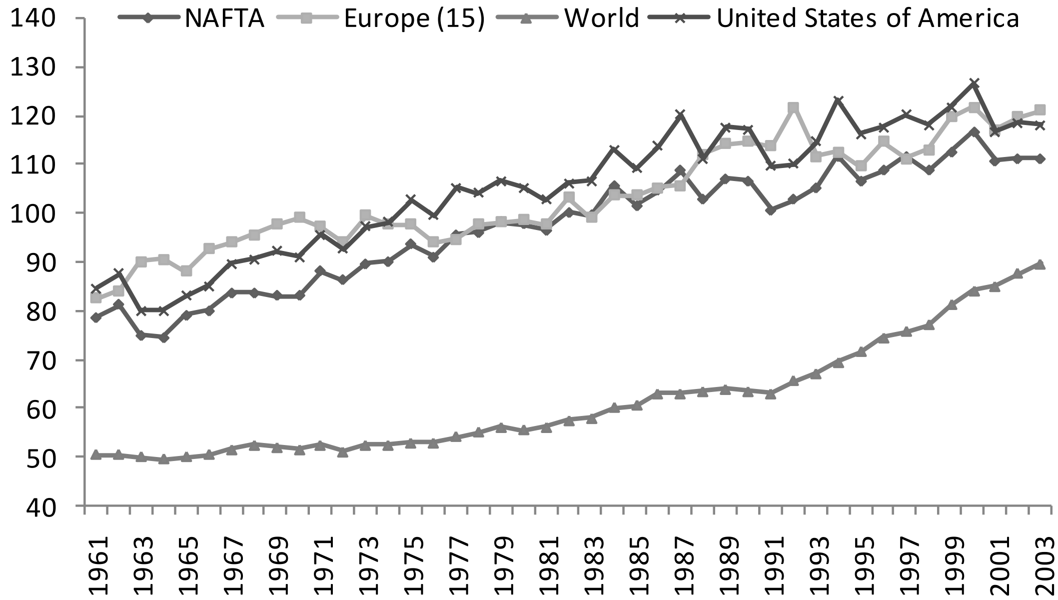


Source: Elaborated based on USDA/FAS, US Internet Trade System. Access 24 August 2009

Data from the UN Food and Agriculture Organisation (FAO), suggests that the consumption of fresh produce had been growing all over the world. The main consumers were the European Union (EU-15) and the North American Free Trade Agreement (NAFTA) area. Interestingly, the rest of the world, on average, grew at about the same rate as the EU and the NAFTA countries, albeit lagging until 1991 and then began growing faster (see Chart 2, p.88).

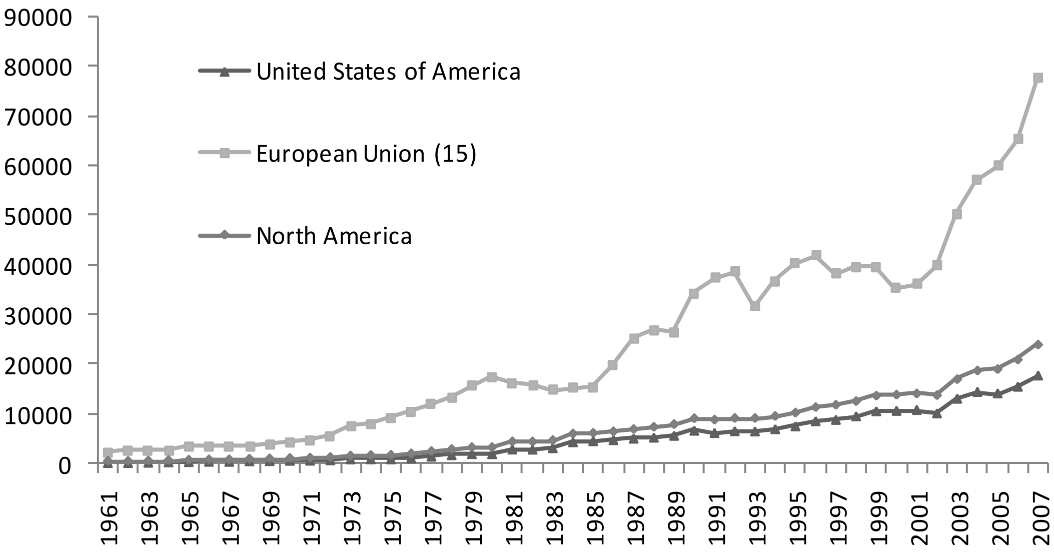
Such consumption trends have been followed by the international trade of fresh produce. The EU-15 have increased its imports since the late 1970s and again after 2001, while a noticeable growth in North America was experienced in the late 1980s followed by NAFTA and another period of growth in 2002 (see Chart 3, p.88).

Chart 2: Fruit and vegetable consumption by selected regions. (Kilos/per capita/per year)



Source: Elaborated based on faostat.fao.org. Accessed 24 August 2009

Chart 3: Import Value (Million US dollars)



Source: Elaborated based on faostat.fao.org. Accessed 24 august 2009

Maranon (1997) argued that North American agri-business influenced the transformation of Latin American agricultural activities (Maranon, 1997). The leading US southern distributors were also growers, whom, driven by insufficient production during winter seasons, engaged with Mexican growers. Their role was more than just consolidating US and Mexican agricultural products for the US markets; they were the main capacity builders of the Mexican fresh produce exports, providing technological, knowledge, and financial support (Borbon-Galvez, 2000, pp. 6, 75; Salazar-Solano, Sandoval, & Wong-Gonzalez, 1999).

The growth of the production and consumption of fresh produce had influenced the US-Mexican agricultural trade since before NAFTA; they created alliances, mergers, and acquisitions at all stages of the supply chain (Boehlje, Akridge, & Downey, 1995; Cook, 1998). Also, many US distributors/growers secured sufficient supplies of fresh produce, mainly during the winter seasons. For this, they engaged in yearly contractual arrangements for the distribution of given shares of the Mexican production for exports (Dimitri & Oberholtzer, 2009; Rama & Rello, 1979).

The organisational, productive, technological, trade, and logistical strategies developed by the Mexico-US industry substantially reduced intermediation costs, transaction costs, availability risks, and variability of year round supply (Calvin & Barrios, 1999; Goldberg, 2007, p. 5; P. N. Wilson & Thompson, 2003, p. 30; P. N. Wilson, Thompson, & Cook, 1997).

Hence, a hate-love relationship between US and Mexican growers developed; more of hate during the summer seasons, when they were competing for the same markets; and more of love during the winter seasons, when they have to consolidate production from different growing sites to meet the demand[45].

However, these trends were not felt equally across all Mexican regions. Two Mexican States, located on the northwest coast, produced around 50% of the total value of winter produce (the normal export season to the US) (see Chart 4, p.90).

[45] According to a Congressional Research Service Report for the Members and Committees of the US Congress (RL34468), the counter-seasonal imports had not only complemented US production, but also the extension of the US production season had narrowed down the winter window for foreign suppliers, yet, the net US imports had grown steadily from 1999 to 2009. http://www.fas.org/sgp/crs/misc/RL34468.pdf

The main growers from Mexico had a natural access to the US with the Canada-US-Mexico (Canamex) corridor, used by Mexicans to move their exports and supply the western US markets, through Nogales[46], the main port of entry to the US. This port of entry had been the most specialised in the US in cross-border operations of fresh produce. It moved around 55% of the total US imported produce from Mexico to US (Wong-Gonzalez, 2005).

Chart 4: Share of autumn-winter production value of main Mexican States

Rank	State	2007	Cumulative	2000	Cumulative	1992	Cumulative
1	SINALOA	44%	44%	43%	43%	27%	27%
2	SONORA	14%	58%	14%	57%	15%	42%
3	TAMAULIPAS	8%	66%	1%	59%	11%	53%
4	GUANAJUATO	5%	71%	6%	64%	10%	63%
5	BAJA CALIFORNIA	5%	76%	8%	72%	6%	69%
6	MICHOACAN	4%	80%	5%	77%	6%	74%
7	JALISCO	3%	83%	3%	80%	2%	77%
8	PUEBLA	2%	84%	1%	81%	2%	79%
9	BAJA CALIFORNIA SUR	2%	86%	1%	83%	2%	81%
10	MEXICO	2%	88%	1%	84%	2%	83%
11	NAYARIT	1%	89%	3%	87%	2%	85%
12	GUERRERO	1%	91%	2%	88%	2%	86%

Source: Elaborated based on SIAP/SAGARPA www.siap.gob.mx, Access 25 August 2009

46 There are two Nogales cities, one on the Mexican (Nogales-Son) and other on the US (Nogales-Az) side of the border.

Figure 2: CANAMEX Corridor

Source: www.canamex.org, in Wong-Gonzalez (2005)

Moreover, the demand for cross-border crossing of fresh produce from Mexico to the US throughout Nogales increased from around 58,000 thousands cross-border crossings crossing in 1992-93 to 100,000 in 2005-06, which represents an increase of over 70%. The most export intensive season of fresh produce from Mexico to the US had historically been January to March. Nogales port of entry traded over 60% of the yearly exports for all agricultural products to the US, and in the 2006-2007 season it saw a cross-border operation every 30 seconds, a maximum of 1000 trucks per day in 10 hours of service (CAADES/CIDH, 2007).

Mexico-US fresh Produce Supply Chains[47]

Moving fresh produce to the US requires an important logistical activity organised across a number of actors. First, not all the small and medium sized produce growers in Mexico had enough supply or packing capacity. In some cases, they had to sell to large growers who were already operating in international markets, or sell to consolidators or brokers. The consolidator/broker did not actually grow anything but purchased or distributed produce from various growers who were individually unable to supply because of their low production volume.

Later the produce needed to be labelled and packed. This stage was crucial to sustain the traceability of the produce, and had been supported with coding and information systems to trace the produce back to its origins. This required high precision to identify the different growers of consolidated cargos.

Often, large firms had internal packing facilities. Since they did not deal with multiple growers their traceability systems were more reliable. However, they still dealt with multiple origins of the produce, and needed to know where and when the produce was picked up from.

Once the produce had been packed and labelled, it was normally transferred to a cooling warehouse where it was treated to reduce its temperature and (in some cases) to keep the environment controlled. This is where the cold chain normally started, requiring control over the produce's environmental conditions to regulate its shelf life[48].

[47] The supply chain and logistical description in this section is based on observations in the present investigations, as much as observations in previous investigations, reported in several publications (Borbon-Galvez, 1998, 2000, 2001, 2004; Nunez-Noriega & Salazar-Solano, 2007; Wong-Gonzalez, 2005).

[48] Shelf life is the time lapse between harvest and the moment in which the product has gone bad. There are various systems used by the Mexican agri-food chains to control various gases in the environment such as ozone, oxygen, carbon dioxide, ethylene, etc., which allows regulation of the shelf life of the produce. For instance, in the packing facilities, melons (honey dew) may be treated with ethylene at 20ºC, followed by being washed with cold water. In the warehouse, they may be stored at 7ºC with 90% relative humidity, 10-15% CO_2 and 3% O_2, to achieve 3-4 weeks of shelf life (Borbon-Galvez, 1998, p. 30).

The next stage in the chain involved sending the produce from the shipping point in Mexico to the US distributor's warehouse[49]. However, between those supply chain stages were various inspection points, some of which were the subject of complaints from the fresh food industry. The Mexican Secretary of Defense used inspection points to search for drugs. Such inspections increased the lead times of cargo in transit[50].

Further inspection points were located in Nogales-Son[51] before the US port of entry. These were dedicated to ensuring the cargo was in perfect condition, and performing logistical operations to change from double trailer hauling per truck (which is legal in Mexico but not allowed in some of the US national highway network, nor in critical highways of Arizona) to single trailer hauling per truck (legal and allowed in both the US and Mexico)[52].

In the distributors' warehouse, the produce could be arranged according to the needs of each buyer. Growers may have had different distributors, according to the distributors' specialty. There were also re-packers, who used to take advantage of the fact that some growers choose to classify top quality produce as lower grade. The grower does it to make sure the consumer only gets the expected or higher quality, to maintain the market. However, re-packers might re-classify produce and charge a premium price for the top quality produce.

---

[49] There are different economic entities that may control various stages of the supply chain, which will be indicated by adding the sections the entity controls, for instance: grower, grower/packer, exporter, packer/exporter, grower/packer/exporter, grower/consolidator/packer/exporter, so on.

[50] One of the inspection points (Benjamin Hill, Sonora) was modernised, and new technology is used to screen the cargo without physical manoeuvre, using X-Rays and Gamma Rays. The time to realise 100% inspection of the cargo was reduced from 60 minutes to 3 minutes. Another two critical inspection points were removed (El Desengano, and Potam) on 17 February 2009. However, the new inspection point started operations at the end of the export season on 27 April 2009 (the export season is normally November to May), hence the effects of the new technologies and inspections operations will be seen during the next export season (November 2009 to May 2010), and specially in January, February and March, which are the pick of the export season.

[51] Trocadero de CAADES (Confederacion de Asociaciones de Agricultores del Estado de Sinaloa) is one of the most important facilities for inspection in the city, serving member and non-members of the association.

[52] It is the practice that Mexican long-haul trucks carry two trailers; on the other hand, the US Federal Highway Administration, which is the agency responsible to regulate and enforce the Surface Transportation Assistance Act of 1982 and its amendments (72 FR 7747, Feb. 20, 2007), imposed a freeze to the truck and trailer sizes, weights, and routes using the national highway network that forbids the truck-trailer-trailer combinations, but only allows truck-trailer-semitrailer combinations. Although States are allowed to set their own limits on inter-state regulations, the routes across the US are not uniformly connected, such that makes it economically impractical for Mexican long-haul trucks-trailer-trailer to operate in the US. In the State of Arizona for instance, the only inter-state route allowed to operate truck-trailer-trailer combinations are the inter-state from Nevada to Utah, and other limited connections to New Mexico (FHWA/USDOT, 1984).

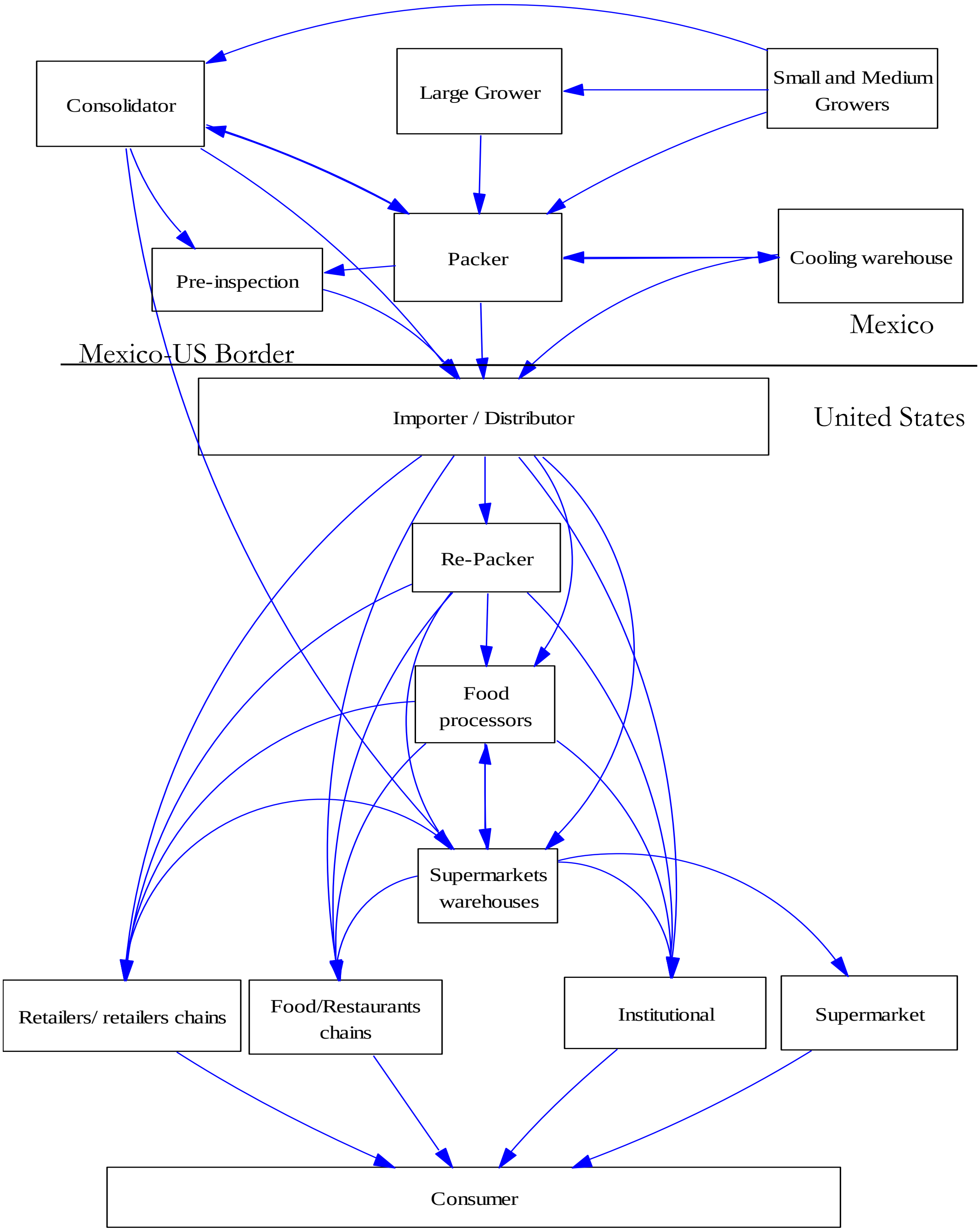
In the US, the market comprised a complex network of commercial or wholesale buyers. Each buyer had specific food standards related to quality, safety, security, environment, and social issues. The buyers ranged from food processors, supermarkets, food and restaurant chains, retailers, to institutional buyers (educational, hotels, and public administration).

The purchases along the chain were only unidirectional; it appeared more like a network than a chain. For instance, some food processors used to buy from supermarket warehouses and then sold semi and fully processed food back to the supermarket warehouse.

Some factors might have had negative effects on Mexico-US supply chains performances. One of them was the lack of feedback controls systems between partners, leading to increasing variability in lead times and lack of traceability capability of the systems (van der Vorst, Beulens, de Wit, & van Beek, 1998); this had been commonly known as the *bullwhip effect*[53]. Another big issue was the use of supply chains for illegal purposes. A third important factor was the presence of foodborne illnesses. Others included: inefficient facility designs, inefficient monitoring and information systems/technologies, lack of training, non-existence of alternative SCs and logistics in case of emergencies, increased complexity of regulatory environment, etc. (Nunez-Noriega & Salazar-Solano, 2007; Wong-Gonzalez, 2005).

[53] "The bullwhip or whiplash effect refers to the phenomenon where orders to the supplier tend to have larger variances than sales to the buyer (i.e. demand distortion), and the distortion propagates upstream in an amplified form (i.e. variance amplification)" (Lee, Padmanabhan, & Whang, 1997, p. 546).

Figure 3: The Basic Fresh Produce Supply Chain from Mexico to United States



Source: The author

Post 9/11 security regulatory regimes: safeguarding the food chains

As noted earlier, one of the main concerns in the international trade of fresh produce to the US had been the control of foodborne illness. Harris *et al.* (2003) identified a growing number of outbreaks in the US over the years. They stressed that although pathogens rarely reproduce on the outer surfaces of most fresh fruit and vegetables, pathogens survival and multiplication is enhanced under broken epidermal barriers of the fruit and vegetables. Environmental conditions will hardly affect their survival, and some pathogens only need a very small dose to provoke illnesses. What is more, the increased complex logistical systems and use of modified environments characteristics of the food supply chains had driven the growth rates of pathogens, such as Salmonella, E. Coli, C. Botulinum, and others (Harris et al., 2003, p. 86). On the other hand, although leafy greens have been seen capable of retaining pathogens due to their vascular structure, a recent investigation showed no evidence of retention in spinach (Perry, 2011, p. 7). However when lettuce is bruised during harvest or at the processing plants, the plant releases hydrogen peroxide, stressing the E. coli and leading the pathogen to activate genes to overcome the stress. Once such genes have been activated, E. coli can withstand chlorine - the most frequent sanitizer in the food industry for washing and processing (Wood, 2011, p. 14).

As a result, there were sound concerns of risks of conducting bioterrorism attacks by disseminating biological agents through insects, contamination of water and food supply, contact, spreading powders, liquids and aerosols (Cordesman, 2001), or by deliberate damage to plants that are exposed to pathogens.

Zilinskas (2003) noted that the risk of BW attacks may have lowered by involving critical stakeholders. In fact, he suggested that responsibilities had already been transferred to non-state parties to counter and even to respond to bioterrorism. However, this suggests that new security policies required understanding the vulnerabilities of the new stakeholders, to develop the appropriate technological capabilities to prevent or mitigate such activities (Zilinskas, 2003).

Although food supply systems were not the most likely or best delivery mechanism for bioterrorist attacks (Zilinskas, 2003), there were incentives for the State and the international food supply chain to ensure security. Firstly, the fresh produce exporters had always been concerned with the potential closure of cross-border operations and the damage to their reputational capital associated with delivering dangerous biological agents (Palac-McMiken, 2004)[54].

Secondly, there might have always been benefits of compliance. For instance, a previous study showed estimations that CTPAT certified agribusiness might have reduced the maximum cross-border operations times by certified truck from 17 to 4 hours. In addition, a combination of public and private efforts to improve efficiency through security had the potential to bring maximum times of cross-border operations down to 1.5 hours, which means increasing the actual efficiency measures in lead times by more than 1000% (Wong-Gonzalez, 2005).

The attacks on 11 September 2001, reinforced the need to enhance the security of the United States. In November 2001, the US Customs Border Protection (CBP) and industry representatives developed a programme called Customs-Trade Partnership Against Terrorism (Flynn, 2004:105), a public-private partnership regulatory regime (PPP) that aimed to reduce the risks of terrorists' attacks on the US population through international supply chains.

Soon after, the US Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (US BioAct 2002), which President Bush signed into law on 12 June 2002. This took the form of a traditional command-control public regulatory regime (PR) aimed at preparing American society to prevent and respond to bioterrorism.

Later, in September 2003, the programme 'Free and Secure Trade' (FAST) was published by the CBP to update an electronic cargo release system prototype set in 1997 and published in the Federal Register (62 FR 14731) (Department of Homeland Security, 2003). This was aimed at gathering advance information and expediting cargo release from the border.

[54] An example of what the industry might face is the case of the Tylenol Effect. Two decades ago seven people died after taking Extra-Strength Tylenol that had been laced with cyanide and placed on Chicago-area pharmacy shelves. Tylenol manufacturer Johnson & Johnson initiated one of the largest drug recalls in US history at a cost of more than US$100 million. The company stopped producing capsules and replaced them with caplets as well as unveiling new tamper-resistant packaging, which has now become the industry norm. Congress then passed legislation making drug tampering a federal offence (Fintor, 2002).

Public regulation

Section 307 of Subtitle A of Title III of the US BioAct 2002, required exporters (Mexican) to issue a Prior Notice (PN) to the FDA that a food shipment would arrive at a US port of entry by truck (US BioAct 2002, pp. 670-671). Prior notice (PN) required *ex ante* knowledge of the conditions of the food shipment, such as US port of entry, arrival time, cargo conditions, importer, exporter, Transport Company, truck, and driver specified in the PN.

Although the regulation required very straightforward information, the Fresh Produce Association of the Americas, together with several distributors and agri-businesses, expressed their concerns that such measures did not consider the complexities of the Mexico-US fresh produce supply chains. Furthermore, they commented on the dockets of the Prior Notice[55], that there should be better coordination between the FDA and the Customs Border Protection (CBP), allowing CTPAT/FAST certified firms to issue a Prior Notice at the same time it was issued to the CBP, 1.5 hours before arrival at the port of entry. This had important consequences, as shipment information may have needed to be changed after re-packing, re-loading, changing driver, change of trailer, etc. As a result, shipments needed to wait at least two more hours on the highway before they were able to join the border queues, whilst the FDA analysed the information to decide whether to grant access to the shipment.

Public Private Partnership Regulation: CTPAT/FAST

CTPAT was launched on 16 April 2002 as a voluntary programme that consisted in enhancing the supply chain security practices (Laden, 2007, p. 83). The Customs Border Protection (CBP) would issue a certification of partnership with CTPAT. Participating in the programme gave a number of benefits to its members, as it reduced the number of inspections at the border, provided priority in processing inspections, assigned a supply chain security specialist, members would become eligible for self-policing, and they would be allowed to attend CTPAT supply chain security training seminars.

[55] http://www.fda.gov/ohrms/dockets/dockets/02n0278/02n0278.htm

Its related programme was FAST, which is exclusive for transport providers, and that gave similar benefits as CTPAT. The difference was that it allowed members to use FAST lanes to cross the border, and advanced technology to clear the cargo and cross the border in few minutes. However, to be eligible to use the FAST lanes, not only the transport provider had to be a member, the driver must have had a FAST-commercial driver card, the cargo should belong to a CTPAT certified exporter/packer, and it had to be destined to a CTPAT certified importer. This combination of memberships allowed advanced electronic cargo information transmission to the CBP, and expedited cargo processing based on risk assessment[56] (C-TPAT/CBP, 2006).

The guidelines and criteria were tailored for each partner of the SC[57], however, they all had to develop resources for the various security aspects (See Table 4.1.1).

According to the level of compliance, CTPAT granted three different certifications (tiers). First, for those meeting the minimum criteria that were not yet validated *in situ*, second for those validated, and third for those exceeding the minimum criteria. The main advantage of acquiring higher levels of compliance had been the reduction of rate of inspections in customs based on risk assessments[58]. This implied a reduction in lead times across the border, where the third level meant the closest to having the status of "green light" for cargo at customs. The best practices and technologies applied by higher compliant firms were used to continuously update a document for communicating SC security best practices (C-TPAT/CBP, 2006, p. 4).

To sum up, in order to obtain the benefits of the CTPAT/FAST programmes, at least the Mexican exporter (Foreign Manufacturer), Mexican transport provider (Long Haul Carrier in Mexico), driver (with FAST-Commercial Driver Card), and distributor (Importer) had to be certified. This extended the lead certified firms' external controls over their providers and clients to meet the same requirements, and this might have been done by specifying it in their contractual arrangements.

---

[56] For information on the development of the programme, see http://edocket.access.gpo.gov/2003/pdf/03-24260.pdf.

[57] There are Third Party Logistics Providers, Marine Port Authority and Terminal Operators, Long Haul Carriers in Mexico, Customs Brokers, Air Carriers, Rail Carriers, Foreign Manufacturers, Highway Carriers, Importers, Sea Carriers, Air Freight Consolidators, Ocean Transportation Intermediaries, and for Non-Vessel Operating Common Carriers.

[58] In case of another incident like 9/11, only CTPAT certified firms will have access in case of closing borders to international trade.

Table 4.1.1: CTPAT Security criteria/guidelines sections

Section	Criteria/guidelines
Business partner requirement	Participation/certification in foreign customs administrations SC security programmes Point of origin Security procedures (service provider screening and selection procedures and customer screening procedures) Other internal criteria for selection
Physical security	Alarms systems & video surveillance cameras Building structure Fencing Gates and gate houses Lighting Locking devices and key controls Parking
Physical access controls	Challenging and removing unauthorized persons Deliveries (including mail) Employees (authorised access) Visitors Visitors/vendors/service providers
Personnel security	Background checks / investigations Personnel termination procedures Pre-employment verification
Procedural security	Bill of lading/manifesting procedures Cargo (traceability) Cargo discrepancies Document review Documentation processing Manifesting procedures Shipping & receiving
Information technology security	Accountability Fast transponder controls Password protection
Container and trailer security	Container inspection Trailer inspections Container and trailer seals (ISO 17712) Container and trailer storage
Conveyance security	Conveyance inspection procedures Conveyance tracking and monitoring procedures
Security training and threat awareness	

Source: CBP.www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat

However, there were firms unable to comply with CTPAT/FAST even though they had committed resources to enhance their security practices. The rate of non-compliance is relatively high given the number of rejections of applications for certification in CTPAT. In April 2005 there were 4,574 certified firms out of 8,297 applications, so that 18% were rejected and 26% were pending information (see Table 4.1.2, p.102).

In 2006, from more than 10,000 firms applying for the certification, 6,000 had been accepted (C-TPAT/CBP, 2006, p. iii, 2007, p. 3). Although this data does not show rejected and pending applications, 4,000 out of 10,000 applications did not receive certification, which suggests that 40% of the firms were unable to develop the necessary resources for compliance. Extrapolating statistics from April 2005, in 2006 the number of rejected applications was around 1,800, and 2,600 of the applications would had been pending due to insufficient information being provided by the firms. Interestingly, there was no apparent change in the rate of non-compliance. This meant that either potential supply was not negotiated and re-channelled through complying channels, or the supply entered the market with lower efficiencies compared to complying channels, accumulating fewer benefits in the long run yet with higher risks than compliant channels.

Furthermore, data revealed that non-US parties of international SCs were the ones striving more to meet CTPAT security regulations, especially Mexican firms who, without considering pending applications, have the lowest certification to rejection ratio (See Table 4.1.2, p.102).

To conclude, the Mexico-US fresh produce supply chains have had to face challenges in their everyday operations, including the awareness of illegal immigrants and drug smugglers. It seems that the post 9/11 security regulations added to those challenges. However, the adverse effects of the security regulations may have been mitigated with the incentives associated with compliance. It might be advisable for the Mexico-US agri-businesses to engage with such measures, given the benefits for both brought by their growing international trade.

Table 4.1.2: CTPAT Statistics (April 2005)

Business Type	Certified	Rejected	Certified to Rejection Ratio (CRR= Certified/Rejected)	Pending Additional Info.	**Grand Total**	**Sector Share**
Air Carrier	26	7	3.7	6	**39**	**0%**
Consolidator, NVOCC, Ocean Trans Inter, Intl Air	428	59	7.3	153	**640**	**8%**
Importer	2521	794	3.2	1315	**4630**	**56%**
Licensed U.S. Customs Broker	505	59	8.6	133	**697**	**8%**
Mexican Non-Related Manufacturer	10	13	0.8	30	**53**	**1%**
Mexican Related-Party Manufacturer	118	67	1.8	105	**290**	**3%**
Rail Carrier	7	1	7.0	4	**12**	**0%**
Sea Carrier	74	18	4.1	29	**121**	**1%**
U.S. / Canada Highway Carrier	719	304	2.4	244	**1267**	**15%**
U.S. / Mexico Highway Carrier	142	203	0.7	155	**500**	**6%**
U.S. Marine Port or Terminal Operator	24	8	3.0	16	**48**	**1%**
Grand Total	**4574**	**1533**	3.0	**2190**	**8297**	**100%**
Status Share	**55%**	**18%**	3.8 (Average)	**26%**	**100%**	

Source: (Rojas, 2005)

5. CHAPTER 5 Case Studies

The present chapter is a synthesis of the content analytical matrix of each case study. The research questions roadmaps described the processes that firms followed to build up capabilities, which in turn would support the development of security resources required for compliance (see Section 3.2, p.55). There are three issues to be discussed in each of the cases, and these are structured in the case study template, or case outline (see Table 5.1).

Table 5.1: Case study outline[59]

1. The process Story telling of the compliance process 2. Figure: Summary of the compliance process 3. Security resources and capability building Descriptions of the resources development for supply chain security; and descriptions related capabilities building processes. 4. Internal and external sources of knowledge and learning for capability building 5. Table: Summary of relationship between resources development and capabilities building

Sections 2, 3 and 4 of the case study outline correspond to the compliance process, the security resources and compliance capabilities of the firm, respectively.

The variables to classify the processes, resources and capabilities are summarised below (see Table 5.2).

[59] This template is a short version of template presented in the methodological section.

Table 5.2: Classification of variables from case studies

Variables		Coding
Compliance Process (P)	Regulatory identification	*P.RI*
	Regulatory Interpretation	*P.I*
	Compliance assessment	P.A
	Compliance level and regime	P.OL
	Communication systems	P.Com
	Implementation strategy	P.Imp
	Compliance evaluation and monitoring	P.E
	Feedback loops	P.Fb
Security Resources (R)	Business partners	R.BP
	Physical security	R.Phys
	Access controls	R.A
	Personnel security	R.Per
	Procedural security	R.Pro
	Information systems security	R.IT
	Container security	R.CT
	Conveyance security	R.Co
	Training and threat awareness	R.TA
Compliance Capabilities (C)	Organisational competencies	C.OC
	Management systems	C.MS
	Internal coordination systems	C.IC
	Stakeholders support	C.SH[60]
	Supplier development	C.SD[61]
	Vertical alignment	C.VA[62]
Temporal dimension		T

It is important to note an overlap between the first and second sections of the case outline. Unsurprisingly, the description of the resources and capabilities building processes relates directly to the regulatory implementation, monitoring and evaluation[63]; in other words, they occur mainly during the implementation and evaluation stages of the compliance processes. However, the resources and capabilities building are described in their own section within the case description (See Table 5.1, p.103).

[60] Stakeholders comprise: network of suppliers (excluding the supply chain partners) and external organisations not directly related to the firms' normal operations. Exporter, transport, and distributors were classified in Supplier Development (C.SD), the rest of the actors (technology and service providers, consultancies, research centres, business associations, private certification agencies, customs agencies, so on) were classified as stakeholders support (C.SH).

[61] Supporting the development of the suppliers' resources and capabilities may contribute to the efficient operation of the firms' own security resources.

[62] Capabilities built both ways and in coordination with supply chain partners (exporter, transport provider and distributor).

[63] This is not to neglect the need for resources and capabilities in the previous regulatory stages (P.RI, P.I, P.A, P.OL, and P.Com), but to narrow the attention on what is the regulatory requirement, i.e. implementing, monitoring and assessing security and safety resources according to the regulators' standards.

Although this is an attempt to exhaustively account for the resources and capabilities of the firms within the limitations of the data gathering, it includes what the firms' CEOs considered to be the 'main' security resources and capabilities available in their firms.

Finally, all cases include figures with the summary of the firm's compliance processes, and tables (matrixes) with the summary of the firm's security resources and capabilities built[64].

As a reminder, the case studies were first selected based on supply chain partners with similar compliance levels[65]. We selected low compliant supply chains (SC1 and SC2), middle compliant supply chains (SC3 and SC4), and high compliant supply chains[66] (SC5)[67]. The production sites of the supply chains were not as important as the location of the distribution centre, which was Nogales, Arizona, US. However, most of the growers were located in the province Sinaloa, whilst one was in Nayarit, the neighbouring province of Sinaloa.

[64] A reference to a capability building and resource development is numbered in [brackets] and listed in the matrixes.

[65] In this selection process, the support of the Fresh Produce Association of the Americas (FPAA) was crucial for the identification of supply chains, and for the information regarding the perception that FPAA had about the overall security/conformance levels of the potential supply chains to be sampled. The FPAA experience had grown as a result of the continuous exchange of information with CTPAT officials regarding the compliance of US fresh produce distributors (members) and their supply chains.

[66] SC6 was another candidate for a high compliant firm, however the supply chain did not provide sufficient information for a reliable analysis, hence this supply chain was dropped from the sample.

[67] For more detail on the selection criteria go to the section on Research Process (p.91), subsection: instrument development and case selection.

5.1. Supply Chain 1 Distributor (SC1D)

The compliance process

In 2003 (T), after the creation of the CTPAT, the CEOs were informed by the US government, third party certifiers, and its industry associations that a new programme – CTPAT – had been developed, and that it would involve the produce industry (amongst others). The CEOs had been actively engaged with one of the strongest fresh produce distributors associations of the United States – The Fresh Produce Association of the Americas – which gave them access to key information regarding US regulatory and policy initiatives (P.RI) in due time.

According to the CEOs, should a regulation not contribute to three aspects together – protecting the produce, the clients and the service – there would not be any reason to comply (P.I). Moreover the CEOs did not agree with the notion of the firm needing to control their transport providers, as declared in the interview "we have no control whatsoever on their compliance decision" (P.A).

The CEOs decided to comply with the food safety standards GMP/GHP (Good Manufacturing Practices/Good Handling Practices) (P.OL) in summer 2005 (T). This was after the grower/exporter was 'practically'[68] in full compliance with such standards (GMP/GHP) and beginning to implement security measures. SC1D was in the process of partially implementing CTPAT standards (P.OL), such as physical security and access controls, and traceability systems. However, the CEOs decided to follow a self-regulatory approach to enforce security standards, and 'not looking forward' to apply for certification in CTPAT (P.OL).

The firm's own personnel conducted assessments (P.E) of their own security procedures. Before implementing tight systems related to conveyance security, the personnel and CEOs identified costs associated with the lack of tracking systems (P.A). It was necessary to implement security measures (P.Imp) to prevent intrusions in the supply chain. The measures have to be not already covered by GMP/GHP regulations (P.OL). Thus the firm

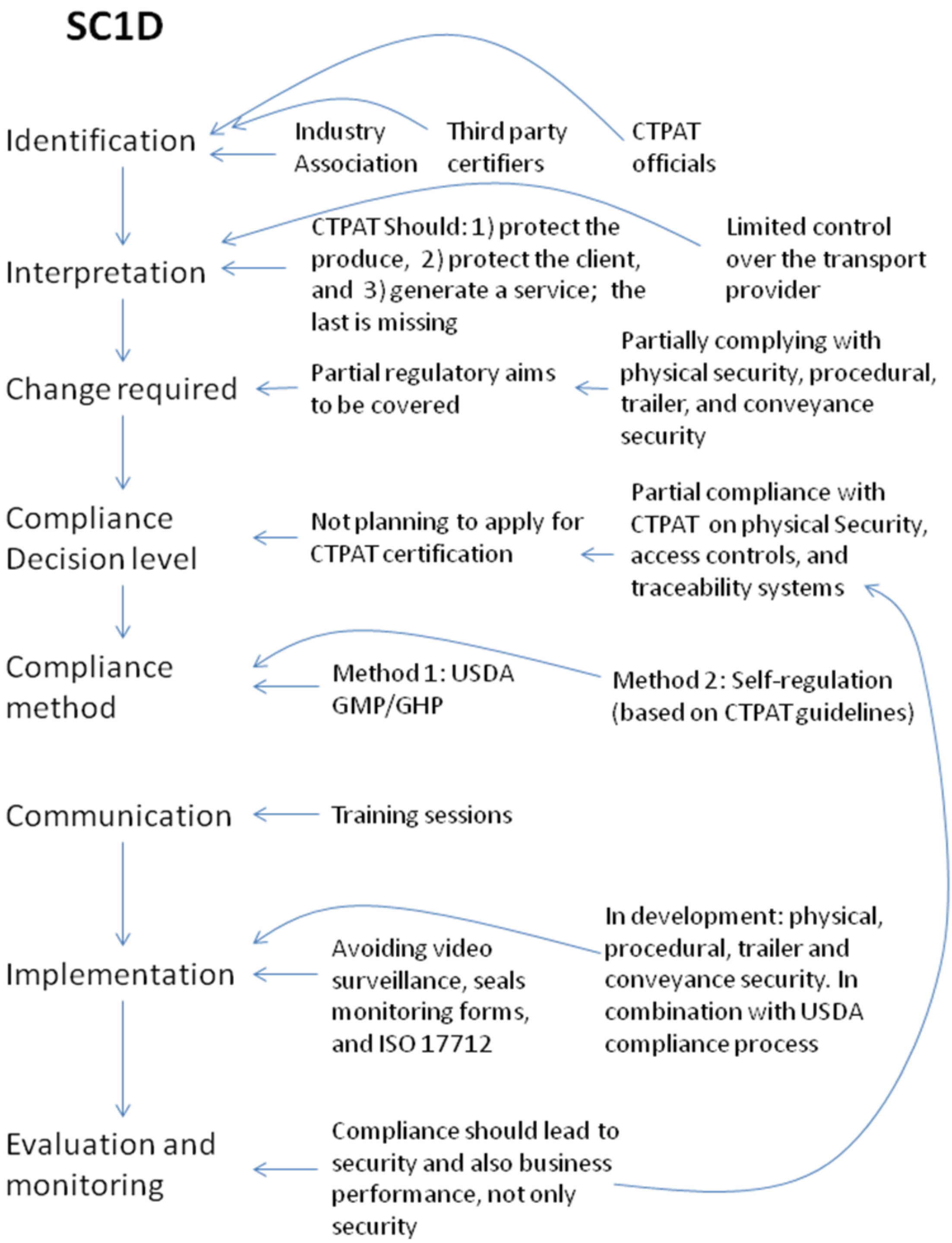
[68] Some third party certifiers in food related standards rate the compliance level of the firm in certification based on audits conducted on at least a yearly basis. The third party certifier reports the compliance rate to any buyer interested in doing business with the certified firm. Although the firm can be certified it may not comply in full with the standards, which means that it may have not received 100% rate in the audit.

decided to set its own security regulations for conveyance tracking systems (P.OL), complementing their ongoing certification process in GMP/GHP (P.OL), which, according to the CEOs, was closer to the principles of produce protection, client protection and service (P.I).

Since the GMP/GHP compliance process was given priority in SC1D, the firm only partially followed the security guidelines from CTPAT (P.OL). The CEOs final decision was not to comply but only to partially meet the CTPAT standards (P.OL).

The CEOs decided to tighten the security measures by monitoring the cargo 'transit' from the shipping point to the distribution centre (P.A), based on cost considerations. Their post-assessment (P.E) led them to conclude that better monitoring protected the produce and contributed to costs being reduced (P.I). SC1D's cargo monitoring throughout radio and mobile (P.E) was saving overtime payments to the USDA inspectors, who charged US$400 per hour for waiting for cargo to arrive at the inspection facilities in Nogales-MX (P.I).

Figure 4: Summary of the compliance process by SC1D



Source: The author, based on interview with SC1D

The Compliance Resources and Capabilities

The CEOs prioritised the implementation of security measures without the involvement of the supply chain, apart from the normal information sharing and recommendations (P.Imp). By November 2007 (T), SC1D had security resources related to physical, procedural, trailer and conveyance security in place. However, those resources were not in full compliance with the CTPAT, since the firm did not have CCTV[69] (P.OL), there was no analysis of the seals monitoring form and trailer inspection before unloading the produce, there was no systematic use of high security seals on the container (P.A).

Most of the security implementations were developed internally. The interaction to external organisations in this stage was limited to developing procedural security, i.e. traceability systems. This resource was developed by the grower/exporter for produce identification and traceability, and later adopted by SC1D who added labels useful for their own operations [1]. As mentioned before, the conveyance tracking had to be done in close coordination with the driver; however, the firm did not develop any system to monitor the status of the 'cargo' in transit [2] (SC1D wanted to know where the cargo was, not the condition of the produce inside the container).

The firm also implemented security and safety measures by upgrading the employees' skills. Security measures included setting up administrative systems leading to reliable alarms operation [3], and internal training in threat awareness [4]. Safety measures included internal training in cargo inspection at shipping and receiving [5]. Safety measures were a requirement for certification with GMP/GHP – USDA Food Safety regulations (P.OL), which, according to the CEOs, although related well with CTPAT security guidelines, are closer to the needs of any distribution centre (P.I, and P.Fb-P.A).

[69] According to the CEOs, this is apparently a key security system required by CTPAT/FAST. It is not only to record the facilities operations, but to have trained personnel watching the monitor identifying suspicious behaviours or threats, before they happen, rather than to analyse past events. However, storing the video recordings gives the capability to indentify annomalies in the normal business operations.

Sources of knowledge and learning

Actors external to the firm provided information on regulations and insights on how to develop security resources; however the employees are the ones that know how to proceed in any circumstance.

> *"Although the operations in the grower's packing facilities are similar to ours and the technologies to be implemented are the same, we have different procedures, for that reason although they may suggest security operations we have our own training systems for the firm, they have theirs. Let's take an example, the grower packs a big bulk and send it to me, with a standard security procedure paying attention in the pallet, but we need to re-pack, re-load, re-label, and arrange by quality grades for each client, each client therefore will require different security procedures, it is not the same monitoring 50 pounds bulks of produce than 10 x 5 pounds boxes; the ways to protect the produce in each case is different" (SC1D, 2007).*

Moreover, the grower/exporter (SD1E) had specialised loading capabilities, whilst SC1D has unloading and loading capabilities. Therefore SC1D required specific training programmes, which were developed within the firm.

Table 5.1.1: SC1D Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC							5	2	4	**3**	**5**
C.MS		3								**1**	
C.IC											
C.SH					1					**1**	
C.SD											
C.VA											
Resources count		**1**			**1**		**1**	**1**	**1**		
Total resources	**5**										

Source: Elaborated based on SC1D

5.2. Supply Chain 1 Grower/Packer/Exporter (SC1E)

The compliance process

The CEOs in the firm SC1E had been aware of CTPAT since 2003 (T), when the prior notice and electronic manifest were required. They initially believed that CTPAT was going to be part of such public regulations. The CEOs believed at that time that the programme consisted of 1) the protection of the produce, and 2) the protection of the supply chain (P.I).

Before the implementation, the firm had the supply chain protection functions located in the shipping department. The CEOs would make sure that the systems and procedures were in place to protect the produce but from a food safety point of view (P.A). Later it was not as clear to the CEOs whether protecting the produce was related to CTPAT guidelines (P.I). For the CEOs only those elements overlapping with food safety were clear enough, and the firm was already certified in that area (P.OL).

By the time CTPAT diffused in the US and Mexico, i.e., by 2004-2005 (T), the firm was already partially implementing CTPAT guidelines (P.OL). The main security implementations were procedural, i.e. shipping and receiving security developed for compliance with the certifications in Good Manufacturing Practices (GMP) with Scientific Certification Systems (SCS)[70] (P.OL). Additionally, the trailer inspecting procedures were developed to meet the GMP (P.OL). However, the CEO currently rejects the possibility of applying for certification in CTPAT (P.OL). The reason is the belief that there is still much to do in that matter in the firm (P.A). On the other hand, the firm would continue upgrading their security resources in a self-regulated fashion (P.OL).

The implementation included two strategies: internal developments and outsourcing. The decision to follow one or another would depend on whether or not the expertise required for each specific measure was readily available within the firm (P.A, and P.Imp).

> *"There are operations for which I rely more in other personnel, for instance, there is need to inspect the trailer before loading the produce, that inspection should be done in a rather efficient and reliable way, that set of activities are performed by the PEP (State Preventive Police under Sinaloa*

[70] Third party certifier in environmental, sustainability and food standards (http://www.scscertified.com/).

> *Department of Public Security) with dogs, trained to detect drugs and other chemicals. The access controls and surveillance in the packing facilities are also performed by them (PEP)" (SC1E, 2007).*

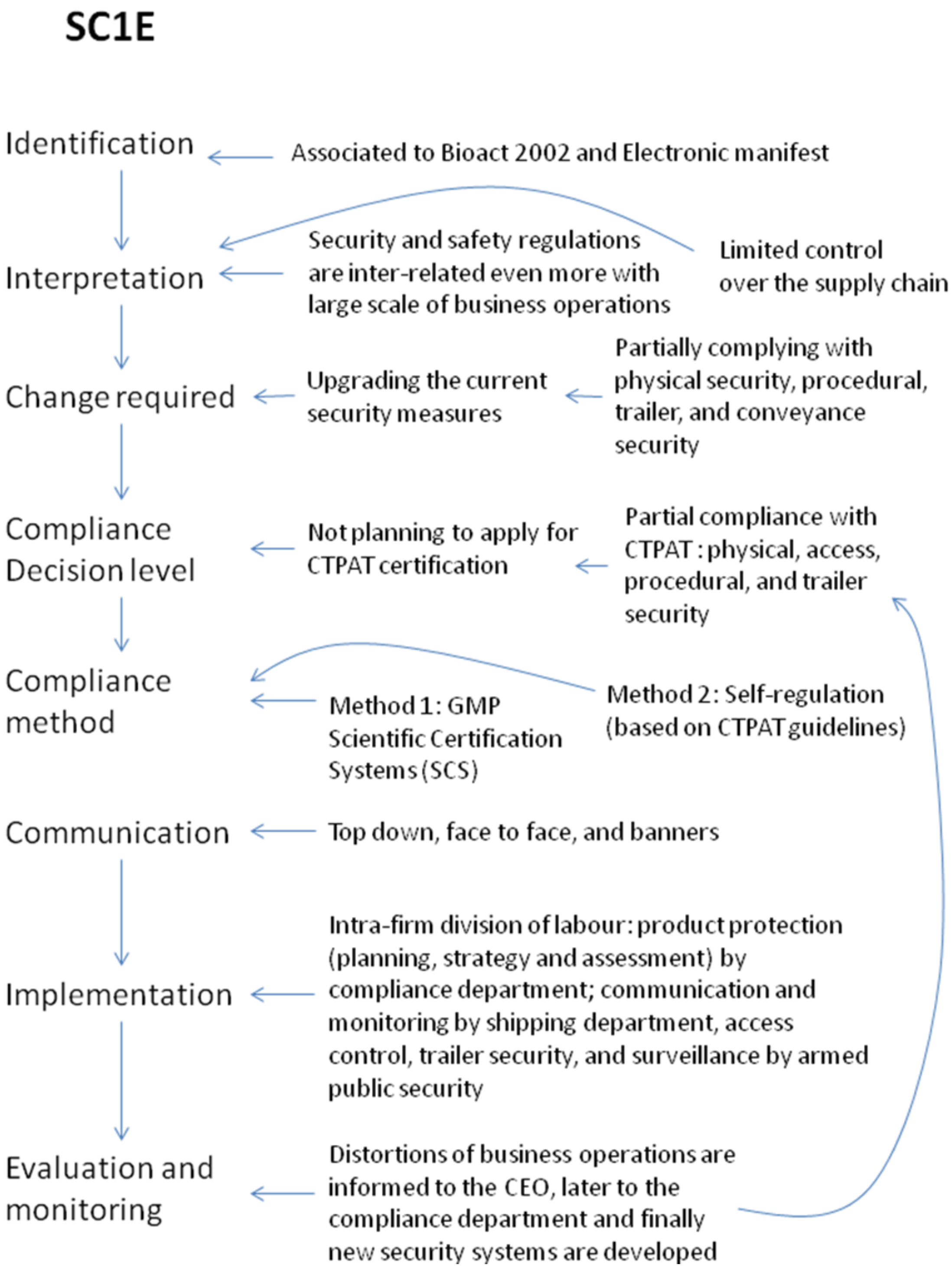
The implementation of security measures started before 9/11 and CTPAT (P.Imp) with the initiation of their greenhouse production in 1998 (T). The scale of the operations drove them to secure their facilities. The firm employed thousands of people in the packing and fields[71].

In summer 2001 (T), the firm established a compliance department driven by a food safety compliance process. This department was in charge of developing the policies, plans, strategies and handbooks that included the criteria to monitor and evaluate whether the procedures were efficiently safeguarding the product (P.E). The shipping department, on the other hand, had to deal with reporting incidents in the packing and loading areas, monitoring the facilities and the behaviour of the personnel (P.E, and P.Imp). Armoured public security officers were present to act accordingly in case of any incidents (P.E, P.Imp, and P.Fb-P.Com).

---

[71] The firm had stressed that they had the responsibility of providing, among other services, housing, kindergartens, schools, health services, public security, and transportation, which are all important for the wellbeing of the employees.

Figure 5: Summary of the compliance process by SC1E



Source: The author, based on interview with SC1E

The Compliance Resources and Capabilities

The firm has had a long term relationship with its only distributor; there was no need, therefore, to perform background checks. SC1E used to have one transport provider; however the scale of the operations was becoming too big to depend only on one provider, so the firm agreed with one more transport provider to diversify operations. The new transporter committed to comply with all public regulations, mainly to perform the electronic manifest: however, there a thorough background check was not carried out.

Nowadays, the operations of the firm attract a great number of employees for harvesting and packing. When the security risks increased with the density of the population in the firm, the CEOs negotiated with the Mexican authorities to bring public security and safety into the firm. For such specialised services the firm pays fees to the authorities [6].

Image 1: Screening and controlling the access to the packaging facilities (Public security personnel and antidrug/chemicals dog)

Source: Images by the author in the packaging facilities of SC1E

The firm have incorporated management systems technologies to increase physical security of the facilities and for access controls [7]. These systems were to make sure that the personnel were only in pre-authorised areas. The technology consists of biometrics to grant and register access to the packaging and greenhouses facilities.

These systems were not originally introduced for access controls, but to have accurate human resource management systems, to identify in which area of the company each employee was working and at what time, as well as to have accurate control of the overtime paid to the employees. With such a system, therefore, the compliance managers had the capacity to assess the overall security status of the company, based on the identification of unauthorised or unidentified personnel in specific areas (P.E). The compliance managers are capable of denying access to the facilities to suspicious persons. Furthermore, since the system is in each one of the greenhouses in the field, the compliance managers have the ability to know whether and when unauthorised, authorised, or suspicious persons had been in contact with the produce [8].

Image 2: Access control to packaging and greenhouses (biometrics)

Source: Images by the author in the packing facilities of SC1E

Cargo traceability systems were developed by the shipping department [9], [10]; however, when an operation can be effectively managed by external organisations, e.g. electronic manifest by the transport provider, the outsourcing of that operation is encouraged.

Procedural security required internal coordination and external support. For the shipping procedures to make sure the trailers and containers were clean by the time they left the packaging facilities, the firm used antidrug/chemical detection dogs, managed by the Preventive Police under the Sinaloa Department of Public Security (PEP). These operations were developed to comply with GMP. When a trailer arrives, it is screened by antidrugs/chemical detection dogs, later the container is sanitised with a quaternary ammonium compound, the cargo is loaded and the trailer sealed (non CTPAT/ISO 17712) [11].

The warehouse, linked to the shipping area, is equipped with unmanned technologies to prevent contamination. In 2003, the CEOs identified (T) an ozone generator during the GMP compliance process. The system attacks bacteria, viruses and some chemicals, preventing the contamination of the fresh produce, and had been more reliable than human surveillance in the warehouse. Moreover, the system acts as a preventive and, in cases of minor contamination, as a corrective measure [12].

There are security criteria from CTPAT and other self-regulations that were not implemented. It was suggested to the rest of the supply chain partners to use the ozone system in the containers in transit to the US. However, there was a strong negative reaction from their supply chain partners, arguing that it represented unnecessary costs. Another rejected aspect was the background checks, "it would be the biggest department in the firm", the CEOs declared. This is because of the nature and, again, scale of the operations, with a high annual turnover of personnel, based on migrants from the south of Mexico, who are hired as groups rather than as individuals. In the near future the probability of using background checks would be even lower, since the firm was expecting to increase its current operations of more than 100 hectares of greenhouse production by 50 more hectares in the following years. However, there is a record of conduct of the employees available in the current system.

The security systems are interrelated with the safety measures (GMP). The firm prohibits any foreign substance in the greenhouse and packaging areas. The produce needs to be handled with care, and with clean and sanitised hands; this is part of the basic induction an employee receives for GMP, and reminders of the rules are visible in every section where produce is being handled. According to the CEOs, this procedure clearly contributes to the prevention of bioterrorism activities.

Internal and external sources of learning and knowledge

The firm have cumulated knowledge throughout time; this required training sessions with GMP certifiers (P.E), including security procedures. The implementation of security measures were mainly based on internal capabilities and, when external support was provided, it was tightly interrelated with internal operations, excluding the electronic manifest, which was entirely outsourced.

Image 3: Banners, Sensor-activated hands sanitizer, and GMP no contact with the produce

Source: Images by the author in the packing facilities of SC1E

The CEOs were clear in their strategy of exploiting resources that were already available elsewhere. This had important consequences to the internal capability building for security resources development. For instance, the firm did not invest resources in awareness skills or competencies to identify drugs and chemicals; all those resources were acquired from outside the firm.

To summarise, the CEOs relied on their own knowledge, experience and internal learning systems. Also, they realised that they had limited control over the supply chain, based upon their experience with trying to introduce the ozone generator. On the other hand, they also realised that resources, in the form of expertise, were available outside the firm for their deployment within; for this they had to reach agreement with public stakeholders.

Table 5.2.1: SC1E Security resources and compliance capabilities sophistication

Resource Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC					9					**1**	**7**
C.MS			7		10					**2**	
C.IC		8			12		11			**3**	
C.SH			6							**1**	
C.SD											
C.VA											
Resources count		**1**	**2**		**3**		**1**				
Total resources	**7**										

Source: Elaborated based on SC1E

5.3. Supply Chain 1 & 5 Transport Provider (SC1&5T)

The compliance process

When it was made public that the FAST lanes would become operational in August 2006[72] (T), (P.RI), various truck drivers in the firm SC1&5T estimated the potential time reductions by users of the programme. The CEOs gathered information from the CBP webpage, and later from the CTPAT seminars held in Nogales, Arizona. Other sources of information were seminars for the electronic manifest (P.RI). According to the CEOs, compliance with CTPAT/FAST was not a problem since drivers in the firms were dealing with security issues all the time (P.I).

However, the firm would not deploy resources before being audited by CTPAT. They were not speculating about what they really needed, rather, it was preferable to be told by the officials what they required to get certified (P.I). The results of the audit at the end of 2006 (T) by CTPAT officials (P.E) was that they required important investment in physical security, and that CTPAT officials would not believe the firm was committed to such investment if they were hiring the facilities, rather than owning them (P.A).

The firm was also unwilling to invest in physical security, most of which was fixed capital, in a property not belonging to SC1&5T (P.OL). The implementation of the physical security was delayed due to the need to first acquire an area in which to build up their secured facilities (P.OL, and P.Imp), which was done in early 2007 (T).

The entire personnel in the firm was involved in the design of operations and redistribution of roles, including compliance-related responsibilities, in the new facilities (P.E). However they were still not located in the new facilities, since they were being built at the time of this investigation. The CEOs were eager to achieve compliance and the certification for the firm, to be able to gain the benefits of using the FAST lanes (P.I, and P.OL).

In the redesign of the security procedures and responsibility, the CEOs were trying to strike a balance between centralising and delegating the responsibilities of the implementation stages in the new facilities (P.Imp, and P.Com). However, there was no

[72] (http://www.bip.arizona.edu/news_pdf/082106_FASTNogales071806.pdf)

systematic supervision and checklist of steps to follow in the implementation of security measures (P.Imp). The centralisation of the security measures consisted of:

1) each area of the firm would propose security procedures for their own area and conduct P.A, P.OL, and P.E;
2) the supervision of all operations and activities would be done by the general manager (P.E); and
3) the security guard would be in charge of the surveillance of the facilities, trucks and trailers: the guard is provided by a private security company (P.Imp, and P.E).

At the moment, the managers are able to monitor and control all the security operations (P.Imp, and P.E) due to the small scale of their operations. SC1&5T has 37 drivers, 37 trucks and 62 trailers.

The highest responsibility is held by the drivers (P.Imp). They need to check for cargo discrepancies, what was loaded and unloaded, and match it with the electronic manifest. They need to make sure the trailer had not been opened, since they need to keep the produce at a constant, low, temperature. The CEOs argue that it is always possible to poison a consumer unintentionally. For instance, a common scenario is that the truck is under inspection by the Mexican Department of Defence, which do not have the technologies in place to perform the inspections. The inspections are performed by hand, and exposed to outdoors environments in the Sonora dessert, where even in the winter season the maximum temperatures range between 37 to 40 degrees Celsius. If the cold chain is broken, the produce might get spoiled; these may not necessarily be detected by the random samplings in customs or in the distribution centre, hence the consumption of this food could poison consumers (P.A and P.E). If the spoiled produce is detected, the transport provider pays for it. To summarise, the truck driver needs to be very careful with the produce (P.A).

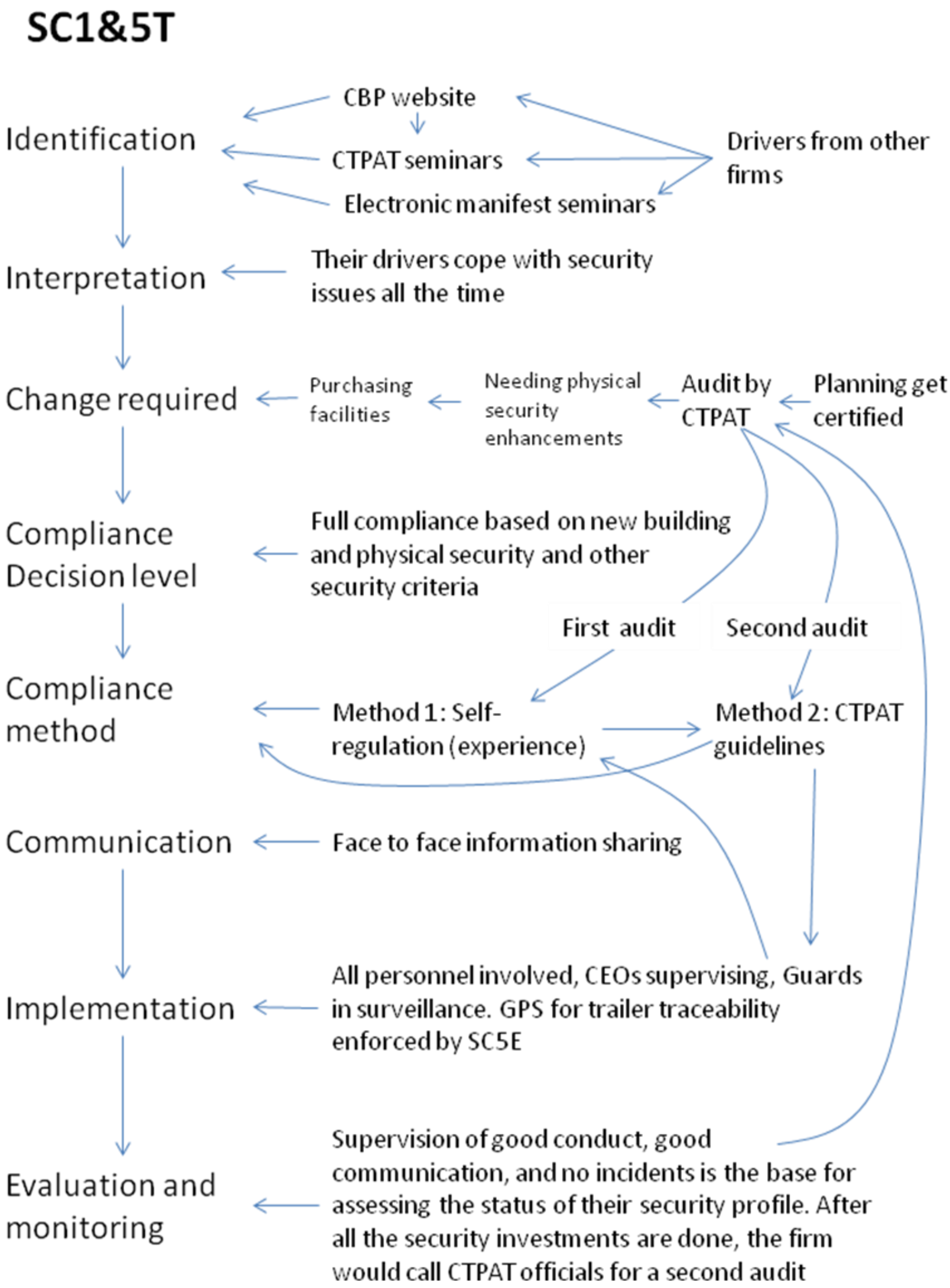
At the moment the CEOs are considering a request made by SC5E (P.A) to introduce GPS (P.Imp) in their trailers. Furthermore, according to the CEOs, SC1&5T has procedural security based on communication systems, such as radio, mobile, and that needs to be very accurate to be able to perform the electronic manifest of the cargo: this needs to be transmitted exactly two hours before arriving at the port of entry.

SC1&5T knows the location of the trucks, based on basic communication with the drivers in transit. They inform the firm's managers when the produce is being loaded and unloaded, either at the shipping point, inspection points (Mexican and US), or the distribution centres. Furthermore, the firm's CEOs are collaborating with the electronic manifest software developers to link it with the GPS and georeferencing to locate and identify suspicious behaviour by the driver in transit. Hence the GPS is in turn becoming part of the CTPAT security profile of the firm, and it is planned that this should apply for all exporters to whom they may provide their services.

The drivers follow procedural security criteria. The trucks are sealed when they are loaded, and there is a form that needs to be completed in case the seal is broken by an inspecting authority: that document needs the signature of the official that broke the seal. However, the firm have not developed any procedure for re-sealing the trailer, because after breaking the first seal, "all that is needed is trust in the driver" (SC1&5T, 2008). As the firm have not had incidents before, they continue trusting the personnel.

The drivers are also competent in the identification of suspicious behaviour by individuals on the road. Training was provided by US governmental agencies, consultancies and associations.

Figure 6: Compliance process SC1&5T



Source: The author, based on interview with SC1&5T

The Compliance Resources and Capabilities

The physical security is under development, based on recommendations from CTPAT officials. This required considerable investment, and CEOs' involvement for the entire design of the new facilities [13]. It is planned that the physical access controls are performed by the firm's guards, with basic record-keeping of the entrance and exit of people to the firm's facilities. However in relation to the areas within the facilities, it is planned that each person in each area is responsible in allowing only authorised personnel to have access to restricted areas [14].

The firm is not developing personnel security profiles, since they rely strongly on well-known and trusted drivers, and their hiring strategy has worked well so far. Therefore networking and personal contacts are still the mechanisms by which to hire personnel in the firm.

Procedural security had been performed according to routines established by the exporters and the distributor, while the main concern of the driver is to make sure the cargo is legal, that it matches the electronic manifest and the bill of lading, that the trailer was not opened, and extra care in case the trailer had been inspected due to transiting with a broken seal [15].

The conveyance traceability systems have been in development with the software provider. It requires constant communication to verify that the units are effectively identified in the GPS system and that the software is integrated with the electronic manifest systems [16]. However, this development did not require any coordination with SC1E or SC5E.

Finally, the awareness of the drivers has been acquired by experience; however, it has also been enhanced by the training seminars provided by the US Department of Transport (USDOT) and CTPAT seminars [17].

Learning and knowledge sources

The firm has developed experience on its own, and the security changes are planned and implemented internally. The required external support in the compliance process comes from CTPAT agents, who assessed the facilities and explained what the firm needed in order to get certified (P.A and P.E). The exporters may require certain procedures, which are normally granted since they do not require substantial changes, apart from adding more operations to the business. This is except for the GPS, which indeed required strong collaboration with software developers to integrate the two different systems into one in order to be able to monitor and trace the trailer, not the cargo. When all the resources are in place, the firm expects to have a second audit to either achieve compliance or introduce the changes indicated by the CTPAT auditors.

Table 5.3.1: SC1&5T Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC		13								**1**	**8**
C.MS		13								**1**	
C.IC		13	14		15					**3**	
C.SH					15;16			16	17	**3**	
C.SD											
C.VA											
Resources count		**1**	**1**		**2**			**1**	**1**		
Total resources	**6**										

Source: The author, based on interview with SC1&5T

5.4. Supply Chain 2 Distributor (SC2D)

The compliance process

The FPAA first informed the firm about CTPAT in 2002 (P.RI) (T), and the compliance manager followed up the regulation. For the CEOs it was not initially clear how the regulations would influence the business operations (P.A), it was necessary to attend the CTPAT seminars (P.I). After the seminars the firm understood that the CBP would treat cargo coming from compliant firms as safer, and therefore benefits would be associated with compliance; a good indication for the CBP of more secured cargo would be the sealed trailers (P.I, and P.A).

In order to be able to qualify for the benefits of the regulations the firm agreed on pursuing full compliance at the end of 2002 (P.OL). The compliance manager then had the responsibility of developing a handbook of security procedures for the whole distribution operations, submitted the firm's security profile to CTPAT programme at the beginning 2003 (T), and was granted the certification and validation at the end of 2003 (T) (P.OL).

The issue of compliance with security regulations is who controls the supply chain (P.I). For instance, there is currently a dilemma of who will be held responsible for the use of the high security seals, not yet in use in our supply chain. The high security seal is seen by the CBP as a very safe measure, reducing the probability of inspections and reducing the cross-border times (P.I.) (P.Imp).

Should the seals be managed by SC2E&T, the distributor would be transferring the responsibility to them, but the whole supply chain would be accountable. The other option would be not giving any duty to SC2E&T, and therefore every cargo would be inspected in Nogales-Mex in CAADES, Maynar, or at the Mexican Customs Brokers warehouse. The trailer would be sealed just before joining the port of entry. The first option would be cheaper than, but not as safe as, the second option; the risks would be higher and costs lower in the first option. At the time of the interview, the firm was planning to choose the second option, for higher security and control over the supply chain (P.Imp, P.A, and P.OL).

The firm had used the usual meetings to inform the personnel about the implementation of the new security regulations, and they had training sessions on security procedures. There are signs around the facilities indicating whether areas are restricted or not and how to proceed in case of intrusion. These are reminders of the lines of action given in the training sessions to all employees (P.Com).

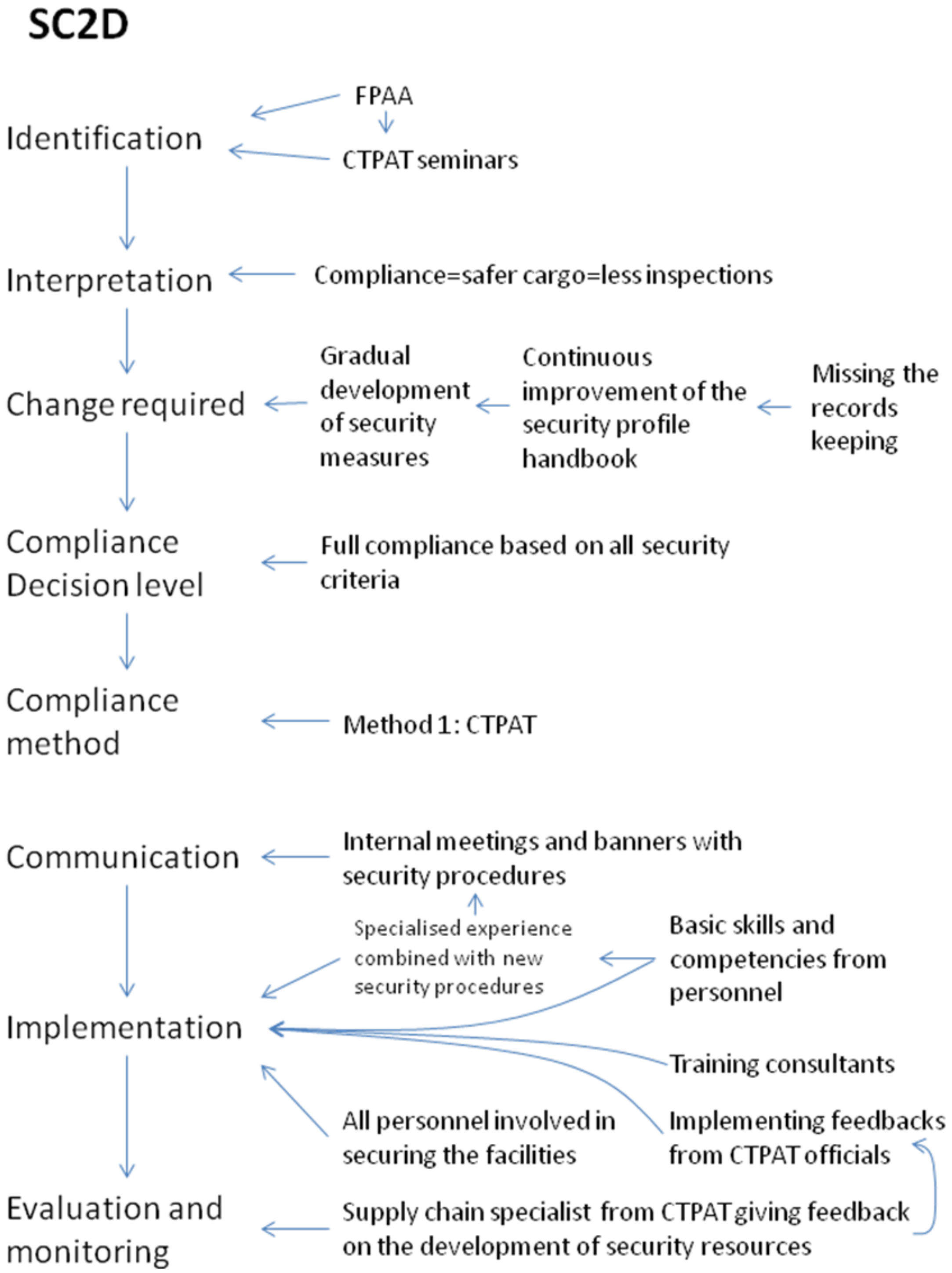
The implementation stage required re-organisational capabilities in SC2D. There was a need to re-learn and re-design the organisation of the warehouse facilities; there were materials that had to be re-located to protected areas (P.Imp). Previously, the produce could be contaminated even with other produce. Therefore, each type of produce required special storage conditions: if one cargo was contaminated, the organisation of the facilities and storage conditions should prevent cross-contamination between cargos [18]. Hence, on top of the security awareness and procedural security training, the personnel received post-harvest handling training, which also contributes to preventing contamination of the produce (P.Imp, P.Com).

The whole personnel have been assigned more activities in their daily routines. Specific security training and skills have been developed in each area, built upon previous skills. For instance, the compliance officer used to do general background checks before CTPAT, based on information supplied by The Blue Book[73], and, once or twice per season, in relation to food safety regulations. Previously, there were no written reports, however the assessments are no longer only for SC2D, but for the regulatory and certifying agencies. Therefore written reports of SC2D and its business partners (exporters, and service providers) need to be issued to the relevant agencies. Furthermore, the background checks of business partners have been enhanced to analyse whether the firms are implementing or developing CTPAT or other security criteria, and the firm need to assess whether the measures are sufficient to be considered a partner. The firms had the assessment competencies, but they were upgraded and formalised for monitoring purposes.

The firm keeps contact with CTPAT officials to share the status of the security resources being developed with them, having continuous feedback from them on how much such measures conform to security criteria (P.E).

[73] Source of information on credit ratings and trading practices by firms (http://www.producebluebook.com/).

Figure 7: Compliance process SC2D



Source: The author, based on interview with SC2D

The Compliance Resources and Capabilities

The business partners security procedures were upgraded from previous knowledge of research of credit history and trade practices of all its business partners. The compliant officer developed the procedures for investigating the firms' security status, and then trained the relevant personnel in charge of investigating and establishing relationships with clients and suppliers [19].

The physical security and access controls required investment and warehouse re-arrangements [20], with relevant training of the warehouse personnel on the handling and restricted access to the produce and materials [21]. The training came from the fire departments and the post-harvest specialist for the prevention of produce cross-contamination [22][74], as well as from the acquisition and installation of CCTV equipment [23].

The compliance officer has developed a strategy to conduct background checks on the personnel hired to work in the distribution centre, and shared this with human resources personnel. However, such activities only required basic internet searching skills, where it is possible to find information about individuals with criminal convictions. Again, such investigation skills were added to the basic human resources hiring strategies and work records examinations [24].

According to the compliance manager, their information systems require personnel to have basic computing competencies (R.IT). The firm has password protected information systems but this is a single password for the whole firm. There is no monitoring of individual modifications of the databases and records.

The procedural and trailer security are tightly coordinated with the grower/transport provider (SC2E&T), who had integrated growing, packing and transport operations. The cargo and shipping procedures are shared with the partner (SC2E&T) to make sure they were followed [25]; furthermore, these procedures were upgraded taking into consideration SC2E&T capabilities [26]. The compliance manager argued that this resource is developed

[74] This capability is classified as physical security resource and not as Training and Assessment, as it is not a formal training system, but a more practical training. It was also not classified as an organisational competence, because the knowledge for the training was not based on the internal personnel or organisational, but external (C.SH). Yet, in this practical training it was necessary internal coordination capacity (C.IC), so that on the job training was possible.

mainly by them (SCD2). This is different from the trailer security, which is a result of a joint development between SC2D and SC2E&T.

The trucks and trailers are the property of SC2E&T, which has particular interest for sustaining good trailer security inspections. Therefore SC2D and SC2E&T regularly updated each other on how to perform better inspections of the trailer during visits of SC2D to SC2E&T's facilities [27].

The conveyance security was almost non-existent: the cargoes are transiting unsealed, and they have been using the services of the border-crossers (burreros)[75]. Since the supply chain was still not using seals (R.Co), the only way of securing the cargo was by procedural security.

Such vulnerability in conveyance security drove SC2D to train their personnel on security awareness in relation to the trailer inspections, thus reinforcing their use of CCTV among 17 areas in the facilities. One of these areas is the cargo dock area where CCTV is used to analyse cargo unloading in case of any incident [28].

Learning and knowledge sources

SC2D have supported the upgrading of the supply chain security through internal mechanisms, support from specialised stakeholders (consultants, CTPAT supply chain security specialists, post-harvest safety), and have been eager to share information and encouraging about compliance with the CTPAT regulations to its supply chain partners, including SC2E&T. Participation of their suppliers in the new CTPAT regulation will precede any transfer of responsibilities to the initial phases of the supply chain (P.A, P.OL, and P.E)

[75] Trucks may carry two trailers from the packing facilities, and one more truck is needed to cross to the US, since they do not allow one truck to carry two trailers. The additional truck crossing the trailer to the US is hired from a border-crosser (burrero) service provider together with the driver. Therefore the driver from the transport provider is responsible for one truck and one trailer together with the transport provider: the border-crosser (burrero) is accountable for the other truck and trailer, together with the transport provider. In that context, the driver must implement the procedural security before transferring the responsibility to the border-crosser (burrero), since the driver is making the transport provider accountable for the actions of the border-crosser (burrero).

Table 5.4.1: SC2D Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC	19	23		24	28					**4**	**12**
C.MS		20,18	20							**2**	
C.IC		22	21							**2**	
C.SH		22			26					**2**	
C.SD					25					**1**	
C.VA					27					**1**	
Resources count	**1**	**4**	**2**	**1**	**4**						
Total resources	**12**										

Source: The author, based on interview with SC2D

5.5. Supply Chain 2 Grower/Packer & Transport Provider (SC2E&T)

The compliance process

The compliance manager from the distribution company (SC2D) provided information on safety and security measures to SC2E&T (P.RI, and P.E). Since the firm has its own transportation company, at the end of 2003 (T) the distributor (SC2D) and CBP suggested participation in the CTPAT to SC2E&T's CEOs (P.RI). Later, the firm was visited in early 2006 (T) by CTPAT officials coming from Washington to assess the firm and inform about security regulations (P.RI, P.A, and P.E). Later the CEOs attended a series of CTPAT seminars (P.RI).

The CEOs had the impression that getting certified would be important (P.I), however at the moment the resources need to be oriented towards an ongoing certification on food safety regulations (P.OL, P.A).

In August 2007 (T), SC2D requested that the firm to become certified in good agricultural, manufacturing and handling practices with PrimusLabs[76] (P.I), in order to maintain their clients in the United States. The firm's CEOs believe that such food safety regulations contribute to security compliance as well.

The CEOs mentioned that the good manufacturing practices certification includes a section on traceability (P.A), which is also an essential criterion of the security regulations from CTPAT (P.A). They criticised the inspection points set up by the Mexican authorities, arguing that they spoil every security measure implemented by the firm (P.I). This is because once they break the trailers' seals, the cargo remains exposed to any intrusion on the road after the inspection points (P.A, and P.I).

The CEOs were delaying compliance with security regulations (P.OL). However they were expecting that upon successfully developing and implementing food safety practices and certification, various resources developed for that purpose would also contribute to security compliance (P.A). According to the CEOs, a security compliance delay does not, in fact, represent a security resources development delay (P.I, P.A, and P.OL).

[76] Third party certifier, laboratory and consulting of safety, quality and growing practices and systems of for food supply chains (www.primuslabs.com)

Although the security compliance process would follow the food safety compliance process, the CEOs did not expect to achieve full compliance in CTPAT (P.OL), because there is little incentive to fully comply with CTPAT, since the industry is not compliant (P.A, P.I).

> *"From the transport provider view point, at the moment, we cannot find enough qualified drivers to move the produce to the US. At the moment, I have trucks not being used, because I have not enough drivers. Now, as soon as I inform a potential driver that I was to conduct a background check on them, and they are required to perform extra security operations compared to what the rest of the transport industry in Mexico is requiring, they would leave to other firms to work. That is what I mean, the CTPAT regulation is possible if the rest of the industry applies the criteria as I do" (SC2E&T, 2008).*

According to the firm, the security measures implementation process could be done in two ways: within-firm development or outsourcing (P.A, and P.Imp). Since the firm is relatively new (its initial operations were in 2000) (T), and the scale of the operations is very small compared to the rest of the exporters from the region, the firm decided that security measures would be designed and carried out internally since they are able to maintain control over the facility (P.A, P.Imp).

Since all people get involved in the implementation process, and there are only a few managers (P.A), the CEO plans to have face-to-face communication systems and controls incorporated into the daily routines (P.Com). The CEOs considered that safety and security issues were interrelated; hence the safety compliance manager would be made responsible for security compliance processes (P.Imp).

In cases where the businesses' partners have the competencies, the firm outsourced the security activities. For instance, with the operations to comply with Public Regulations, their customs brokers performed the Prior Notice, whilst their insurance providers performed their Electronic Manifest (P.OL).

Those services were offered to the firm (SC2E&T) as gratuities for doing business with them (P.A, and P.Imp). The CEOs accepted such offers as a result of lacking the information technologies and trained personnel to make the electronic transmissions on their own to the FDA and CBP (P.A).

The firm was also strategically avoiding investment (P.A) in 'unnecessary' security resources. One of those investments was CCTV, even though the CEOs acknowledged that, for CTPAT officials, using CCTV was good security practice (P.I). According to the compliance managers, the alternative was to enhance the monitoring systems and recordkeeping of the procedures and conditions of the cargo.

Furthermore, the CEOs criticised the regulatory design of CTPAT, because it does not take into account the different configuration of its firm's operations (P.I). Although the firm (SC2E&T) has packing facilities, most of them are in open fields where the produce is picked up with mobile packing systems. Moreover, there are mobile cooling systems designed to load the trailers and cool them down on the fields. In fact, the produce could be sent directly from the field to the United States.

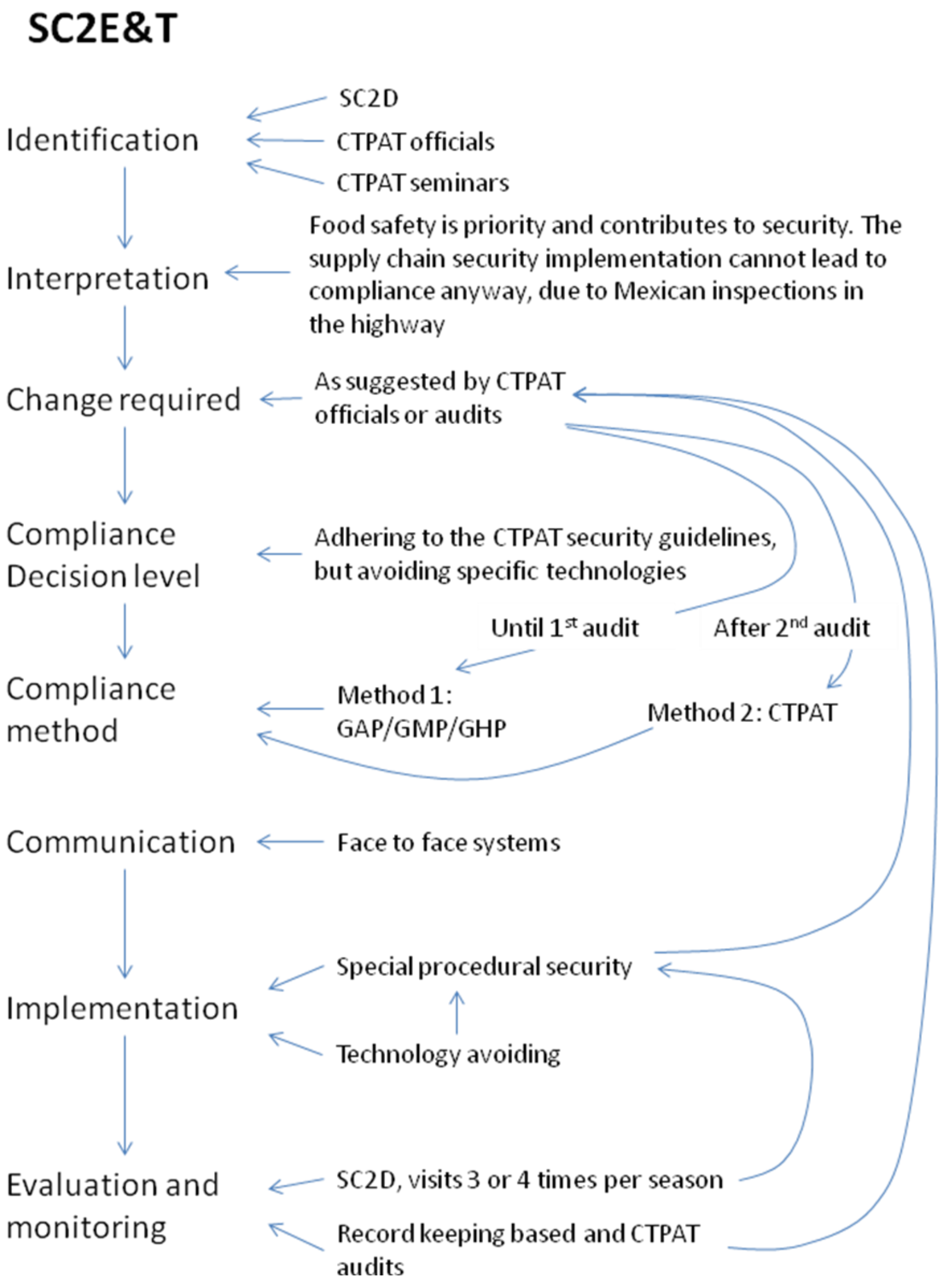
The CEOs argued that they could not achieve security and protect against bioterrorism threats by installing physical technologies in their fixed packing facilities (as required by CTPAT), but by developing procedural securities *ad hoc* to their packaging and logistical systems (P.OL, P.Imp).

There are additional challenges posed by the CTPAT requirements according to the CEOs. This is because they hire pickers by the hundreds from the south of Mexico with practically no information of their background. Background checks are economically prohibitive in these cases.

Although the firm was visited by CTPAT officials (early 2006) (T), and invited to develop the security resources and apply for certification, the firm was reluctant for two reasons: 1) at that time they had no security resources at all (P.A, and P.E), and 2) they were expecting to apply after their certification in food safety (end of the 2009) (T) (P.OL).

Only then would the CEOs request the visit of CTPAT specialists. It is then when the CEOs would determine the precise security resources needed in the firm to achieve compliance and certification (2010) (T) (P.E, and P.A). According to plan, the firm would see security implementations in 2010 (T), aiming at certification in CTPAT (P.OL) at the end of 2011 (T). Notwithstanding, SC2D is already giving feedback to SC2E&T relating to the CTPAT guidelines, and expectedly it would continue to do so during their full implementation (P.E).

Figure 8: Compliance process SC2E&T



Source: The author, based on interview with SC2E&T

The Compliance Resources and Capabilities

The firm had not developed the resources to realise business partner backgrounds, except for credit and marketing ratings that require basic internet browsing and knowledge of the industry [29]. The physical security had not yet been developed, but the firm expected to rely on its internal personnel's competencies to build up such resources and design facilities.

Most of the access control systems and procedural security have relied so far on personnel competencies, skills and internal management systems [30], [31]. The exceptions are the procedures related to traceability of the cargo and the electronic manifests, which are based on close coordination between the firm (SC2E&T), the driver, the customs brokers, and the insurance providers. The Prior Notice and Electronic Manifest are issued exactly two hours before joining the port of entry. This is done when the trailers have been hauled with the border-crosser's trucks in Nogales-Mex [32].

In relation to the information technologies, the firm relies strongly on their insurer and customs brokers. Only they are able to modify or transmit the information to the CBP and FDA, while SC2E&T remains accountable for such operations. It is their business partners who have the software and knowledge to modify the information of the firm according to the US customs and FDA. What the firm has is trust in such business partners, rather than security procedures [33].

On the other hand, the trailer and container inspections are conducted in Nogales, Mexico by the Mexican customs broker or Maymar [34]. Most of the trailers and conveyance securities are spoiled by the Mexican inspectors, who do not take into account whether the trailer is secured according to the CTPAT security guidelines (P.Imp, and P.E).

Learning and knowledge sources

The CEOs (owners) mentioned that the firm (SC2E&T) was relatively young; however they had previously managed another firm for several years, and had a cumulated experience of 30 years. Most of knowledge of security had been acquired through CTPAT seminars (P.RI, R.I); however, the firm SC2E&T was relatively new and they were trying to learn to comply from scratch (P.OL). To summarise, the CEOs argument was that they had enough experience to acknowledge that they had a vulnerable young firm, leading them to delay security regulatory compliance (P.OL), and delay deploying any resource until the CTPAT auditors had indicated what was required (P.A, and P.E).

For the implementation process of public mandates (Electronic Manifest and Prior Notice) they identified external organisations able to provide the services of Electronic Manifest (EM) and Prior Notice (PN), thus covering one security criteria without the use of internal efforts, except using the traditional facsimile transmission to request the EM and PN. The CEOs highlighted that young firms like theirs required state support to build up security compliance:

> *"We do not have the knowledge to assess our security status, but what we need to know is what to do, since the implementation I do not think it will represent a big problem, we have people able to learn and adapt to the new conditions. However, as a small firm, we do require the support from the Mexican State, we require similar regulations as CTPAT in Mexico, which may lead the government to set up the institutional support mechanism, such as technological developments and transfers, trainings, and specialist that lead us to comply, just as it is happening with the food safety regulations" (SC2E&T, 2008).*

Table 5.5.1: SC2E&T Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC	29		30;31		30;31					**3**	**8**
C.MS			30;31		30;31					**2**	
C.IC											
C.SH					32;33		34			**3**	
C.SD											
C.VA											
Resources count	**1**		**2**		**4**		**1**				
Total resources	**8**										

Source: The author, based on interview with SC2E&T

5.6. Supply Chain 3 Distributor (SC3D)

The compliance process

The firm had received information related to CTPAT since 2003 (T) from various sources such as the CBP, FPAA (The Fresh Produce Association of the Americas), third party certifiers offering their services, the Mexican government organising seminars in Mexico, and their suppliers (P.RI). The firm not only received information on security regulations, they also participated in the seminars given by US and Mexican institutions (P.RI and P.I).

The firm SC3D had the intention of following the security guidelines and controlling the entire supply chain. The problem for the compliance manager was how to do that, as well as whether and to what extent the implementations would conform to the regulations (P.I, and P.A). The manager was also concerned with the difficulty of strengthening the weak link of the chain, transport (P.A, and P.E).

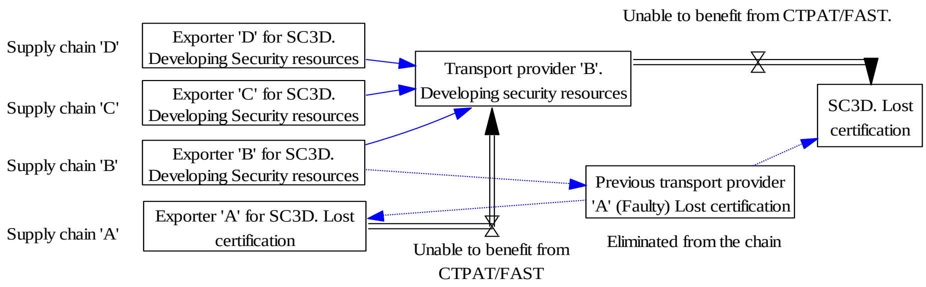
SC3D knew about their limited capacity to control the supply chain, yet they fully engaged with CTPAT (P.OL). The firm went through a trial and error implementation process that continuously updated their security profile, which in turn reflected the guidelines given by the CTPAT authorities (P.Imp). In the firm, people felt that they were partnering with the US government, and they would try to enhance the level of security (P.I, and P.OL).

Initially the firm soon developed the operational procedures to the new security regulations (R.Pro). Since the firm was not far from compliance, it was granted the certification (P.E) in 2005 (T) by CTPAT: not only them, but also their main supply chain (P.E).

One of the limitations of the security measures was the lack of specifications related to the experience of the truck drivers; the whole supply chain suffered the consequences. In early 2006 (T) the transport provider sent a 23 year old driver alone who, although trained, was inexperienced in dealing with the border-crossers (burreros) and implementing the procedural, trailer, truck, and conveyance security in real-life. The driver hired a 'burrero', who had a valid US driver licence for cross-border operations, but later was caught by the US customs with a backpack carrying drugs (P.E).

As a consequence, the all the supply chain partners related with the distributor lost their certifications and therefore the benefits of CTPAT/FAST were also lost (see Figure 9).

Figure 9: Supply chains reorganisation by lost certification by SC3D



Source: The author, based on interview with SC3D

Their exporters (SC 'B', 'C' and 'D'), who at the time were developing security measures with good prospects of gaining certification, lost a certified transport provider 'A', which was thus eliminated as supply chain partner. Since then, the exporter could no longer benefit from CTPAT compliance until the distributor obtains re-certification. It takes a minimum of one year of full clean records to have the right to re-apply for CTPAT re-certification. The exporters (SC 'A' and 'B') switched to other transport providers, 'B' servicing other exporters (SC 'C' and 'D'), but without CTPAT certification.

After losing the certification, the CEOs decided to keep implementing and refining their security practices (P.Imp, and P.OL). According to the compliance manager, the firm have not only developed measures that make the SC3D a low risk facility, but they also encouraged (forced) its growers/exporters and transport providers to engage in lowering the risks of becoming the subject of illegal and bioterrorist activities. They prioritised business with firms committed to leverage the security resources, and able to move the large volumes of produce they distribute.

The compliance manager considers that the inspections performed by the Mexican authorities are not useful to lower the risks of illegal drug smuggling and bioterrorism, in fact they may increase the risks (P.A).

The trailer security criteria include the management of high security seals. SC3D required that SC3E locks the trailer with high security seals, and for SC3T to have full control of the seals in transit.

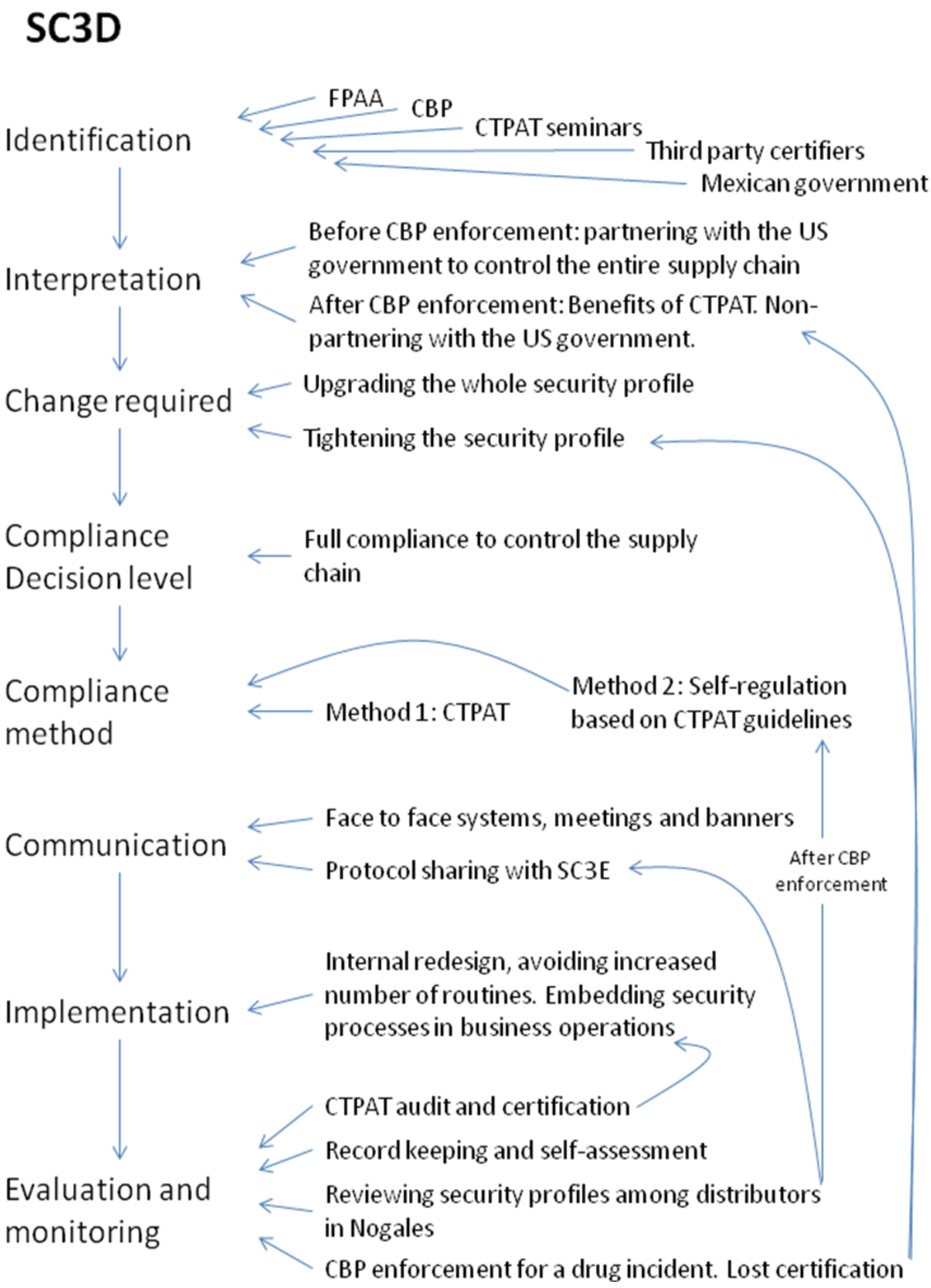
However, at their inspection points, the Mexican Secretary of National Defense (SEDENA) breaks those seals. Furthermore, there is no Mexican mandate requiring the soldier to re-seal or sign the seals monitoring forms, therefore the CEO declared that:

> *"Without the commitment of SEDENA, in terms of monitoring the violation of seals, neither we (SC3D) nor the US customs are able to tell the difference between a broken seal by SEDENA, an irresponsible driver, a drug smuggler, and a bioterrorist. There is no trust on a broken seal; the cargo needs to be inspected. Consequently, even if we were certified, we would not be able to get the benefits in case the cargo arrives to the US customs with a violated seal" (SC3D, 2007).* (P.RI)

According to assessments realised by the firm (SC3D), and other distributors from Nogales, the security resources of the firm conform to the CTPAT security guidelines (P.E). These are the result of years of trial and error implementation processes attempting to redesign the normal business operations to embed security resources in them, rather than just adding more routines to operations (P.Imp). Once the processes are re-designed, they are sent to SC3E, other exporters from Mexico, and to the transport providers that coordinate with SC3E to secure the cargo.

Currently the security measures are self-imposed, with the aim of requesting re-certification (P.OL). The risk factor identified by the compliance managers (P.E) is out of the control of the firm: the inspections are conducted by the Mexican army (SEDENA), which, according to the CEOs in SC3D, interfere with their supply chain security implementations (P.A and P.Imp).

Figure 10: Compliance process SC3D



Source: The author, based on interview with SC3D

The Compliance Resources and Capabilities

Security resources have been leveraged based upon previous experience in quality and safety regulations (P.OL). This knowledge had resulted in re-designing compliance processes that are cost/routine-effective (P.A).

In relation to the business partners, the firm conducts a basic investigation of the capacity of the firm to comply, and their certification records are useful tools that SC3D uses to assess business partners. In the compliance manager's words:

> *"A grower/exporter certified in GAP, has the degree. Every extra module in the certification represents a postgraduate degree; the more the better. Our business partners are ranked by certifications, by auditing scores, and by years being certified, the highest ranked firms are more competent and responsible than the lowest ranked" (SC3D, 2007)* [35].

In relation to the physical security, the redesign of the building structure and organisation of business operations required a trial and error analysis of times, movements and monitoring capacity. SC3D has 1 hectare (100,000 square feet) of cooling facility with multiple access points. The firm closed its access points one by one, and estimated the ratio of tac-time[77] to monitoring capacity. The firm ended up with only one access point and increased tac-time by 5 minutes per cargo; in 20 cargos this represents one more hour of operation costs. However, that is not all: there is an employee exclusively hired and trained to perform the monitoring and record keeping of the security operations, to comply with CTPAT security guidelines [36].

The CEOs declared that the firm's human capital keeps the security implementations. The personnel have been training and experimenting to find ways to embed the security operations into normal business routines [37]. The personnel in the firm contributed to the reorganisation of internal areas, with internal fences that direct authorised personnel into certain areas [38]. Two crucial employees were hired for trailer and procedural security and the analysis of biological and chemical agents in the produce. Another crucial security resource was related to the CCTV that was being installed. The CCTV itself was considered a tool: more important for the firm was the capacity of the personnel managing it [39]. The

[77] In supply chain management, tac-time is equivalent to cycle-time. In manufacturing, it represents the production time per assembly station.

compliance manager thought that CTPAT was not about the analysis of behaviour after the cargo has been unloaded but about preventing actions, which is only done by identification of suspicious behaviours by a specialised person in charge of the CCTV in real time (P.I). Furthermore the CCTV was not arranged to point towards the loading/unloading area, because there is a specialist conducting the trailer and procedural security [40], the firm would not duplicate security resources.

In relation to the procedural security, the specialist was in direct communication with the exporter and together with the driver was able to match and solve document discrepancies, provided by the driver upon arrival. These documents included the electronic manifest, the Bill of Lading, and the seals monitoring forms in case the exporter had implemented the measure. At this stage discrepancies were cleared based on good communication between SC3D, driver and SC3E. SC3D specialist issued recommendations to the exporters and transport providers on how to improve the procedural security. Furthermore, the specialist keeps records of all the matching documents and cargo discrepancies [41].

Learning and knowledge sources

The firm have based its implementations heavily on previous experience and on-the-job training for their personnel. The employees are encouraged to undertake a critical perspective on the implementations, and to try to avoid any increases in number of movements performed in their normal activities: the issue the firm have tried to encourage in their human resources is how to marry security with efficiency (P.Imp). Rather than learning from the supply chain, SC3D had tried to educate its partners (C.SD). Sometimes, the CEOs commented, the firm 'had gone too far' in educating them, since the growers and transport providers have received security profiles from SC3D ready to be implemented to their operations. When the firm encounters problems in any aspect of the implementation, especially in access control and physical security systems, it immediately issues recommendations to its exporters, including SC3E [42] [43].

Table 5.6.1: SC3D Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC	35	36;39	38		40		40			**5**	**11**
C.MS		37								**1**	
C.IC		39	38							**2**	
C.SH											
C.SD		42	43		41					**3**	
C.VA											
Resources count	**1**	**4**	**2**		**2**		**1**				
Total resources	**10**										

Source: The author, based on interview with SC3D

5.7. Supply Chain 3 Packer/Exporter (SC3E)

The compliance process

In May 2005 (T), the distributor SC3D informed the exporter (SC3E) about the need to develop a security profile to comply with CTPAT (P.RI). The exporter SC3E developed the profile by October 2005 (T), which represents the commitment of the firm to develop and implement security resources (P.OL). Development of the security resources was started immediately (P.A), and by May 2006 they were partially implemented (P.Imp). The application for certification was submitted and they were still waiting for the validation from the CTPAT officials (P.E).

The CEOs and compliance managers commented that CTPAT aimed at protecting the food supply chain (P.A), which may be susceptible to bioterrorist attacks. However, since it was voluntary, it had to offer benefits to the firms becoming certified (P.RI).

The compliance manager acknowledged that the firm was still far from compliant, although it was aiming to fully comply and get certified (P.Imp and P.E). In October 2005 (T), the initial evaluation of SC3E conducted by them and by SC3D was disappointing (P.E), finding that they still had to develop many security resources (P.A). However, they felt that their personnel had enough experience in compliance issues, based on previous know-how built out of food quality and safety regulatory compliance processes (P.I).

The CEOs and compliance manager prioritised the development of procedural security, delaying other security criteria for the later stages of the implementation process (P.Imp, and P.OL). However, such implementation did not happen without organisational rigidities in early 2006 (T), leading to intense re-distribution of regulatory compliance tasks (P.A, and P.Com) in early 2007 (T).

This was due to the firm's need to increase the efficiency of their packing operations. The firm had quality and safety routines, and increasingly efficient operations. The packing manager felt that the efficiency had contributed to a better income for their personnel in the packing operations. The personnel rejected the security implementations (P.Imp) since that would considerably reduce efficiency for an unknown period of time, in turn leading to a reduction in income for at least the same period. The firm does not pay for learning to implement security routines, only for the efficiency of their operations. Furthermore, there were personnel unwilling to incorporate more activities in their routines, arguing that they would be overloaded (P.A, and P.Imp).

The CEOs decided to re-distribute the internal roles. The firm had a quality and a safety manager (P.Imp). The packing work floor manager was leading the implementation of the 'implementation of quality and safety' guidelines in the packing operations (P.Imp); therefore, it was rather difficult for her to be assigned the additional task of security guidelines. According to the CEOs, in so doing, SC3E would be at risk of lowering the efficiency of their packing operations. The solution taken by the CEOs was releasing the work floor manager from her quality and safety responsibilities, and asking her to exclusively dedicate herself to the enforcement of security guidelines in the packing facilities (P.A).

At the same time and following recommendations by SC3D, the quality manager was assigned safety and security enforcement, and supervision roles. She was named as CTPAT compliance manager: the safety manager now had safety and quality roles. The CTPAT compliance manager and the packing manager designed the security practices, the latter was then in charge of implementing the measures in the packing area. The CTPAT compliance manager was supervising implementation not only in the packing facilities, but across all departments in SC3E (P.Imp, and P.E).

Table 5.7.1: Compliance enforcement team and roles SC3E

	Design			Implementation		
Roles/Managers	Security	Safety	Quality	Security	Safety	Quality
CTPAT manager	*	*	*	*	*	
Work floor manager				*		
Safety manager		*	*		*	*

Source: The author, based on interviews with SC3E

The CTPAT manager and safety manager designed the safety and quality practices; the latter implemented the safety and quality practices in the packing facilities, while the CTPAT compliance manager assessed the relevance and interrelationship with security measures.

The packing manager was released from his safety and quality responsibilities, to dedicate exclusively to packing operations and security implementation. The packing manager has the priority of maintaining the efficiency of the operations, and ensuring the security of the packing operations. The results of the security practices, quality and safety assurance were being assessed during 2008 (T) (P.E).

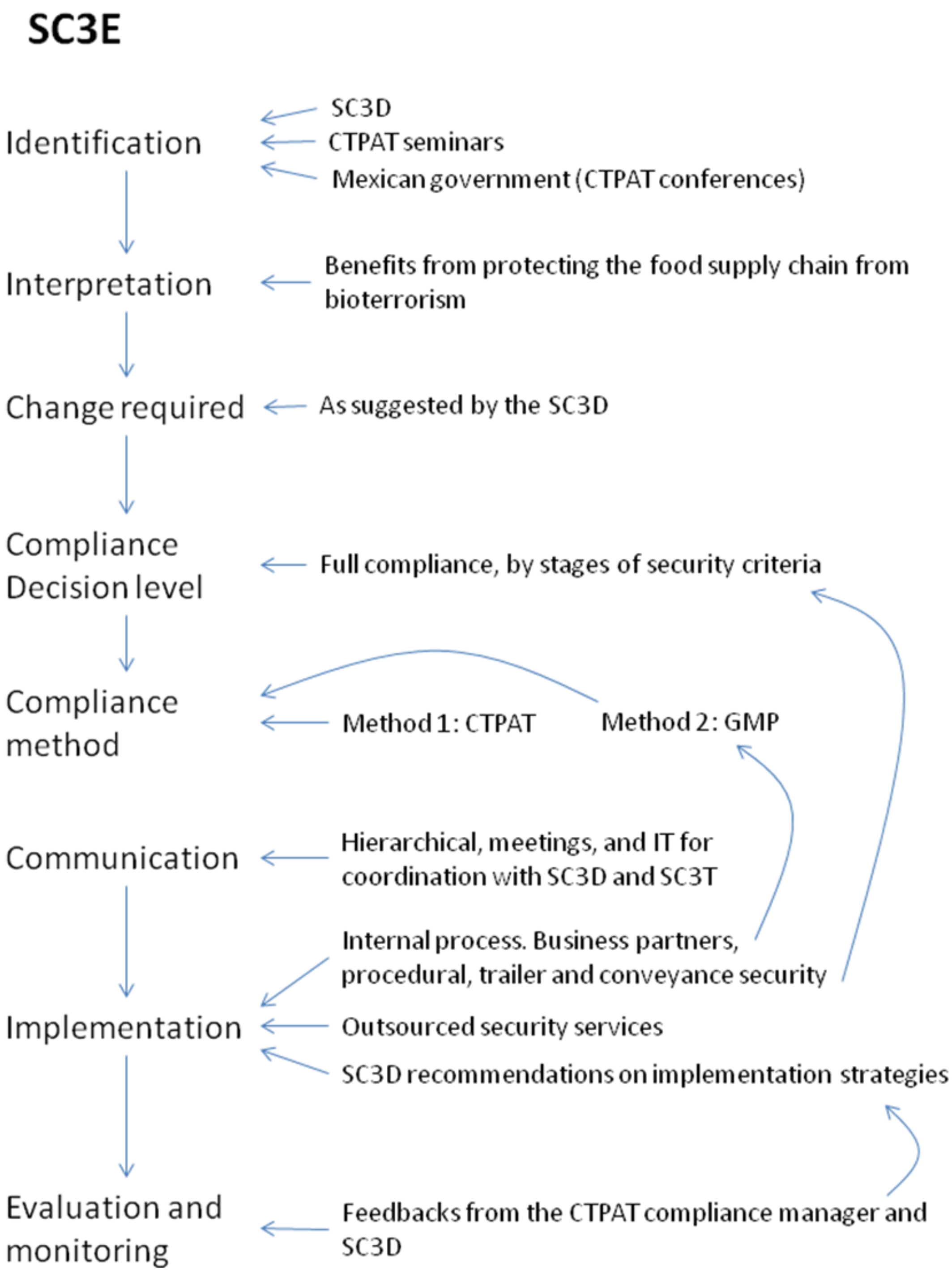
Interestingly, the CEOs and compliance managers in SC3E did not engage in analysing whether the CTPAT guidelines were suitable for the firm (P.A); instead, they followed the guidelines as suggested by SC3D, where and when they were able (P.Imp).

Due to the re-distribution of tasks in critical areas in the organisation, the firm supported its communication mechanisms with regular meetings, and face-to-face throughout the hierarchical structure (P.Com). External communication systems had been tightened with the transport provider, since there was now the need to keep tightly coordinated for cross-border operations; this is supported by the normal communication systems, radio and mobile phones, as well as GPS to match the position of the cargo with the activities of the driver, to improve traceability and enforce trailer security (P.Imp, and P.Com).

The implementation of the security measures were assessed with continuous (T) physical inspections and supervision by SC3D and CTPAT compliance manager (P.E) . SC3E encountered serious problems in assessing the security measures of the transport providers (P.E). Initially (October 2005) (T) the firm would expect to find transporters building up resources to comply with CTPAT. However they were only able to identify one transport provider with such capabilities, and it was the most expensive transport provider in Mexico (P.A).

Later, SC3D recommended that SC3E assess the security implementation of a specific transport provider (SC3T). After visiting various facilities from various transport providers, SC3E's compliance manager found that SC3T, suggested by SC3D, was the one with higher security measures and closer to the required CTPAT security guidelines (P.A, and P.E).

Figure 11: Compliance process SC3E



Source: The author, based on interview with SC3E

The Compliance Resources and Capabilities

Most of the security practices in SC3E relied heavily on the competence of the CTPAT compliance manager. Although there was little information in Mexico to conduct relevant background investigations of potential business partners, there are public records that allow the firm to know how long a firm has been in existence. Together with public registration numbers the firm has conducted visits to the facilities of their business partners, and analysed their potential to become CTPAT certified in the short run, creating a list of potential business partners [44].

The physical and access control securities required coordination between departments, and in some instances with external organisations. Internally, if a visitor says that he is visiting an employee, the guard in the entrance must contact that employee by radio, who must then confirm that he is expecting that visit, and the visitor can only be accompanied by the employee [45]. The packing manager had the responsibility of surveillance in the facilities and coordinated with the private security providers [46]. Furthermore the visitor can only leave with a form signed by the employee authorising their exit from the firm, and with a note of the reason for the visit. Externally, the guards' surveillance and access controls were outsourced to a firm providing private security services to firms. The procedures to authorise [47] and analyse [48] the visitors and personnel behaviour were designed in coordination between the security company and the managers of SC3E. These operations are active from May to July (T), when the packing facilities are in operation.

Learning and knowledge sources

SC3E is heavily dependent on SC3D for the development of their security practices. Although it is information that they receive from the distributor, procedures are tested in SC3D [49]. On the other hand, those procedures required adaptation by the firm, mainly in relation to the packing facilities that require special security control systems, and which do not exist in the SC3D [50]. SC3E later makes requests to the transport provider to implement specific trailer security measures [51]. There is an apparent flow of security recommendations from SC3D to SC3E, and later to SC3T. In the case of the outsourced services of access controls, the measures were developed jointly between the security service provider and the different managers of SC3E. The most important learning mechanisms, however, are based on increasing the firm's efficiency levels while incorporating the security regulations. It was expected that this would be in a similar way to what happened to safety and quality regulations during the compliance process (P.I and P.A).

Table 5.7.2: SC3E Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC	44				50					**2**	**8**
C.MS											
C.IC		46	45							**2**	
C.SH		47	48		49					**3**	
C.SD							51			**1**	
C.VA											
Resources count	**1**	**2**	**2**		**2**		**1**				
Total resources					**8**						

Source: The author, based on interview with SC3E

5.8. Supply Chain 3 Transport Provider (SC3T)

The compliance process

The transport provider had been informed by SC3E and SC3D in December 2006 (T) about the need to implement security measures (P.RI), but, according to the CEO they are not knowledgeable about CTPAT security guidelines (P.I). However, the firm have been chosen by SC3D and SC3E, and evaluated by the latter (P.E), concluding that SC3T is closer to complying with CTPAT security regulations than most of the transport providers (P.A).

The transport provider, however, decided not to pursue any certification, using the argument that it would be costly (P.OL). There are two main impediments for SC3T to engage with the 'voluntary' CTPAT security guidelines. First, they are already implementing security procedures that had prevented them from having incidents, and there was no need to change their security systems (P.Imp, and P.OL). Second, the US and Mexican authorities issue several other standards, including an environmental one, and according to the CEO the firm is not able to cope with all of them at once (P.Imp, and P.OL).

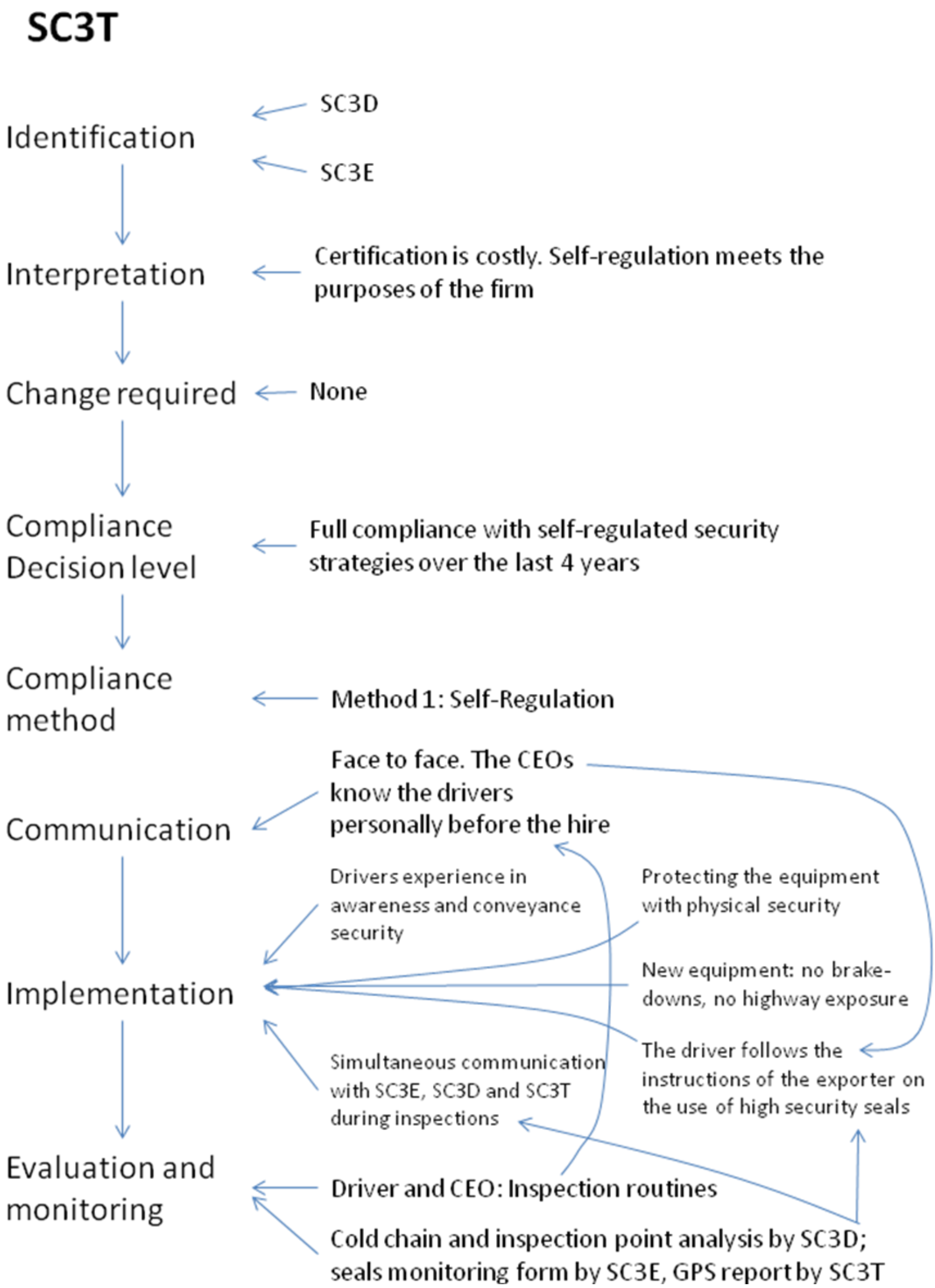
In 2006-07 (T) the United States issued mandatory environmental regulations for the transport industry (P.RI). The mandate drove the firm to initiate the substitution of its trucks for new ones, equipped with environmentally friendly engines (P.Imp, and P.OL). The current trucks were just 4 years old on average, and yet firm is investing in new equipment (P.A). This is stressful for the firm financially, diverting them from voluntary regulations, while not being enough to avoid strengthening its self-regulated security measures (P.OL). The CEO assures that protecting their investments is their priority (P.I).

Their self-regulatory security implementation started in 2003, while 2007 was the first year that SC3T worked with SC3E[78] (T). These measures were developed with the experience and responsibility of SC3T's drivers (P.Imp), as they have been increasingly aware of how to protect themselves and their cargo (P.Imp, and P.A). However, the security strategies and procedures followed by SC3T were the result of protecting, first, the firms' personnel, second, the cargo, and, third, the equipment (P.RI).

[78] The firm is substituting a previous SC3D transport provider (SC3E would be equivalent to Exporter 'B', and SC3T equivalent to transport provider 'B', in Figure 9).

The security assessments were informal (P.Imp). The firm have not been the subject of any incident in all their time in operation (P.E) whilst the rest of the industry complains about the situation. As for the facilities and equipment, every truck arriving at the warehouse is inspected by the CEO and the driver [52].

Figure 12: Compliance process SC3T



Source: The author, based on interview with SC3T

The Compliance Resources and Capabilities

Although the security resources of the firm were not aimed at meeting CTPAT security guidelines, they may be close to fully conforming to them.

The firm has a fleet of new trucks and trailers to avoid high rates of equipment failure. According to the CEOs, this makes their equipment reliable in the delivery of cargo within the time agreed between SC3E and SC3D. The trucks and trailers are well safeguarded in the warehouse and, rather than having fences, the firm decided to build a wall to protect and prevent intrusion into the facilities [53]. There is no access to the facilities unless it is with the authorisation of the managers, and accompanied by the employee that is being visited [54].

The personnel security is more of a trust-based than a formal investigation-based system. The firm does not perform criminal background checks on the drivers, nor of the business partners. The CEOs consider that "it is the responsibility of the US and Mexican authorities, since they are issuing the driving licences, to investigate the drivers and the firms" (SC3T, 2008). Furthermore, drivers are only hired after being known by the CEOs, and after cross-referencing information about their reputation among SC3T's drivers and other firms [55].

The procedural security is rather simple. The exporter and the distributor perform the shipping and receiving procedural security. The transport provider makes sure that the cargo is legal, otherwise they are not responsible for what SC3E loads into the trailer. An external company performs the electronic manifest and prior notice under SC3T's name [56]; the CEOs argued that it was a standard service provided to the transport industry. The transport provider is responsible for maintaining the cold-chain as required by SC3E and SC3D. The trailers are equipped with sensors sending signals to the driver if the temperature in the trailer changes by 1 degree Celsius, warning that the cold-chain has been broken and that the cargo needs intervention by the driver to recover the cold-chain [57].

The issue of the cold chain is tightly related with trailer security, and it is a strategy developed between SC3D and SC3T. SC3E seals the trailer with high security seals (ISO 17712) and there is a seals monitoring form in case of violation during inspection by the Mexican authorities. Usually, the cold-chain gets broken during inspections, and a signal is sent to the driver that this has happened. The driver needs to inform the transport provider that the cold chain has been broken due to the inspection. Using GPS the transport provider matches the location of the truck at the time the driver informs of the broken cold-chain, with the location of the inspection point. After inspection the driver must re-seal the trailer with another high security seal.

Three reports need to match to make sure the trailer security has not been bridged.

1) The transport provider's records of cold-chain breaks, including the time and place of the break;
2) the sensor issued by the trailer cooler, which indicates the time of the cold-chain breaks; and
3) the seals monitoring form, indicating the place of the inspection where a seal was broken, the unique ID number of the broken seal and the unique ID number of the new seal placed at that inspection point.

The coordination comes when the three reports are issued to SC3D, who analyses the three reports, the seals monitoring forms, the trailer temperature report, and the time and location of the inspection. Consequently, the cold-chain should only be broken at an inspection point, location with the GPS, at the time indicated by the temperature monitoring report, with the numbers of the broken and substitution seals of the inspection point shown in the seals monitoring form [58].

The drivers have developed their awareness on conveyance security based on years of experience and tacit agreement with other trusted truck drivers. The truck drivers learnt that they were exposed to violent or life threatening situations. Thieves and drug cartels used to threaten them in case they did not 'cooperate'; mainly smuggling drugs into the US. The firm's drivers agreed to drive in as large a convoy as possible. The problem for SC3E and its drivers is that sometimes they only require one truck hauling two trailers, in which case the driver needs to agree with other trusted drivers from other transport providers to form convoys, accumulating drivers until the convoy is large enough to ensure they feel safe. The driver requires knowledge of the other colleagues' reputations, skills to keep up with the pace of the convoy[79], and coordination to join in the highway [59] [60].

Learning and knowledge sources

The firm have learnt and accumulated knowledge from three main sources; 1) own experience in trying to protect its own personnel, the cargo and the equipment, 2) in the relationship with SC3D for procedural security, and 3) the relationship with the stakeholders, which were important to learn which drivers to hire, and to select the drivers to implement convoy security on the highway. Interestingly there is a trust-based learning mechanism behind these security practices.

[79] The distance from SC3E to SC3D is more than 1,450 kilometres. This is a crucial aspect since the driver may need to rest and the convoy may not be able to stop for a single driver: however the driver may agree with other trusted convoys to stop in a designated resting area.

Table 5.8.1: SC3T Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC				55	57			60		**3**	**11**
C.MS		53	54		52					**3**	
C.IC			54							**1**	
C.SH				55	56			59		**3**	
C.SD											
C.VA							58			**1**	
Resources count		**1**	**1**	**1**	**3**		**1**	**2**			
Total resources	**9**										

Source: The author, based on interview with SC3T

5.9. Supply Chain 4 Distributor (SC4D)

The compliance process

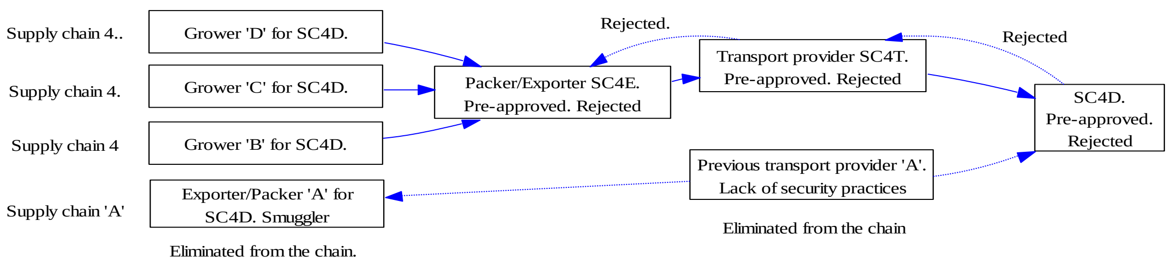
In 2004 (T) SC4D received information about CTPAT through the FPAA (P.RI). However the firm decided not pursue certification (P.OL) due to a lack of resources allocation capacity from the exporter and transport providers (P.A); if their whole supply chain was not certified there was no incentive for SC4D to get certified (P.I). However, in 2005 the firm hired a consultant, who had previously worked for the CBP, to explain what CTPAT was (P.I, and C.SH), and to help the firm to develop a culture of security within the firm (P.Imp, and C.SH). It was only in October 2006 (T) (P.A, and P.E), when the CEOs received a direct invitation from CTPAT to participate in a seminar, that SC4D decided to start their compliance process (P.Imp, and P.OL). The intention of the CTPAT officials was to grant them a pre-approval (P.OL) during the seminar, on successfully passing the assessment of the implementations and plans for implementation of the firm (P.A, and P.E).

SC4D developed the security profiles for the firm, the exporters of their group (SC4E), and for their transport provider (SC4T) (R.Pro, C.OC and C.SD). During the event, the CTPAT officials, together with SC4D's CEO, identified the weaknesses in their security practices (P.A, and P.E). In order to receive the pre-approval from CTPAT, the CEO signed an agreement to develop the security resources for full compliance by the firms (SC4E, SC4T, and SC4D) (P.Imp and C.SH).

The resources that they agreed to develop were physical security and access controls, personnel dedicated exclusively to CTPAT compliance, and training in terrorism and illegal activities awareness. The pre-approval was granted: they then waited for the auditors to visit their facilities (P.OL).

Unfortunately for the whole supply chain, they did not get certified (P.OL). This was due to a drug incident detected in February 2007 (T) by the CBP in an exporter (not directly related with the SC4E), to which SC4D used to provide distribution services (P.E). The CTPAT officials considered that the exporters' supply chain was risky, and all the 'service providers from that exporter were included in a list of risky firms associated to such exporter. As the name of SC4D was on the Bill of Lading of the Exporter that was caught smuggling (see Figure 13, p.163), SC4D was rejected for certification. In addition, all of supply chain-SC4 (Exporter, Transporter, and Distributor) also had their certification applications rejected (P.E). The firm (SC4D), however, continued developing the CTPAT security resources in a self-regulated fashion (P.OL).

Figure 13: Supply chains effects of lost certification by SC4D



Source: The author, based on interview with SC4D

The implementation process required involvement of all the personnel and a compliance team (P.Imp). The personnel contributed in the re-design of the infrastructure, while the firm's compliance team designed the access controls mechanisms (P.Imp, and C.OC). The personnel were not able to monitor the shipping and receiving of cargo through all the access points in the warehouse; some were closed and CCTVs were installed to support the monitoring procedures (P.E, and R.Phy).

The most important changes were related to the operational procedures, which required performing inspections and recordkeeping of practically all security related operations in the warehouse (P.A). However, the firm initially faced problems due to personnel resisting the adoption of the security measures. This was solved with the support of a consulting company, which was intended to induce a culture of security in the firm through seminars and constant meetings (P.Com). Although the personnel eventually agreed that the changes were required, they could not think of ways to incorporate the security activities in their existing routines: the result was that new security operations were just added to their pre-existing routines, increasing the overall time of their business operations (P.A, and P.Imp).

The CEOs mentioned that resistance to change was not a new story in the firm. In fact, they went down the same path when they started the compliance process with GMP (Good Manufacturing Practices), started six years ago (2001) (T): changing the culture of the employees, equipment, procedures, and practices. To the extent that the organisational culture started slowly changing, the personnel started re-thinking their activities and procedures, and small tasks were improving slowly (P.Imp).

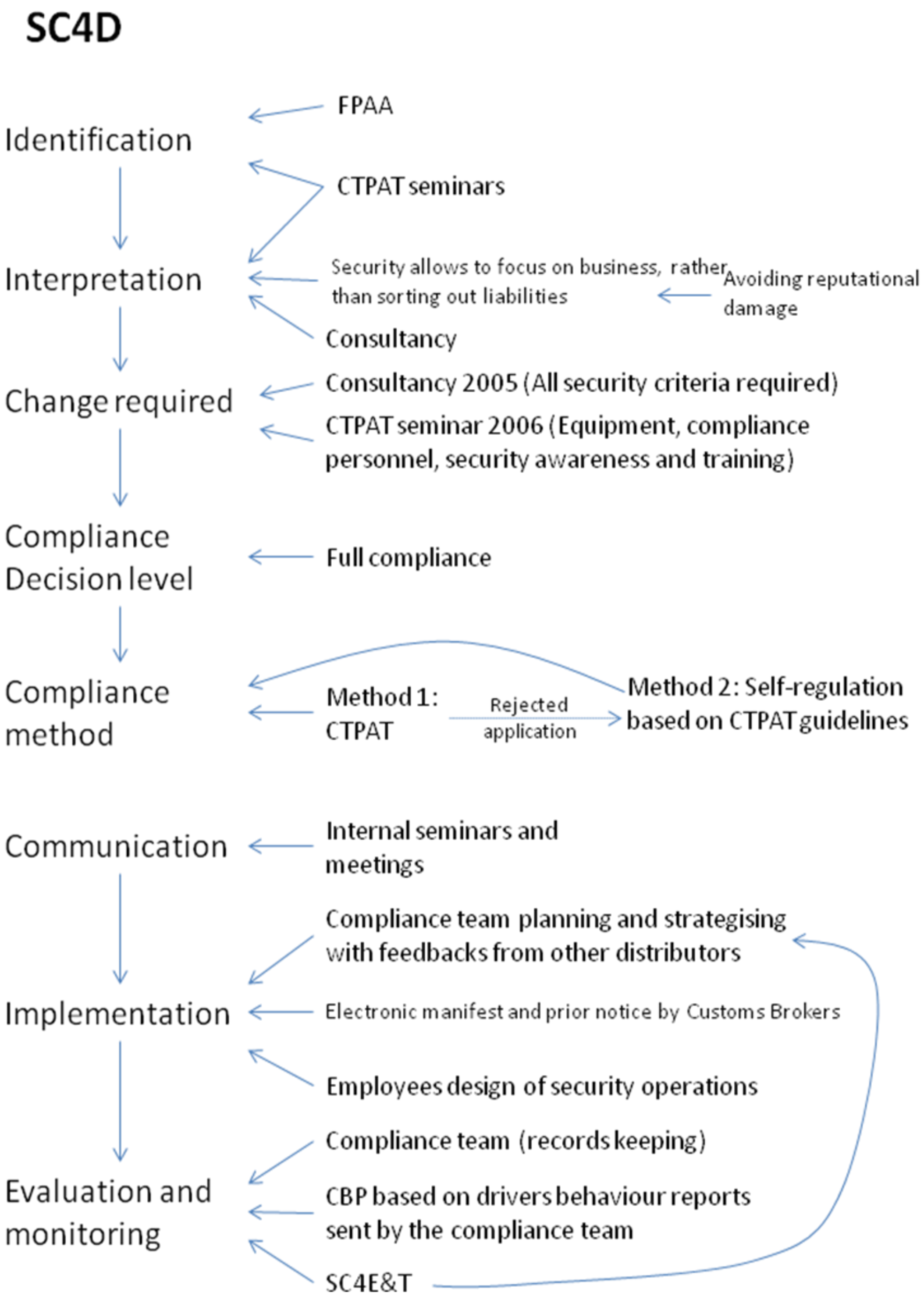
The CEOs estimated that, in November, 2007 (T) the firm was able to comply only one week and not three days in CTPAT (P.A, and P.OL); and he expected, just like with GMP, by the following year (T) they would comply over several weeks and for a couple of days they would fail to comply. Eventually the firm would have an automatic and fluid compliance process (P.E).

The compliance team, which included SC4D's general manager, was responsible for the assessment of the security operations; also for managing the issues raised by the personnel during attempts to implement the security activities. Since records of the operations were kept, the compliance assessment team was able to analyse whether the operations conformed to the guidelines. If that was not the case, the person not complying was encouraged to re-think the procedures. In addition, the CEO discussed the implementation strategies with SC4E&T and other distributors in Nogales, and used to get feedback to improve processes, for instance, on what security criterion to prioritise for implementation (P.E, and C.SH).

The firm also have decided to establish a closer relationship with CBP in making decisions about whether a cargo coming from Mexico was risky or not. That was an attempt to re-build the trust that CBP used to have in SC4D. The CEOs believed that the CBP still considered their whole supply chain unsafe and ineligible for a certification in CTPAT. This is why, every day, SC4D sent transit condition reports of every cargo due to queue at the port of entry waiting to be inspected by the CBP (P.Imp), together with the GPS traceability reports,. The CBP assessed whether a driving behaviour was suspicious or not, therefore whether to inspect them or not (P.E). The compliance team in SC4D have developed a tacit knowledge on what type of driving behaviour is more likely to be considered risky, and then communicated this to the transport provider (SC4T) for further investigation before reaching the port of entry (P.E).

External organisations also played a crucial role in the procedural security implementation for SC4D. The Mexican and US customs brokers are in direct communication with SC4D (P.Com), and they are the ones realising the electronic manifest and prior notice to the CBP and FDA correspondingly. These are the compulsory aspects of the security regulations, which means that these key security procedures are outsourced (P.OL, R.Pro, and C.SH).

Figure 14: Compliance process SC4D



Source: The author, based on interview with SC4D

The Compliance Resources and Capabilities

The firm built up their physical security, based on internal coordination recommendations by re-designing the organisation of their operations [61]. It did, however, require long term cultural change from the personnel.

The physical access controls were developed based on strategies from the compliance team, and new administrative procedures to manage visits and limited access by personnel to certain areas in the facilities [62].

Background checks on personnel were being carried out by the CEOs, however these consisted only of normal references and not thorough checks. The CEO mentioned that they may need to perform more thorough checks soon.

The procedural security was developed by their personnel through trial and error. It required an important cultural change to initiate the learning process, which was induced by the consultancy company [63]. The crucial mandatory aspect of the procedural security performed by the customs brokers required strong negotiation, and, most of all, collaboration from them. This was because, in order to be able to submit the electronic manifest and prior notice for trucks joining the port of entry at 8am, the customs brokers needed to manifest and notify at 6am. They dedicated special personnel to perform such operations, which were also used for the rest of the customs broker's clients [64]. The fundamental element leading the agreement was the long term relationship between the customs brokers and SC4D [65].

The trailer security and conveyance security reflected the changes incorporated because of the rejection of the certification. There was a tight coordination between the shipping receiving department and SC4E&T, especially in the analysis and feedback of the drivers' behaviour on the Mexican highway. SC4D asked SC4E&T to adapt to their needs, as well as providing support to SC4D in any respect related to trailer and conveyance security [66] [67].

The cultural change and the security awareness were all derived from a consultancy firm providing the service in 2005 (T). The firm would have not been able to start the compliance process without such training [68].

Learning and knowledge sources

The physical and access control relied heavily on intra-firm learning and knowledge generation and accumulation. The procedural, trailer, conveyance, and awareness security procedures on the other hand, required more involvement of external organisations, such as SC4E&T, consulting firms, other distributors and the CBP. However, most of the compliance process was closely monitored and supervised by the CEOs.

Table 5.9.1: SC4D Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC		61			63					**2**	**12**
C.MS			62							**1**	
C.IC		61								**1**	
C.SH					63; 65		66;67	66;67	68	**5**	
C.SD					64		66;67	66;67		**3**	
C.VA											
Resources count		**1**	**2**		**3**		**2**	**2**	**1**		
Total resources	**11**										

Source: The author, based on interview with SC4D

5.10. Supply Chain 4 Packer/Exporter & Transport Provider (SC4E&T)

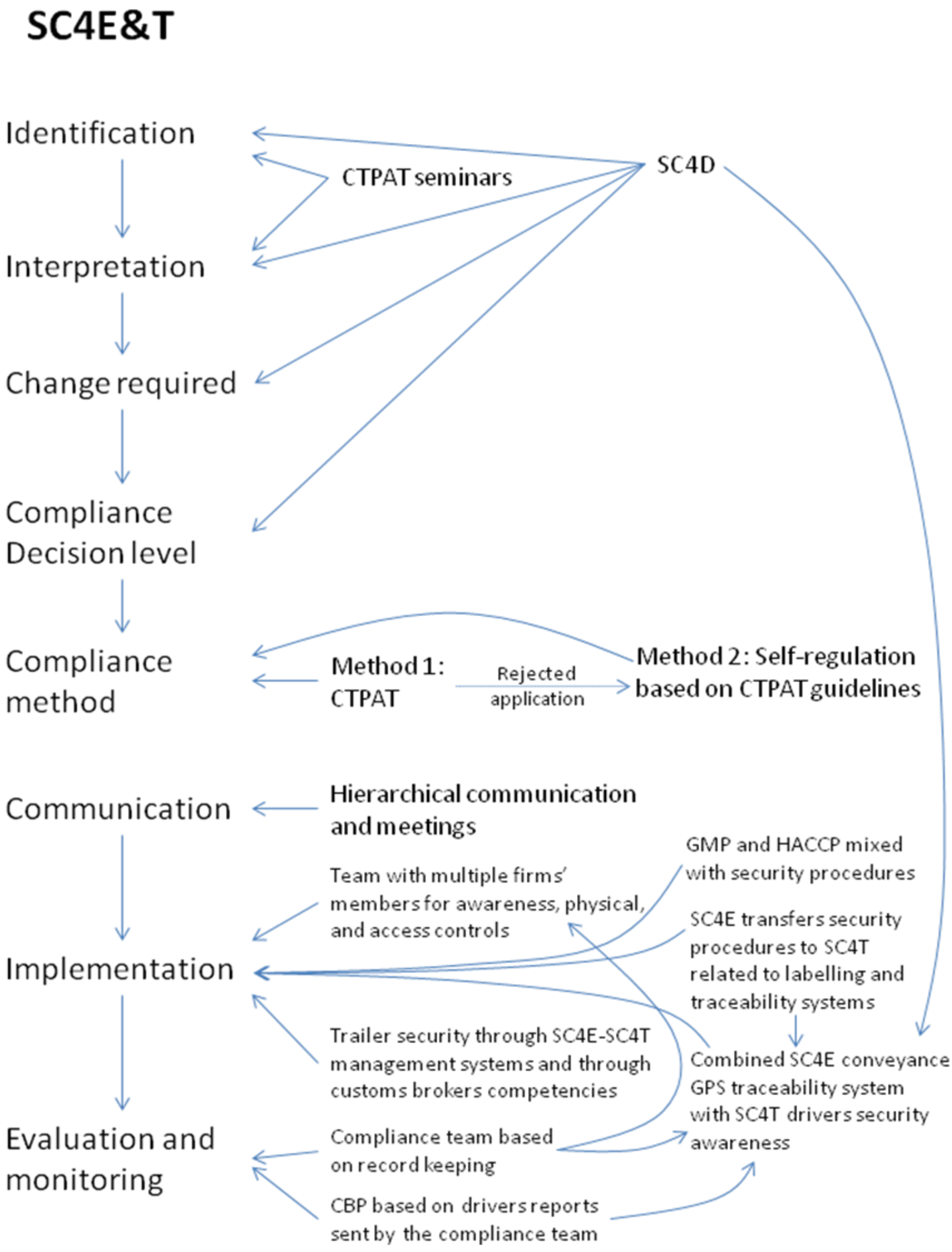
The compliance process

In this section, the compliance process describes the story of two firms (SC4E and SC4T). SC4D decided and instructed that these two firms should form a 'special operations team' (compliance team) in charge of supply chain issues: one of these was the compliance process with CTPAT. The supply chain strategy considered that one compliance team should be in charge of the Mexican side of the supply chain and another in charge of the US side. Consequently, although there are two different entities, this case study presents the compliance process as if they were a single entity (SC4E&T), just as instructed by SC4D's CEOs.

As mentioned in the previous case, SC4E&T was part of the application pack that SC4D developed in October 2006 (T) during a CTPAT seminar, which was rejected in February 2007 (T). What is relevant and different from SC4D is the implementation process. Hence this study focuses on that stage of the compliance.

In relation to the monitoring and assessment of the overall security implementations, that is also continuously done by the compliance team, and the assessments are reported to SC4D, who in turn reports to the CBP (P.E).

Figure 15: Compliance process SC4E&T



Source: The author, based on interview with SC4E&T

The Compliance Resources and Capabilities

The compliance team combined each company's knowledge of the operations (SC4E's packing and SC4T's surveillance) into one procedure, which, according to the compliance team, contributed to physical security, access controls and awareness.

The compliance team members from SC4E contributed with knowledge of the complex times and motions in the facility, something difficult to understand for outsiders [69].

The members from SC4T contributed systematic and random surveillance expertise to help identify suspicious and abnormal behaviour in a facility, something managers were not able to do. The team designed uniforms with different colours per working area, together with the enforcement of mixed systematic and random surveillance rounds by SC4E's security personnel [70].

According to the compliance team, it was easier for the surveillance and packing managers to identify the flow of colours by areas, which could change daily according to the compliance team's specifications [71]. Furthermore, the enforcement of the surveillance was done with a TouchProbe device, which indicates whether a guard made the round in the indicated areas and at specified times. The TouchProbe is unloaded in software that indicates the frequency, location and time of the surveillance, and keeps records of the rounds and the guard that performed the round. Training on the use of the software and its implementation possibilities was delivered by the software supplier [72].

CCTVs were also installed in SC4T's 'Trocaderos' (their cargo inspection and re-packing facilities in Nogales, Mexico), which did not require much effort since the security personnel were already familiar with the system [73].

After the drug incident (February 2007) (T) SC4E&T started performing full background checks on drivers and security personnel. These included more than normally recommended - psychological and physical tests performed by the human resource department, anti-doping outsourced analysis, and a criminal conviction check performed by the State police department. These were later analysed by the compliance team to issue decisions on whether to keep, fire or relocate personnel [74].

Although CTPAT promotes its regulations to prevent terrorism, SC4E&T narrowed it down to bioterrorism, which implied paying particular attention to the prevention of produce contamination (P.I, and P.OL). SC4E's competencies in GMP and HACCP were used to enhance the procedural and trailer security. The aim was to have safer and more secure cargo by sanitising and inactivating any biological or chemical component that may be present in the trailer prior to loading. SC4E&T received this training from CIAD[80] [75] [76].

The firm needed to report all the security measures and monitoring systems and assessments to CTPAT, in case they allowed the firm to re-apply for certification; SC4E&T set up a traceability system for the produce from the pick-up location to the supermarket in the US. Furthermore, the compliance team argued that they were able to identify who was in touch with the produce at a place at any given time. For that, SC4E&T had developed labelling standards before CTPAT. Such labelling systems were part of SC4E's compliance to GMP (Good Manufacturing Practices) [77].

The information technology security resources have been upgraded by further restricting access and narrowing down the identification of potential users of the systems. Access to computers was password protected and shared between SC4E, SC4T and SC4D. However, while the password protection had previously prevented accidental access and manipulation of databases, they were later re-designed to identify the type of personnel that accessed the systems, in addition to identifying intentional/accidental manipulation of information. The type of login profile and password would be indicative of the type of personnel that accessed and manipulated the data. Although it is still not personalised, it allows a potential investigation within the supply chain to be narrowed down to departmental level within each firm [78].

The same is true for trailer security, which requires sharpened competencies by the customs brokers during the analysis of the seals monitoring forms. The trailer security practices were agreed with SC4D and the customs broker; the latter is who authorised the type of seals to be used and monitored them. When a cargo is sent to Nogales, SC4E electronically sends a list with seals ID numbers to the custom broker. In case the cargo requires inspection in SC4's Trocadero (facility for cargo inspections and burreros

[80] Centro de Investigacion en Alimentacion y Desarrollo, A.C. is a Mexican research centre specialised in social, economical, technological, environmental, and policy related to food and alimentation.

attaching the trailers), the custom broker analyses the seals and the monitoring forms of the seals. They have the competencies developed throughout the years to know whether there is something strange on the form: it is the custom broker who considers if a trailer is risky [79].

In relation to conveyance security, the development of the resource required interaction between the GPS systems developers (OmniTrack) and the specialised awareness of SC4T's drivers. The GPS software developer was required to set up the virtual limits and conditions of the highway where drivers were authorised to drive through. Hence SC4E&T was able to identify when a driver was diverting from an authorised route, when he stopped longer than expected, and so on.

The combination of a standards specialised GPS system with the specific knowledge of the highway driving behaviours, allow the monitoring and reporting of conveyance security threats. The compliance team argued that there were many software providers that could equip them with the GPS systems, but only in combination with the knowledge of the drivers could that tool be useful. This was due to the fact that, while the GPS did not need continuous upgrades in terms of its functionality, it required updated reprogramming to reflect the changing conditions of the 'unsafe' Mexican highways. SC4E&T combines the GPS/highway knowledge capabilities with long-haul driving behaviours to create an important security resource to meet the CTPAT security criteria [80].

Learning and knowledge sources

The resources that SC4E&T have been developing may reflect the post rejection effect, and the attempts to recover their reputation and accelerate the permission to re-apply to CTPAT.

Knowledge has been gathered from all possible sources: internal, between SC4E and SC4T, and with other stakeholders, such as CBP, OmniTrack, SC4D, and so on. The weakest areas to secure in these SC was the conveyance and trailer security; consequently, the knowledge and learning process to build up these trailer security resources have leveraged from stakeholder's feedback, whilst conveyance security resources have apparently been leveraged from alignments.

Table 5.10.1: SC4E&T Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC		73		74	75	78	75	80		**5**	**17**
C.MS				74	77				72	**3**	
C.IC					77					**1**	
C.SH				74	76		76;79	80	72	**5**	
C.SD											
C.VA		69	70						71	**3**	
Resources count		**1**	**1**	**1**	**3**	**1**	**3**	**1**	**2**		
Total resources	**13**										

Source: The author, based on interview with SC4E&T

5.11. Supply Chain 5 Distributor (SC5D)

The compliance process

Although the CEOs knew about CTPAT from the CBP (P.RI) and they were implementing security measures, surprisingly, they did not engage in the certification process until several months before attending the CTPAT seminar in October 2006 (T). It was then that the compliance manager started putting together SC5D's security profile (P.A). In the seminar the firm received pre-approval (January 2007) (P.OL), and soon after the approval (P.OL). The firm was still waiting the validation *in situ* by a CTPAT supply chain specialist in December 2007-January 2008 (T). Unfortunately for the distributor, their transport provider (SC1&5T) had been delaying the certification; therefore SC5D would not be able to use the FAST lanes (P.A).

The firm had been engaged in the implementation of the security regulations for two reasons, 1) acquiring the benefits of using the FAST lane, and 2) although at the moment the regulation is voluntary it may become mandatory (P.I). The latter motivation developed after the ACE (Automated Commercial Environment) was phased out as a voluntary programme to become mandatory (P.RI, and P.I). The CEOs had the impression that the US government was refining CTPAT as a regulation, and when there was a critical mass of certified firms and better regulatory design, it would become mandatory (P.RI). Consequently, the firm opted to capitalise on the benefits of certifications as soon as possible rather than perhaps being caught in the chaos of the change from voluntary to mandatory legislation (P.I, P.A, and P.OL).

The CEOs were of the idea that their security measures were rather superficial and their formal assessments not yet fully reliable (P.A). However, the firm had previously performed safety assessments, and the compliance manager was attempting to build up from there. That was due to their understanding of safety and security as interrelated measures (P.OL).

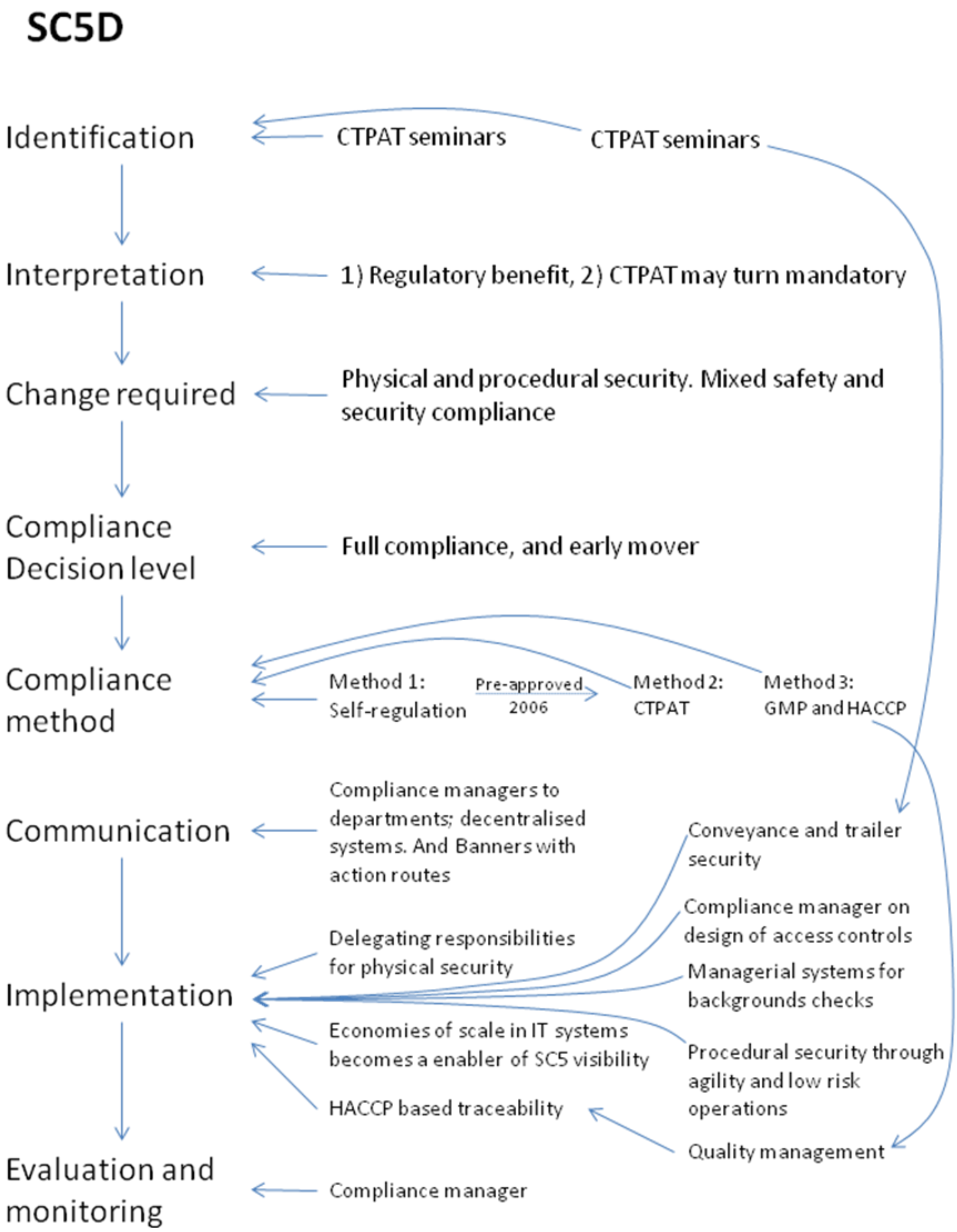
The first self-assessment of the security status was based on the security profile developed for the 2006 CTPAT seminar (P.E). The results showed weakness in the procedural security, and physical and personnel security (P.Imp). The firm would need to introduce radical changes in these two aspects to prevent future major modifications (P.A).

For the firm, full compliance would be achieved on the cost-effectiveness of the security resource (P.OL). They tried to keep expenditure in security resources to a minimum, but not to the extent of leaving the firm unprotected. That required assessing different options for developing or acquiring resources (P.A, and P.Imp). This strategy was learnt from an experience in the CTPAT seminars, where firms declared that the use of batches was useful to identify personnel in restricted areas; other firms introduced uniforms with colours per working area for the same purpose. Since both ways were accepted by CTPAT managers (but coloured identifications were preferred by CTPAT officials), SC5D decided to provide coloured batches, aimed at trying to find ways to save money and invest more substantially in critical security resources (P.Imp).

According to the compliance manager, this is the dominant strategy in the firm. That same notion was followed for the installation of CCTVs and access controls years before CTPAT was considered by the firm. The firm evaluated the coverage, cost, and adaptability of various systems (P.A, and P.Imp).

For the compliance manager, the implementation strategy and procedures had to be based on relegation of responsibilities in formal meetings (P.Com) to different departments within the firm (P.Imp). For instance, CCTV and electronic access controls to the facilities were delegated to the IT department; the procedural security was delegated to the warehouse operations manager; the trailer and conveyance security was delegated to the shipping/receiving department. Delegation played an important role in the security implementations of SC5D (P.Imp).

Figure 16: Compliance process SC5D



Source: The author, based on interview with SC5D

The Compliance Resources and Capabilities

The background checks on business partners were not developed in SC5D, the reason being that SC5D would not investigate their own family business (SC5E and SC5T); however, they were not performing substantial checks on the rest of their exporters either.

Physical security resources were leveraged out of managerial activities and internal coordination systems, consisting in meeting and tasks delegation (P.Com). Before CTPAT, the firm did not have physical security, except from CCTV and electronic access controls. Physical security involved meetings with the heads of each department to plan the reinforcement of the buildings; these department heads had specific knowledge on the status of the building and insights on how it could be reinforced. Most of the contributions came from the operative departments and less from the administrative areas. Once the decisions were made, the delegation of tasks among personnel followed [81].

The physical access control required only incorporating technological resources and compliance manager competencies to design and identify procedures to restrict areas within the facilities. This was combined with the coloured batches given to the personnel to identify their workstation and whether they are allowed in certain areas of the facilities. This resource did not demand much effort, only feedback from the CTPAT seminars and applying the cost-security effectiveness criterion; these were all the responsibility of the compliance manager [82].

The personnel security resources were developed before CTPAT and these were self-regulated systems incorporated into the normal human resources management routines. The compliance manager expressed the seriousness of this practice, and the records of the employees are not difficult to gather from all governmental agencies. These routines are run by the human resources department [83].

The procedural security began to be developed in 1997 (T) when the firm moved to the current facilities. At that time (1997), it was not part of a well-planned or designed strategy, according to the compliance manager however, the criteria were lower risk and more agility (P.I). All started with unloading and loading procedures, where clear spaces and only incumbent operators were allowed [84]. This lowered the exposure of produce and raised the efficiency of the operation. The same criterion was applied in other areas, warehouse, inspection areas, and sanitation materials, etc. The procedures led to safer and more agile operations, which was increasingly appreciated by their clients and the industry in general since the risks of accidents, contaminations, and inefficiency were reduced.

The initial development with procedural security responded to their quest for more efficiency and compliance with GMP, therefore, they were resources dedicated more for shipping/receiving operations. Later (October 2006) (T), they evolved to comply with CTPAT, specifically in traceability systems, increasing the potential identification of suspects of intentional/accidental contamination of the produce [84]. To achieve that, it was necessary to issue contamination reports to be analysed by specialised human resources, who in turn would identify potential suspects [84].

The traceability system was rudimentary, yet it met the security purposes. The boxes do not contain barcodes, only the pallets. Each pallet had a tag attached at the moment when was filled up in the field; that tag relates to the IDs of boxes contained in that pallet, the field, furrow, day, time, truck that moved it from the field to the packing, commodity, size, variety, and so on. It was also possible to know who packed it, as there is a packer (person) ID number written on the box.

The original purpose of the traceability system was to know, just in case, where a produce could have been contaminated. On the other hand, the packer and other human resources ID numbers were used for quality management, performance and payment purposes. The identification of a suspected accidental/intentional contamination would be impossible under separate reports, whereas by cross-referencing the traceability information with the packer numbers, SC5D would identify not only the origin but also the potential person responsible for a contamination. However, the information system for cross-referencing was not developed by SC5D, but SC5E. Therefore, the cross-referencing had to be done by SC5E and passed to SC5D [85].

The IT systems and software were the same in SC5D and SC5E; the difference was the function given by each firm. All the systems were installed by the same developer (SC5E's compliance manager, who previously held responsibilities as SC IT manager). The developer incorporated the functionalities of each firm into the same system; therefore the IT is a fully integrated resource that allowed both firms to access and modify information from SC5D and SC5E, with password identification of data entry and management. This meant that the firms would not have to invest in different IT systems, and the only extra investment would be on the training on the specific functionality of the IT system for SC5D. This system contributed to the visibility of the supply chain information; however the system could also be modified to grant access to critical information from both firms (SC5E or SC5D). According to the compliance manager, however, the user login type helps identify the persons that accessed or modified the information [85].

Before the CTPAT compliance process, trailers were sealed by SC5E; however, after the first inspection by the Mexican authorities the trailer remained unsealed for the rest of the journey until it reached the distribution centre. Since there was no security procedures or monitoring of events on the journey, SC5D was unable to reliably match information related to the cargo, trailer, truck, and driver (P.A).

To meet the CTPAT compliance process, SC5E provided the drivers with extra seals to re-seal the trailer in case of inspections on the Mexican highway; in addition, the violated seals needed to be recovered by the driver. Each seal has a unique identification number. SC5E also gives a signed seals monitoring form to note the ID number of any seal broken by the Mexican inspectors and the ID number of the seal placed by the driver; this form is 'supposed' to be signed by the Mexican inspector, which does not always happen. These seals monitoring forms, together with the violated seals, needed to be given to the receiving manager at SC5D. The receiving manager at SC5D had to match the electronic manifest, drivers' licence, truck number and trailer number associated with the driver, with the name on the monitoring form. If everything matched, the cargo was low risk. The analysis of documentation and monitoring forms and seals require competencies developed over time by the receiving manager, and these were competencies taught during CTPAT seminars [86].

Learning and knowledge sources

The leverage of security resources in SC5D required a strong emphasis on internal knowledge and internal learning processes. Previous compliance with food safety regulations harnessed the firm with a platform to leverage security resources. This was due on one side to the interrelation between safety and security procedures, and on the other to the fact that experience led the firm to follow 'similar ways' to now reach compliance with security regulations. The firm also supported its learning from stakeholders such as participation in CTPAT seminars, close communication with the supply chain specialist from CTPAT, and the resources developed by SC5E's IT department, and implemented in SC5D. Furthermore, the traceability security resource required intense feedback from SC5E to SC5D in order to understand the mechanisms and their potential use for security purposes.

Table 5.11.1: SC5D Security resources and compliance capabilities sophistication

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC			82		84		86			**3**	**10**
C.MS		81		83	84					**3**	
C.IC		81			84					**2**	
C.SH						85	86			**2**	
C.SD											
C.VA											
Resources count		**1**	**1**	**1**	**1**	**1**	**1**				
Total resources	**6**										

Source: The author, based on interview with SC5D

5.12. Supply Chain 5 Packer/Exporter (SC5E)

The compliance process

The firm became aware of the existence of CTPAT in late 2002 (T) (P.RI); however they were not interested in being certified at that time (P.OL). Nevertheless, in early 2003 (T) a CBP official went to their industry association (CAADES) in Mexico to promote the programme, and made it clear that, in the case of another attack, the US government would implement emergency management and during that period only CTPAT certified firms would be allowed to trade with the US. According to the compliance manager, "it was a rather convincing talk" (SC3D, 2007) (P.I).

Consequently the firm started their quest for certification in CTPAT and FAST for their transport providers (P.OL). In summer 2003 (T) the firm contacted a consultant from Ciudad Juarez, Mexico, who advised SC5E and other exporters from the region. However, in 2004 (T) in the middle of the implementation process, the rest of the exporters lost interest in the certification. As a consequence, the consultant stopped providing the service as there was no critical mass of interested exporters, and the fee covered to SC5E would no longer be enough to cover the consultancy costs.

SC5E continued developing its security resources (P.Imp), and by 2005 (T) they felt they were ready for certification, but they had no one to champion their application (P.A, and P.OL). On the other hand, the compliance manager still doubts had about whether their security measures conformed to CTPAT guidelines. In the same year (2005) (T), SC5E got in touch with a consultant from California, who agreed to help them. The consultant provided the service not only to SC5E, but also to other exporters who were increasingly interested in CTPAT due to intense promotion around Mexico and the US at that time (2005) (T). The consultancy fee was very high, but it was shared among the group of exporters.

In that year the consultant assessed SC5E's security implementation, and concluded that most of the resources conformed to CTPAT guidelines (P.A). Therefore the consultant developed the security profiles together with the firm, and, at the end of 2005, the application was sent (P.OL). The firm received minor comments from the CBP (P.E), and then had to make minor changes to get ready for an *in situ* validation by a CTPAT security specialist. However, SC5E was concerned about the time that could pass before they obtained validation, since there was a queue of approximately 300 applications before SC5E could be processed. For the compliance manager that was equivalent to an involuntary compliance delay (P.OL, and P.I).

According to the firm, they were lucky to have that particular consultant, who was well known in Washington, and who convinced CTPAT officials that SC5E was ready for certification and deserved to be moved forward in the queue. CTPAT agreed and placed SC5E around the 20th to 30th positions. In a couple of months the firm received the supply chain security specialist from CTPAT, and in early 2006 (T) the firm was validated (fully certified) (P.OL, and P.E).

The implementation process lasted approximately one year, and was expensive in terms of investment and time spent for the development and deployment of security resources. It required full-time support from the consultant (P.Imp).

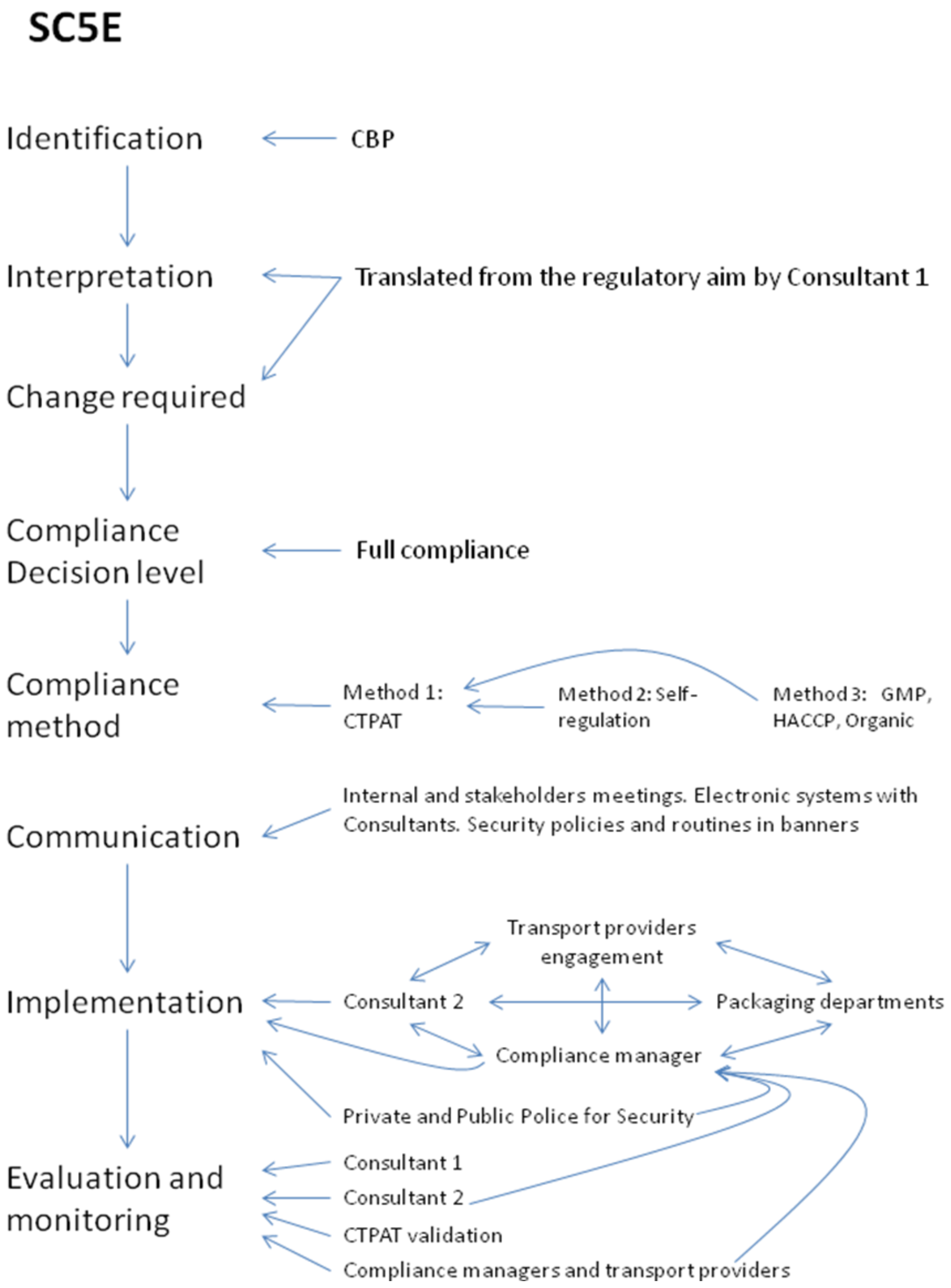
The firm acquired the security resources during 2003-2004 (T), however they did not know how to use such resources. On the other hand, the consultant already had a security programme developed for all the exporters. SC5E then added to the pre-existing security resources what they were told by the consultant. SC5E's main resources missing at that time (2004)(T) were record keeping, checklists, procedural and logistical security (P.A).

At the same time, the resources that were developed and readily available were not being exploited. The firm was unknowledgeable about how to use such resources (P.Imp). It was the consultant who designed the routines to start deploying the security resources (P.Imp). This once again required the presence of the consultant to assess the progress in the implementation of the security resources (P.E). When things were not working well, he would re-design the procedures and operations (P.A). It required constant communication and working as a team with him (P.Com).

Most of the security criteria were developed and enhanced based on a combination of knowledge and learning from key internal managers, transport providers, customs brokers and consultant, with the consultant leading the implementation and records keeping design that contributed to compliance with CTPAT (P.Imp).

Finally, the assessment of the implementation programme was continuously performed by the consultant, the compliance manager and heads of different departments of SC5E, and transport providers. However there were various assessments stages: 1) incomplete implementation and assessment by the first consultant in 2003; 2) complete implementation and assessment with the second consultant from 2005 to 2006 (T), which also considerably enhanced the security awareness of the firm and its supply chain partners; 3) CTPAT validation February 2006; and 4) currently, the compliance manager together with the transport providers running continuous assessments and monitoring, and updating procedures as required by CTPAT guidelines (P.E).

Figure 17: Compliance process SC5E



Source: The author, based on interview with SC5E

The Compliance Resources and Capabilities

Although SC5E was an independent entity, the shareholders were the growers to whom they were providing the packing and exporting services. On the other hand, the transport providers were the same they had been working for years, who had also been developing security measures with SC5E. Hence, the stable relationship with its distributor (SC5D) and its transport providers (SC1&5T and five other transporters) supported their idea of not needing to build up resources to perform background checks on business partners; at most, there was an assessment of their security profiles [87].

However, there was always an element of risk, since at times the transport providers were not able to move all the cargo for SC5E, leading the exporter to hire services from other transport providers. The compliance manager declared "unfortunately this is a business that is driven by market prices, not by implementing security measures, however, if there was a problem with drugs, the transport provider would be completely eliminated from the chain, it had happened before" (SC3D, 2007).

Due to the size of the business operations, the firm needed to build up physical security resources before the CTPAT compliance process. The firm required some degree of protection of personnel and facilities. However, the alarm systems and CCTV were exclusively acquired and installed to comply with CTPAT. Hence, these resources required investment and training on the use of the equipment for the security personnel and managers [88].

The access controls were performed by the PEP (State Preventive Police under the Sinaloa Department of Public Security) and private security guards. Having both organisations allowed the private guards to learn from the public officers, improving their capacity to restrict access to the facilities with bigger coverage [89].

Controlling access to restricted areas within the packing facilities was not part of the duties of the surveillance personnel but of the operations managers. To help in the identification of personnel by areas, the firm had provided coloured vests as suggested by the consultant. However, it was also necessary to enforce the surveillance performed by the private security guards, due to the CTPAT requirement to have records of this particular activity.

The firm was informed by a guard about an automated system (TouchStar) to keep surveillance records. This system is a magnetic pen that records the time and place when it touches magnetic plates, which are fixed to the walls around the packing facilities. The pen loads the information into software that keeps records of the inspected points, times and guards [90].

According to the compliance manager, personnel background checks were not a feasible resource to develop. The firm had 600 people in the packing facilities and 2,000 in the field in 2008 (T). Background checks were plausible, and in fact performed, for personnel in key positions such as security personnel, those in loading and shipping areas, warehouse, etc. To support the backgrounds and behaviour, the firm acquired biometrics equipment and received appropriate training by the technology providers. According to the compliance manager, the firm was continuously updating a database of key personnel [91].

The most difficult resources to develop were the procedural security. All these required not only implementation, but also record keeping for submission to CTPAT as proof of their adherence to guidelines. This required intense coordination among different areas in the packing, the compliance manager, transport providers and the consultant.

The firm had already developed traceability and management systems, and but was not able to give those resources any security related functionality. The compliance manager arranged meetings with different departments and the consultant to identify possible solutions.

Firstly, they looked for ways of identifying a person that intentionally or accidentally contaminated the produce. Personnel from the quality department mentioned that it was not possible to know who, but it might be possible to know where, based on mixing information on HACCP (contaminant and place of contamination) and traceability information printed on the labelling (time of packing and production batch). The human resource department, based on a suggestion from the distributor, SC5D, suggested cross-referencing it with the packer ID number provided by their department and enforced by the packing line supervisors. Hence, if the contamination occurred in the packing facility, it was possible to narrow down a potential investigation to a person or group of people in a packing line. This would in turn facilitate the distributor investigations in case of incidents [92]. The consultant therefore arranged and set up this practice as a standard for SC5E [93].

The prior notice/electronic manifest did not represent problems for the firm, since they had the competencies from the compliance manager in IT systems, who previously headed the IT department. The issue was a notifications design, development, and integration in the database that could contribute to reduce operations costs and time.

The Mexican customs brokers in 2005 (T) were still requiring faxes to transmit Bills of Lading to the US customs, but that was costing the firm too much money and time. The compliance manager developed the software for the customs broker that printed SC5E's email transmissions of Bills of Lading into their fax machine. Later the custom broker started using the email system to transfer the Bills of Lading [94].

There were other important meetings held between shipping departments, transport providers, the compliance manager and the consultant. The transport providers answered questionnaires that would allow the consultant to re-design the truck and trailer screening procedures, and seals monitoring forms [95].

Also based on those meetings, the compliance manager developed a software program that integrated the labelling data into the shipping documentation summary [96]. The software would convert those summaries into the prior notice and the electronic manifest, supposedly to be transmitted by the transport providers. However, since it was integrated with the Bill of Lading transmission system to the Mexican customs broker, the compliance manager offered the transport providers to realise the transmission for them. The electronic manifest and prior notice were going to be enforced by the end of 2006 (T). The transport providers welcomed this since they would outsource the operation to SC5E, even though they were still accountable for any mistake in the transmission [97]. Interestingly, SC1&5T did not agree on outsourcing the operation because they were already complying with it before SC5E developed the system.

In relation to the driving routes; the use of advance technologies was ruled out against traditional technologies to monitor conveyance security. During the meetings there was an assessment comparing the costs and functionality of GPS against the use of radio, mobiles and toll receipts (P.E). The transport providers chose to cross-reference information from the invoices of tolls on the Mexican highway, which included time and location, and the information provided by the truck driver including, location, time, whether they were in transit or at an inspection point [98] [99] [100].

Should drivers follow the designed routes and schedules, the toll receipts and information from the driver had to correspond with the plans, especially with tolls located, on average, 100km from each other. According to the discussions in the meetings, the GPS was not superior to the tolls, radio and mobile documentation/information systems. The fact that SC5E and its transport providers were monitoring the conveyance routes may have contributed to the prevention of drivers deviating from the plans [101].

Learning and knowledge sources

All in all, the firm required the use of specialised knowledge from its internal departments during discussions, which used to lead to a learning process in the implementation of the strategies from the meetings. The same strategy was applied in a vertical alignment fashion with the transport providers for trailer and conveyance security. Furthermore, the stakeholders' involvement was not only at the level of IT systems redesigns and integration but also at the level of planning and implementation processes led by the security consultant.

Figure 18: CTPAT related security resources[81]

Source: Provided by the SC5E compliance management.

[81] The pictures show: 1) the surveillance officer form the State Police Department, and two private security guards; 2) Alarm systems for the offices in the packaging facilities; 3) The monitors of the CCTV; 4) The electronic pointer downloading the surveillance routes followed by the guards in the facilities; 4) Sealed trailer; 5) Employees biometrics; 6) Vest with colour indicating the person was granted access in the loading area only (there are other colours for other areas); and 7) State Police Department and dog to detect drugs and other chemicals for trailer inspection.

Table 5.12.1: SC5E Capability building and resource development

Resource / Capability	R.BP	R.PhyS	R.A	R.Per	R.Pro	R.IT	R.CT	R.Co	R.TA	**Capab. count**	**Total capab.**
C.OC	87	88	89							**3**	**19**
C.MS			90	91						**2**	
C.IC					93					**1**	
C.SH			89	91	93		98	98	101	**5**	
C.SD					94					**1**	
C.VA					95;97	92	95;100	99	101	**7**	
Resources count	**1**	**1**	**2**	**1**	**4**	**1**	**3**	**2**	**1**		
Total resources	**16**										

Source: The author, based on interview with SC5E

5.13. Brief remarks on the case studies

From the previous case studies, one may note an increasing degree of complexity of the processes, capabilities and, perhaps not so clearly, of the diversity of the security resources deployed within the firms and across the supply chains. However, at this stage it is still not yet possible to make any conclusions due to the need to conduct the corresponding comparative case analysis, upon which this investigation should be based. Therefore, the next chapter compares each one of the variables described in previous cases, and later integrates these cross-case comparisons with the results of the assessment of the governance structures, which relied on questionnaires rather than interviews.

6. CHAPTER 6 Empirical results

The results follow a similar structure as the case study outline. In order, we will summarise the compliance process, the capabilities building process, and the governance structures. The later results from the questionnaires applied to the firms, rather than from the case studies description.

In each of the sections there will be a summary of results, followed by the qualitative comparative analysis (mvQCA), a brief interpretation of the results of the mvQCA, and concluding remarks in relation to the results.

6.1. Regulatory compliance process

6.1.1. Summary of compliance processes

Identification of the regulation

The firms' awareness of CTPAT relied heavily upon the resources and personnel available outside their organisations. Despite the lack of internal resources and great internal complexities, the attention of firms to CTPAT regulation relied upon nine different sources. As expected, the CTPAT agency (officials) was the most active in gaining the attentions of the firms. However, other CBP personnel and departments, industry networks and industry associations also played important roles in introducing the regulation. As expected, the supply chain parties with the most sources of regulatory awareness were the distributors (see Table 6.1.1.1, p.196).

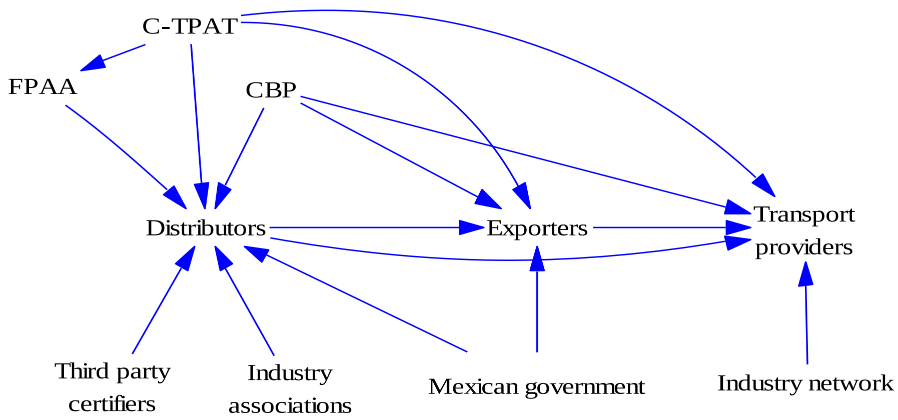
Table 6.1.1.1. Sources of regulatory information

	Receptors			
Sources of information	Distributor	Exporter	Transport	Grand Total
CTPAT	5	3	3	11
Distributor (D)		3	3	6
CBP	2	2	1	5
FPAA	3			3
Third party certifiers (TPC)	2			2
Mexican government (Mex)	1	1		2
Exporter (Exp)			1	1
Industry association (IA)	1			1
Industry network (IN)			1	1

Although the initial regulatory diffusion may have been formal and direct from CTPAT officials to the firms, or indirect throughout the FPAA, the international supply chains served as conduits of regulatory awareness. Figure 19 (p.197) shows how awareness followed upstream information flows (from distributors to exporters to transport providers) but never downstream (from transport providers to exporters to distributors) along the supply chain.

There were three sources of regulatory awareness: 1) the US government (CTPAT and other CBP departments); 2) the international supply chain; and 3) stakeholders. The information flows related to regulatory awareness reduced formality as it passed from distributors to exporters and to transport providers. The distributors have been informed via two governments (the US and Mexico) and their industry associations, the exporter from both governments, while the transport providers had been informed only through the US government and informal networks. Furthermore, the pattern of regulatory awareness is not only due to the fact that information sources vary in formality, it is also a matter of receptive capacity. Distributors and exporters have departments in charge of regulatory issues such as safety and quality assurance, while the transport providers did not report departments exclusively dedicated to respond to regulatory compliance (see Figure 19, p.197).

Figure 19: Regulatory awareness diffusion



Interpretation, assessment and compliance method

Regulatory Interpretation and perception of change required for compliance

Once firms were aware of CTPAT, their CEOs appear to have undertaken a general assessments of the regulation based on the interplay between two important factors: 1) possible benefits offered by the regulation to the firm, and 2) whether the regulation would be easy or difficult to implement, which was evaluated relative to the capacity of the firm to implement the security guidelines where required.

The first factor resulted in firms with two different views: the first of these reflected in the views of SC2D, SC3D, SC3E, SC4D, SC4E&T, SC5D and SC5E was that there was a positive relationship between regulatory compliance, safer cargo, CBP trust in the firm, and a reduced number of inspections; while the other view, represented by firms SC1D and SC3T did not see that relationship so clearly.

Additionally, within the first group there were claims of two main incentives for early compliance. Firstly, firms would enjoy the regulatory benefits for a longer period while the rest of the industry was not compliant; this benefit is not only relative but also absolute, and tends to disappear to an extent when the rest of the firms reach compliance[82] (SC5D). Secondly, under the scenario of another terrorist attack, the US would temporarily suspend trade with non-compliant firms; hence, the earlier the firm becomes compliant, the sooner it will stop running this risk (SC5E). The second group on the other hand considered that compliance would be too costly (SC3T), or would not contribute enough towards protecting the product, client and service as a whole (SC1D); nonetheless these firms decided to develop security resources based on self-regulation.

In relation to the second factor, there were positive and negative views on whether firms would be able to implement the guidelines where security changes were required. On the positive side, even though most of the security criteria needed to be developed, it was argued that personnel had sufficient experience with security practices, helping the firm to deal with the required changes (SC1&5T). Also, having a high security profile but with not many changes required, it was thought that safety and security were interrelated, and that compliance with the safety or security-related self-regulations contributed to compliance with CTPAT (SC1E). Lastly, although all security criteria needed to be implemented, it was preferred as a measure to avoid reputational damage and focus on normal business operations, rather than building up capabilities and developing resources to rebuild the trust from CBP in case of incidents. Building up a reputation for CBP is considered more cumbersome than compliance with CTPAT (SC4D).

There were also negative views on the possibility of implementing security guidelines. For instance, a firm that was required to change all its security practices prioritised the compliance of safety over security, since the former may contribute to the latter, while the opposite may not be the case; furthermore, security implementations may not contribute to reaching the regulatory aim anyway, since there were Mexican inspection points breaking the security seals in the highway, which weakened security practices along the whole supply chain (SC2E&T). Additionally, although firms had a partial development of the security

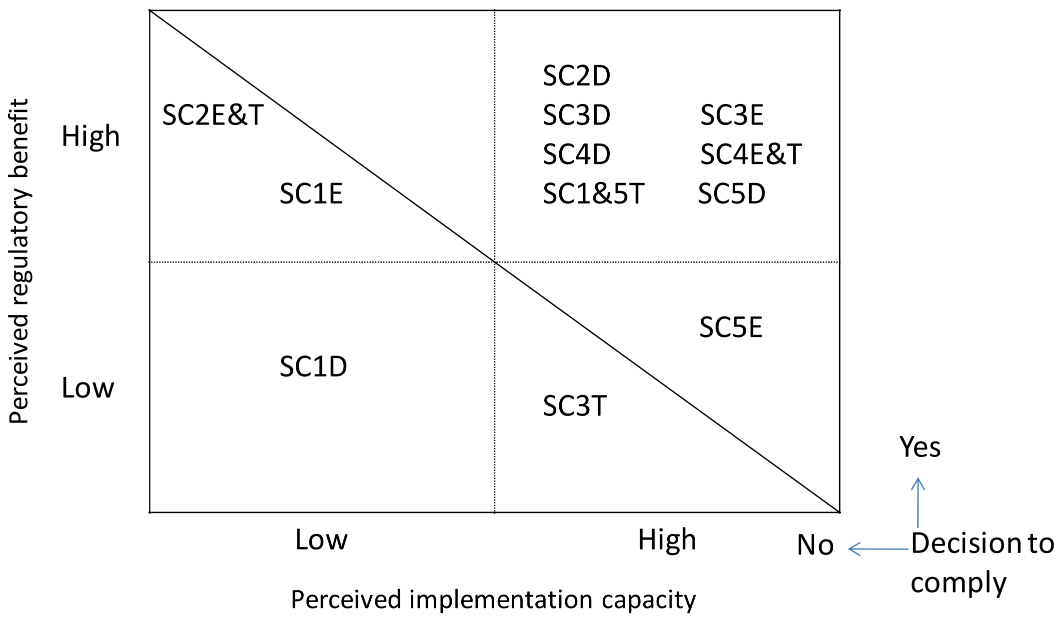
[82] The number of fresh produce chains using FAST lanes was almost inexistent. Should the whole industry become compliant, more than 100 thousand trucks would use the FAST lane (CAADES/CIDH, 2007), adding pressure to the infrastructure and slowing it down.

criteria, they argued that they were only able to manage their own processes; they could not monitor the transport providers (SC1D), and even less the whole supply chain (SC1E).

It is therefore the interplay between regulatory benefits and implementation capacity that informs the firms' interpretation of the regulation and contributes to the decision making processes leading to compliance.

Firms which identified regulatory benefits and implementation capacity positively decided to comply, whereas a lack of regulatory benefits and a lack of implementation capacity drove firms towards not pursuing compliance. The decision to comply required the regulatory benefits to outweigh the lack of implementation capacity, or the implementation capacity to outweigh the lack of regulatory benefits.

Figure 20: Compliance decision making[83]



[83] SC5E based its decision meking only on risk reduction, rather than on researching any of the direct regulatory benefits, such us reduced inpections and/or the use of the FAST lanes.

Compliance and regulatory regimes

Although firms may have decided not to comply with CTPAT, they did try to conform at least partially to the CTPAT security guidelines. Since compliance relates to the adherence of a firm to a regulation, and conformance relates to the actual implementation and processes that meet the regulatory guidelines and standards (Gilliland & Manning, 2002, p. 322; Scharfeld, 2003, p. 11; R. Wilson, 1997, p. 48), it was useful to avoid mixing compliance and conformance[84]. Firms not looking for adherence to CTPAT (not wanting to apply for a CTPAT membership) were classified as low compliant, while those without actual development of security resources according to the CTPAT criteria were classified as low conformant (having less CTPAT security criteria covered). This means that while firms may not be compliant (not searching for certification in CTPAT) they may still conform to the CTPAT security criteria (developed security resources) by showing more counts in each criterion, as well as in more CTPAT criteria.

For instance, in spite of 4 out of 13 firms deciding not to become compliant, all firms were at least partially and increasingly conforming. However, one firm (SC1E) decided not to conform to any more security criteria, while another was delaying the compliance and conformance processes (SC2E&T).

Firms built up compliance and conformance to CTPAT security regulations based on three regimes: firstly, to CTPAT guidelines; secondly to self-regulated security measures; and thirdly to food safety standards. After starting their compliance or conformance processes, one group of firms redefined their previous self-regulatory criteria to prioritise CTPAT guidelines (SC1&5T, SC5D, SC5E), and another group redirected efforts from food safety regulations to CTPAT criteria (SC2E&T, SC3E, SC5D, SC5E). This however was not to substitute former regulations, but to run them jointly.

Due to the drug incidents reported in four cases (SC3D, SC4D, SC4E&T), firms reapplied to gain certification. They then had to keep implementing and developing security resources in a self-regulating fashion.

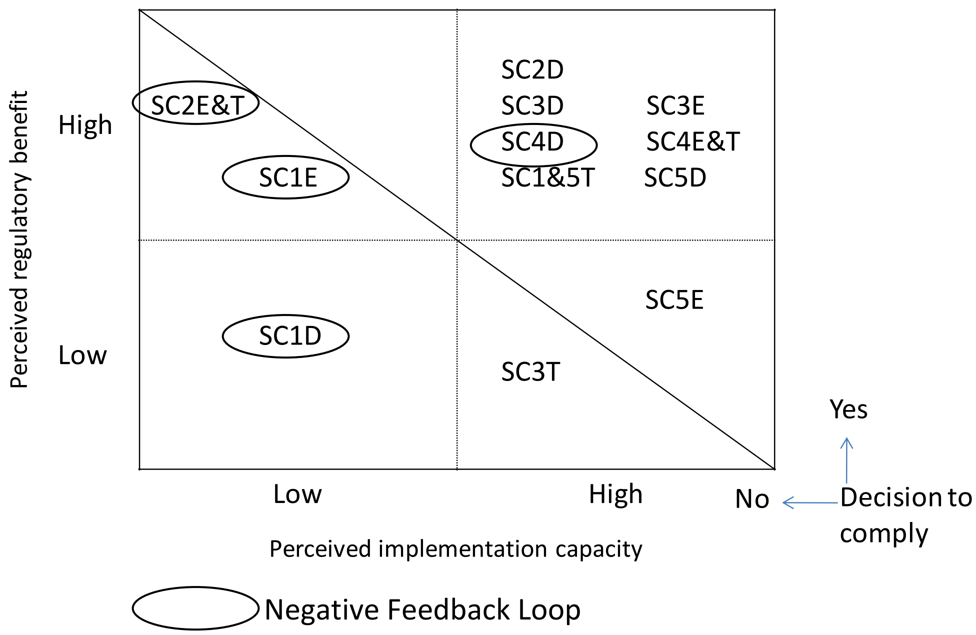
[84] Measured by the type of security resources that firms were missing during their first general evaluation of their implementation capacity, leading to their decision of whether to comply or not. The measures for this construct are low, middle and high, which were assigned according to the initial regulatory assessments by the CEOs and compliance managers according to how far the firm was from having the necessary CTPAT security resources.

The compliance methods varied across firms. Those aiming to become compliant prioritised security development based upon CTPAT guidelines, while firms not seeking compliance directed their efforts towards self-regulation and partially conforming to CTPAT. Also, without a clear pattern, but with more relevance to distributors and exporters, food safety implementations were applied to build up capabilities and security resources.

This decision however, locked firms such as SC1E, SC1D, SC2E&T and SC4D into negative feedback loops because even though existed between previous compliance methods and the decision regarding whether or not to comply with CTPAT. It was described in the previous section that either high regulatory benefit or implementation capacity was required in order for firms to pursue compliance. Interestingly, where self-regulation and food safety regulation implementation processes were considered in the decision making process, firms decided not to comply.

In terms of regulatory benefits and implementation capacity, self-regulations and food safety regulations have been perceived as more beneficial and easier to implement (SC2E&T, SC1E, and SC1D). The exception that proves the rule was found in firm SC4D, where the perception of regulatory benefits was reinforced upon rejection of their certification, driving the firm to intensify their security resource development in a self-regulated fashion, later re-applying to CTPAT. According to the CEOs, the self-regulation was undertaken to mitigate the reputational damage they suffered. In general, when the compliance methods were perceived as better in terms of regulatory benefits or implementation than the CTPAT regulation, firms decided not to comply, whereas if the compliance method contributed to absorb CTPAT regulatory benefits, the firm decided to comply.

Figure 21: Negative feedback loops in the compliance decision-making



Communication, implementation and evaluation

The communication systems in firms were interrelated with the implementation process and the assessment of the regulatory aims. Firms mainly used seven different communication systems, and the ones pursuing compliance with CTPAT had more diverse communication systems that those not pursuing compliance. Furthermore, there was a clear history of using formal meetings to communicate firms' security policies and strategies within firms, except for SC1&5T and SC5D (Table 6.1.1.2, p.203).

Table 6.1.1.2: Regulatory regimes and communication systems

Regulatory regimes			Firm	Formal meetings	Face to face	Banners	Vertical	IT systems	Training sessions	Horizontal
Self-regulation	CTPAT	Food Safety								
X		X	SC1D						X	
X		X	SC1E		X	X	X			
		X	SC2E&T		X					
X			SC3T		X					
X	X		SC1&5T		X					
	X		SC2D	X		X			X	
	X		SC3D	X	X	X		X		
	X	X	SC3E	X			X	X		
	X		SC4D	X					X	
	X		SC4E	X			X			
	X		SC4T	X			X			
X	X	X	SC5D	X		X				X
X	X	X	SC5E	X		X		X		

After the CEOs established communication systems to inform their companies about the need to initiate the compliance and/or conformance processes, firms built up capabilities (organisational competencies, managerial systems, internal coordination across departments, contribution of stakeholders to the implementation process, development of the suppliers' capabilities and resources development as a product of the implementation in the firm, and vertical alignment of capabilities with the capability development of its client or supplier) to be used to develop or acquire the security resources (business partner, physical, access, personnel, procedural, IT, conveyance, trailer, and awareness).

Firms may have been partially conforming (pre-conformance) to specific CTPAT guidelines. The fact that firms had other compliance regimes (self-regulation or food safety) did not seem to contribute to their pre-conformance or conformance, as shown in Table 6.1.1.3, p.204.

Table 6.1.1.3: Regulatory regimes, conformance, and implementation strategies

Regulatory regimes			Firm	Pre-conformance	Resource avoiding	Dominant Implementation Strategy	Post-conformance	Change in conformance*
Self-regulation	CTPAT	Food Safety						
		X	SC2E&T	Low	X	Additive	Low	0
	X		SC4D	Low		Additive	High	2
	X		SC4E	Low	X	Merger	High	2
	X		SC4T	Low	X	Merger	High	2
	X		SC2D	Middle		Additive	High	1
	X		SC3D	Middle		Merger	High	1
X			SC3T	High	X	Merger	High	0
X		X	SC1D	Low	X	Additive	Middle	1
X	X		SC1&5T	Low		Additive	Low	0
	X	X	SC3E	Low		Additive	High	2
X		X	SC1E	Middle	X	Additive	High	1
X	X	X	SC5D	Low		Merger	High	2
X	X	X	SC5E	Low	X	Merger	High	2

* Represents the number of levels in conformance that firms progressed (e.g. from low to middle=1; from low to high=2)

The challenge for firms was to prevent interferences with their normal business activities or with other compliance activities. As shown above (Table 6.1.1.3, p.204) some firms also tried to avoid the introduction of time consuming or cumbersome routines. This was reflected in avoiding or delaying prescriptive security activities that represented higher costs or duplicated security functions such as background checks (SC1E, SC3T, SC4E&T and SC5E), CCTV (SC2E&T) and GPS (SC5E).

The firms deployed two basic strategies to develop security resources. Their organisational capabilities would seek to either add new resources, or to merge them with the existing business operations.

The 'adding' strategy (SC2D, SC3D, SC4D, SC4E&T, SC5D and SC5E) was preferred when the security resources would not interfere with business operations (e.g. surveillance by guards and CCTV monitoring). This facilitated the upgrading of firms' conformance levels over time.

The 'merging' strategy was used to create security functions that individual resources would not be able to perform. Examples of this include combination of expertise of packing complexities and surveillance by SC4E&T, avoiding the use of GPS and merging a series of resources to create a comprehensive traceability and monitoring system by SC5E, and the experimental re-designs to reduce times and movements, and increase monitoring capacity by SC3D[85].

When new security functions were required, but the resources were not able to deliver them, resources were merged. Such resources may have been already available or purposely created. The development, addition and merger of resources that conform to the regulatory guidelines went through trial and error processes (SC3D, SC3E, SC3T, SC4D, SC4E&T, SC5D), design-implement processes (SC1D, SC1E, SC1&5T, SC2D, SC2E&T, SC4D, SC5D, SC5E), the outsourcing of resources management processes to external organisations (SC1E, SC2E&T, SC4E&T, SC5E), or combinations of all of these.

The previous resources development strategies and processes (Table 6.1.1.3) suggest that, rather than showing a pattern towards high conformance, various pathways exist, regardless of their pre-conformance (e.g. SC4T vs SC3T) or the regulatory regimes (e.g. SC1E vs SC4E) they conform with, or their supply chain stage (e.g. SC1E, SC3T, and SC4D). In other words, high conformance does not depend on pre-conformance, regulatory regime, or supply chain stage (Exporter, Transporter, or Importer).

Therefore it is crucial to closely evaluate the development of such resources by both the internal and external human resources of the firm. Data shows for low conformance firms (SC1&5T and SC2E&T) the main evaluator of security resources were CTPAT officials, and secondly, CEOs, supply chain partners, and the firm's personnel. On the other hand, for high conformance firms the main evaluators were the compliance managers followed by their supply chain partners (Table 6.1.1.4, p.206); which suggests a need for dedicated managers for compliance and supply chain engagement for higher conformance to CTPAT guidelines.

The feedbacks of the evaluation stage modified various elements of the compliance processes. Firstly, they changed the perception of the CBP from that of being a partner to being a command control regulator (SC3D). Secondly, they influenced firms' decisions to avoid or delay compliance (SC1D and SC2E&T), as well as boosting confidence about

[85] Similarly, Sproull (1981) discussed the idea that new programs compete against dominant programs for management support, attention, and skilled participants (Sproull, 1981, p. 452).

their capacity to develop the required security resources needed to comply (SC1&5T, SC3D and SC5E). Thirdly, in the implementation processes they contributed to the better coordination of tasks (SC1E and SC5E), the redesign of security resources (SC2D, SC2E&T, SC3E, SC3T, SC4D, SC4E&T and SC5E), and to the monitoring of the performance of the security resources on a real time basis (SC3T, SC4E&T and SC5E).

Table 6.1.1.4: Participation in the evaluation of the development of security resources

		Participants							
Conformance	Firm	CEOs	Compliance managers	Personnel	SC Partners	Food safety certifiers	CTPAT	Enforcement CBP	Consultants
Low	SC1&5T	X		X			X		
Low	SC2E&T				X		X		
Middle	SC1D	X							
High	SC1E	X	X			X			
High	SC2D		X				X		
High	SC3D		X				X	X	
High	SC3T	X			X				
High	SC3E		X		X				
High	SC4D	X	X		X		X	X	X
High	SC4E&T		X		X			X	
High	SC5D		X		X		X		
High	SC5E		X		X		X		X

Conformance speed and intensity

The initial dates of development of resources for conformance to CTPAT regulations show no clear patterns across firms, and neither does the intensity of resources development (Table 6.1.1.5, p.208). Although some early-movers have high on-time conformity levels, newcomers have also managed to conform to a great degree. This applies equally across firms starting implementations that conform to CTPAT since 1998 as well as for those who started since 2005.

Table 6.1.1.5: Speed and intensity of the conformance process

Firm	Pre-conformance	Initial date	Time block = 2 (Early Movers)												Time Block =1 (On-time movers)						Time Block = 0 (Newcomers)					Conformance
			Jul-97	Jan-98	Jul-98	Jan-99	Jul-99	Jan-00	Jul-00	Jan-01	Jul-01	Jan-02	Jul-02	Jan-03	Jul-03	Dec-03	Jan-04	Jul-04	Jan-05	Jul-05	Dec-05	Jul-06	Jan-07	Jul-07	Jan-08	
SC2E&T	Low	Aug-07																						-	-	Low
SC1&5T	Low	Jan-07																					-	-	-	Low
SC1D	Low	Aug-05																		-	-	-	-	-	-	Middle
SC1E	Middle	Aug-98			-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	High
SC2D	Middle	Jan-03												-	-	C	-	-	-	-	-	-	-	-	-	High
SC3D	Middle	Jan-05																	-	-	-	-	-	-	-	High
SC3T	High	Dec-03												-	-	-	-	-	-	-	-	-	-	-	-	High
SC3E	Low	Oct-05																		-	-	-	-	-	-	High
SC4D	Low	Dec-05																			-	-	-	-	-	High
SC4E&T	Low	Dec-05																			-	-	-	-	-	High
SC5D	Low	Aug-97	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	High
SC5E	Low	Aug-03													-	-	-	-	-	-	-	C	-	-	-	High

– – – Period implementing measures for conformance

C Certification granted

Summary of the conformance processes

The description of the compliance processes suggests that there is no such thing as 'a compliance model'. The 14 firms, clustered in 12 cases, show rather complex iterative compliance processes, and although some of the overlapping stages are presented independently, this is purely for analytical purposes[86]. Yet there are still compliance patterns departing from the pathways towards compliance with CTPAT (Table 6.1.1.6, p.211).

The summary (Table 6.1.1.6) of pathways available for firms to follow includes two exemplar firms (low and high compliant), with their real compliance processes.

The conformance process of the low compliant firm (SC3T): 1) starts by gathering information from exporter and the distributor, 2) the CEO decides not to comply, 3) they decide to self-regulate, 4) the company uses face to face communication systems for informing about internal security compliance processes and guidelines, 5) the company avoids specifically prescribed security technologies and/or systems, and prefers trial and error processes and combining previous experiences with new security procedures, 6) the security procedures are evaluated by the firm's CEO and their supply chain partners, finally 7) since the company did not apply to CTPAT/FAST, from the regulators' view point they are low compliant (See the full compliance process in page 155).

The conformance process of the high compliant firm (SC5E): 1) starts by gathering regulatory information from the Customs Border Protection, 2) the CEO believes that there are regulatory benefits from compliance, and also believes to have the capacity to implement the changes required by the regulation, 3) they engage with the conforming (implementing) and compliance (filling the application for certification) processes, 4) the company pull self-regulated measures, food safety measures adopted for security purposes, and the CTPAT security guidelines, 4) the company displays banners with security compliance related information, calls for regular formal meetings, and adapts its information technology systems for security, 5) the company decides to avoid some prescriptive security technologies, design and merge security processes with pre-existing ones, or with merges outsourced security processes with the internal security operations, 6) the evaluation of the security compliance processes are performed by compliance

[86] It is important to note that the methodology did not capture the cut points between stages; therefore it was not possible to determine the temporal dimension by stages, only of the overall compliance capability building processes.

managers, supply chain partners, CTPAT officials, and the CBP; 7) the firm filled the application for certification and implemented the security measures in ways that to the regulators granted the certification (See the full compliance process in page 184).

The SC3T and SC5E followed a variety of compliance processes, but none of them used the Fresh Produce Association of the Americas (FPAA), CTPAT, Third Party Certifiers (TPC), Mexican government (MEX), Industry Associations (IN), or Industry Networks (IN) for gathering regulatory information. Also, in the communication systems, they did not use training sessions, and these two companies did not just create resources and added them up to the existing ones, but they merged new security functions in pre-existing procedures. For evaluating the compliance process, the two firms did not reply on consultants, or TPC, nor their own personnel.

It is clear that, compliant or not, firms converge in some stages of the compliance process (e.g. in their perception of their implementation capacity, or by using an implementation strategy of avoiding specific security resources), while in other stages they diverge (e.g. in sources of regulatory identification, or in communication systems). These diverging and converging paths complicate the identification of the underlying patterns leading towards compliance.

It is therefore important to find reliable ways of identifying patterns out of a combinatorial diversity (complexity) generated even with a limited number of cases and observations. The Multi-Value Qualitative Comparative Analysis (mvQCA), as explained in the research process, is used to support that analysis.

This methodology (mvQCA)[87] and the software to run the analyses (TOAMANA) were introduced by Cronqvist (Cronqvist, 2005; Ragin, 1989, 2000), and is a variation of the Fuzzy and Crisp Set Qualitative Comparative Analysis (fsQCA and csQCA) described in chapter 3, p.81.

[87] As a reminder, this method is used not to discover what produces an effect, but to identify what co-varies with it.

Table 6.1.1.6: Summary of the conformance processes (Selected firms: SC3T and SC5E)

Stages	SC3T=▼ ●=SC5E								
1. Regulatory awareness	FPAA	CTPAT	D ▼	Exp ▼	CBP ●	TPC	Mex	IA	IN
2. Regulatory interpretation and change required	Regulatory Benefit ●	No Regulatory Benefit ▼	Implementation Capacity ●▼	No Implementation Capacity					
3. Compliance decision	Compliance ●	Conformance Increase ●	Delayed or not participating ▼						
4. Compliance method	Self-regulation ●▼	CTPAT ●	Food Safety Regulations ●						
5. Communication	Face to face ▼	Formal meetings ●	ITS ●	Banners ●	Training sessions	Others			
6. Implementation	Avoiding ▼●	Adding	Merging ▼●	Trial and Error ▼	Design-Implement ●	Outsource ●			
7. Evaluation	CEO ▼	CM ●	SC ●▼	CTPAT ●	CBP ●	Consultant	TPC	Personnel	
Outcome: Compliance	**Low** ▼	Medium	**High** ●						

6.1.2. mvQCA of the regulatory compliance process

mvQCA: model specifications

To proceed with our analysis of the regulatory compliance process and determinants of compliance, it is necessary to specify a model. The outcome in this investigation is, in most cases, compliance. Compliance has three levels (low, middle and high); thus thresholds were set to differentiate the conditions of low compliance, which takes value 0, against those conditions of middle or high compliance, which take value 1. Hence, firms are grouped into two sets: low compliance (value 0) groups, and the remaining (value 1) groups.

The model for the identification of causal conditions of the process to achieve compliance needs to go through seven stages, corresponding to the number of stages in the compliance processes. For each stage the outcome (dependent variable) is compliance=1 (middle-high) and the causal conditions (independent variables) are the components of each stage of the regulatory process. Thus, the model for middle-high compliance is a function of the compliance processes causal conditions.

Model: *Middle-High compliance = f (seven stages causal conditions)*

Stage 1: Minimise (identify) the configurations of '**regulatory awareness**' or regulatory information providers (CTPAT, Distributor, CBP, FPAA, TPC, Mex, Exp, IA and IN) causing (co-varies with) middle-high compliance levels (M-H Compliance). (See Table 6.1.1.1, p.196 and Table 6.1.2.1, p.215)

Stage 2: Minimise the configurations of '**regulatory interpretation and change required**' (Perception of Regulatory Benefit and Perception of Implementation Capacity of the Firm) causing M-H Compliance. (See Figure 20, p. 199 and Table 6.1.2.1, p.215)

Stage 3: Minimise the configurations of '**compliance decision**' (Compliance, Conformance Increase, Time Block) causing M-H Compliance. (See Table 6.1.1.5, p.208 and Table 6.1.2.1, p.215)

Stage 4: Minimise (identify) the configurations of '**compliance methods**' (CTPAT, Self-regulation, Food Safety) causing M-H Compliance. (See Table 6.1.1.3, p.204 and Table 6.1.2.1, p.215)

Stage 5: Minimise the configurations of '**communication methods**' (Formal Meetings, Face to Face, Banners, Vertical/Hierarchical, IT systems, Training Sessions, Horizontal) causing M-H Compliance. (See Table 6.1.1.2, p.203 and Table 6.1.2.1, p.215)

Stage 6: Minimise the configurations of 'implementation strategies and processes' (Avoiding Specific Resources, Implementation Strategy-add Routines vs. Merge Routines, Trial and Error, Design and Implement, and Outsource the Development of Resources) causing M-H Compliance (See Table 6.1.1.3, p.204 and Table 6.1.2.1, p.215)

Stage 7: Minimise the configurations of 'evaluating actors' (CEOs, Compliance Managers, Personnel, SC Partners, Food Safety Certifiers, CTPAT, Enforcement CBP, Consultants) causing M-H Compliance (See Table 6.1.1.4, p.206 and Table 6.1.2.1, p.215)

mvQCA: the compliance process

The model tries to find the most parsimonious causal configurations of compliance for each stage of the regulatory process. The analyses, however, yielded some contradictory results: configurations of causal conditions related to compliance in some firms, and to non-compliance in other firms. In this case, the model was run again to identify the causal conditions of the contradictions. These results are reported in the right-hand side of the summary of results.

Although the model identifies the causal conditions of compliance, contradictions suggest that interpretations of the model should be made with care. That is, some causal conditions may lead towards compliance; however, if such a causal condition is combined with another, this may lead to non-compliance[88]. On the other hand, in some instances a cause can only produce compliance if another cause is not present.

The following section, mvQCA: Evaluation and interpretation of the model results, explores in detail each one of the seven stages of the compliance processes displayed in Table 6.1.2.1, p.215.

[88] Identifying contradictions is an additional advantage of using QCA methods, one that is hardly picked up on by traditional case analyses, especially when there are multiple explanatory variables involved. This is the value of using a formal method for the analysis of causal configurations.

Table 6.1.2.1: Causal configurations of regulatory process for Middle-High Compliance *

Stages	**Causal configurations**			**Contradictions****
1. Regulatory awareness	CBP$_s$ *SC15T, SC3D, SC5D*	FPAA$_s$ *SC2D, SC4D, SC3D*	[ia*(CTPAT+distributor+exp)]$_s$ *SC15T, SC2D, SC4D, SC3D, SC5D*	[tpc*exp]+[exp*ia] *SC1E, SC5E, SC2ET, SC3E, SC4ET*
2. Regulatory interpretation and change required	IMPLEMCAPACITY$_s$ *SC15T, SC2D, SC3D, SC3E, SC4D, SC4ET, SC5D*			regbenefit*IMPLEMCAPACITY *SC3T, SC5E*
3. Compliance decision	COMPLIANCE$_{ns}$ *SC15T, SC2D, SC3D, SC3E, SC5E, SC4D, SC4ET, SC5D*			
4. Compliance method	CTPAT$_{ns}$ *SC15T, SC2D, SC3D, SC4ET, SC3E, SC4D, SC5D, SC5E*			
5. Communication	FORMAL MEETINGS$_s$ *SC2D, SC3D, SC3E, SC4D, SC4ET, SC5D, SC5E*			[FACE2FACE * banners] *SC15T, SC2ET, SC3T*
6. Implementation	[OUTSOURCE*IMPSTRATEGY]$_s$ *SC4ET, SC5E*	resourceavoid$_s$ *SC15T, SC2D, SC3D, SC3E, SC4D, SC5D*		
7. Evaluation	PERSONNEL$_s$ *SC15T*	[COMPLIANCEMANAGER*fsc]$_s$ *SC2D, SC3D, SC3E, SC4D, SC4ET, SC5D, SC5E*		

*The model was run with Tosmana 1.301 (Cronqvist, 2009) to Minimise (find most parsimonious causal configurations)=1 (Middle-High Compliance), Including=C(Contradictions)+R(Reminders). ** Minimising=C, Including=R+1(Middle-High Compliance).(See Appendix D for a guide to read TOSMANA reports, p.322).

1. Regulatory awareness: for definitions see Table 6.1.1.1, p.196.
2. IMPLEMCAPACITY= Capable to implement security resources; REGBENEFIT=Regulation is beneficial.
3. COMPLIANCE=Decision to comply.
4. Compliance method: CTPAT=Complying with CTPAT (see Table 6.1.1.2, p. 203).
5. FORMAL MEETINGS=Using formal meetings as communication systems; FACE2FACE=Using face to face as communication systems.
6. OUTSOURCE=Outsourcing the development of security resources. IMPSTRATEGY=Merging resources or routines with existing business operations. Impstrategy=Adding resources or routines to existing business operations. RESOURCEAVOID=Avoiding specific security resources.
7. PERSONNEL= Security resources evaluated by firm's personnel. COMPLIANCEMANAGER=Security resources evaluated by the compliance managers; FSC=Security resources evaluated by food safety certifiers.

CAPITAL LETTERS INDICATE THE PRESENCE OF THE CAUSAL CONDITION, while lowercases indicate the absence of the causal condition (except for impstrategy, which indicates adding routines).

s=Sufficient condition; n=Necessary condition; ns=Necessary and sufficient condition; variables without subscripts imply that it is neither a necessary nor a sufficient condition.

mvQCA: Evaluation and interpretation of the model results

Stage 1: Regulatory awareness/identification

There are three configurations of regulatory information for 'middle-high compliance': 1) information from the Customs Border Protection (CBP); 2) information from the Fresh Produce Association of the Americas (FPAA); and 3) information from CTPAT, which is only useful if the industry associations are absent. Overall, regardless of the presence of other sources of regulatory information, it is sufficient to have CBP's or FPAA's regulatory information to attain firm compliance. The exception is when industry associations in concert with firms (distributors or exporters) try to pull the regulatory information together for other firms. In that case we would not have compliance (See Figure 22, p.217). A possible explanation is the fact that regulatory information should be tailored to the type of firm, e.g. for an exporter or for a distributor, hence, regulatory information provided from a distributor to an exporter may not be fit the type of firm. Industry associations may too be collecting only very generic information, not tailoring the regulatory information enough to fit the firm's compliance needs.

In relation to the CBP as a source of regulatory awareness and information, the influence it might wield on firms compliance may have come from the good impression it presents to their CEOs (SC1&5T), as well as its capacity to encourage them to get informed and participate in the CTPAT seminars (SC3D).

The FPAA was also an advocate of the need of CTPAT to reduce the risks of the supply chains of its members. The FPAA, in addition to providing information to its members, promoted the CTPAT seminars, which eventually catalysed firms' compliance (SC2D, SC4D).

Surprisingly, CTPAT itself as a source of regulatory awareness was important for compliance, as long as industry associations were not complementing it with regulatory information. This suggests that industry associations are not good sources of regulatory information.

Figure 22: mvQCA of regulatory awareness as causes of middle-high compliance

Tosmana Report
Algorithm: Graph-based Agent
Model settings:
Minimizing Value 1
including C R
Variable Settings:
Crisp Set (No Thresholds)

Truth Table:
v1: P.RI.CTPAT v2: P.RI.Distributor
v3: P.RI.CBP v4: P.RI.FPAA
v5: P.RI.TPC v6: P.RI.MEX
v7: P.RI.EXP v8: P.RI.IA
v9: P.RI.IN
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	v8	v9	O	id
1	0	1	0	0	0	0	0	1	1	SC15T
1	0	0	0	1	0	0	1	0	0	SC1D
0	0	1	0	0	0	0	0	0	C	SC1E,SC5E
1	0	0	1	0	0	0	0	0	1	SC2D,SC4D
1	1	0	0	0	0	0	0	0	C	SC2ET,SC3E,SC4ET
1	0	1	1	1	1	0	0	0	1	SC3D
0	1	0	0	0	0	1	0	0	0	SC3T
1	0	1	0	0	0	0	0	0	1	SC5D

Result: (all)
P.RI.CBP + P.RI.FPAA
(SC15T+SC3D+SC5D) (SC2D,SC4D+SC3D)
P.RI.CTPAT * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
p.ri.distributor * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
p.ri.exp * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
Created with Tosmana Version 1.301

Tosmana Report
Algorithm: Graph-based Agent
Model settings:
Minimizing Value C
including 1 R
Variable Settings:
Crisp Sets (No Thresholds)
Truth Table:
v1: P.RI.CTPAT v2: P.RI.Distributor
v3: P.RI.CBP v4: P.RI.FPAA
v5: P.RI.TPC v6: P.RI.MEX
v7: P.RI.EXP v8: P.RI.IA
v9: P.RI.IN
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	v8	v9	O	id
1	0	1	0	0	0	0	0	1	1	SC15T
1	0	0	0	1	0	0	1	0	0	SC1D
0	0	1	0	0	0	0	0	0	C	SC1E,SC5E
1	0	0	1	0	0	0	0	0	1	SC2D,SC4D
1	1	0	0	0	0	0	0	0	C	SC2ET,SC3E,SC4ET
1	0	1	1	1	1	0	0	0	1	SC3D
0	1	0	0	0	0	1	0	0	0	SC3T
1	0	1	0	0	0	0	0	0	1	SC5D

Result: (all)
p.ri.tpc * p.ri.exp
(SC1E,SC5E+SC2ET,SC3E,SC4ET)
p.ri.exp * p.ri.ia
(SC1E,SC5E+SC2ET,SC3E,SC4ET)
Created with Tosmana Version 1.301

For a reminder of how to read the report, see the Section 9.4 Appendix D: Guide to Read TOSMANA Reports, p.324)

Stage 2: Assessment of perceived regulatory benefit and implementation capacity

In order for compliance to be present it is necessary that firms perceive that they have implementation capacity; however, this is not in itself sufficient. If firms perceive that CTPAT does not provide regulatory benefits, compliance may not occur (SC3T). Yet SC5E became compliant even though it did not see direct benefits in CTPAT, only the potential of reducing the risks of being trapped behind the border, in cases of US border closures for security purposes.

Stage 3: Decision to comply and to conform as a determinant of compliance

In this stage, compliance was assessed against the improvements in the firm's conformance level, the length of their implementation, and their decision about whether or not to comply.

As expected, regardless of when the compliance process was initiated, it is sufficient that firms take the decision to comply, which implies that whilst early movers had sufficient time for their compliance processes, newcomers engaged in very intense conformance processes (Figure 23, p.219). But the necessary and sufficient condition is that of firms' making up their minds to comply, not just to conform, regardless of the intensity of the processes.

Stage 4: Regulatory Regimes for compliance

It was shown that various regulatory regimes are at play in developing security resources (See Table 6.1.1.3, p.204). Nevertheless, compliance terms are only relevant within the context of CTPAT. Self-regulation/food safety regulations used in combination with CTPAT do not contribute to compliance, contrary to what was expected by various firms (e.g. SC1E, SC2E&T, SC4D and SC5D). In this study, it is clear that security resources derived from regulatory regimes neither compete with nor support the development of security resources for CTPAT. In other words, CTPAT-related security resources seem to be valuable on their own, when they stand well away from other regulatory regimes.

Figure 23: Compliance decision and conformance decision as drivers of compliance

Tosmana Report
Algorithm: Graph-based Agent
Model Settings:
Minimizing Value 1
including C R
Variable Settings:
Name Thresholds
Months 26;55
Truth Table:
v1: ComDecision v2: ConformanceIncrease
v3: Months
O: compliance id: firm

v1	v2	v3	O	id
1	0	0	1	SC15T
0	1	1	0	SC1D
0	1	2	0	SC1E
1	1	2	1	SC2D
0	0	0	0	SC2ET
1	1	1	1	SC3D
1	2	1	1	SC3E,SC5E
0	0	2	0	SC3T
1	2	0	1	SC4D,SC4ET
1	2	2	1	SC5D

Result: (all)
ComDec{1}
(SC15T+SC2D+SC3D+SC3E,SC5E+SC4D,SC4ET+SC5D)
Created with Tosmana Version 1.301

Stage 5: Communication mechanisms for compliance

It was sufficient for middle-high compliant firms to have formal meetings to communicate all aspects related to compliance with CTPAT. However, there are also other communication systems relevant to compliant firms, i.e. face-to-face communication systems. However, this communication system is valuable only in the absence of banners in the firms. Banners may be used as a substitute for face-to-face systems to deliver information, yet will not carry enough of what is relevant to become a positive contributor for compliance on their own. The same may be said about face-to-face and hierarchical communications systems. The dangers of the last two systems are their contradictory results, as they are also associated with non-compliant firms (Figure 24, p.220).

Figure 24: Communication mechanisms for compliance

Tosmana Report
Algorithm: Graph-based Agent
Model Settings:
Minimizing Value 1
including C R
Variable Settings:
Crisp Sets (No Thresholds)
Truth Table:
v1: Meetings v2: Face2Face
v3: Banners v4: Hierarchical
v5: ITSys v6: Trainings
v7: Horizontal
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	O	id
0	1	0	0	0	0	0	C	SC15T,SC2ET,SC3T
0	0	0	0	0	1	0	0	SC1D
0	1	1	1	0	0	0	0	SC1E
1	0	1	0	0	1	0	1	SC2D
1	1	1	0	1	0	0	1	SC3D
1	0	0	1	1	0	0	1	SC3E
1	0	0	0	0	1	0	1	SC4D
1	0	0	1	0	0	0	1	SC4ET
1	0	1	1	0	0	1	1	SC5D
1	0	1	0	1	0	0	1	SC5E

Result: (all)
MEETINGS
(SC2D+SC3D+SC3E+SC4D+SC4ET+SC5D+SC5E)
Created with Tosmana Version 1.301

Tosmana Report
Algorithm: Graph-based Agent
File: D:\MYDOCU~1\PHDRES~1\METHOD~1\FIELDW~1\ANALYS~1\COMPLI~1\MVQCAC~1.TOS
Model Settings:
Minimizing Value C
including 1 R
Variable Settings:
Crisp Set (No Thresholds)
Truth Table:
v1: Meetings v2: Face2Face
v3: Banners v4: Hierarchical
v5: ITSys v6: Trainings
v7: Horizontal
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	O	id
0	1	0	0	0	0	0	C	SC15T,SC2ET,SC3T
0	0	0	0	0	1	0	0	SC1D
0	1	1	1	0	0	0	0	SC1E
1	0	1	0	0	1	0	1	SC2D
1	1	1	0	1	0	0	1	SC3D
1	0	0	1	1	0	0	1	SC3E
1	0	0	0	0	1	0	1	SC4D
1	0	0	1	0	0	0	1	SC4ET
1	0	1	1	0	0	1	1	SC5D
1	0	1	0	1	0	0	1	SC5E

Result: (all)
FACE2FACE * banners + FACE2FACE * hierarchical + banners * trainings + hierarchical * trainings

(SC15T, SC2ET, SC3T)
Created with Tosmana Version 1.301

Stage 6: Implementation Strategies

There are three causal conditions in two configurations related to the implementation strategies of the firm leading to compliance. The first configuration indicates that it is sufficient that a firm does not avoid the development of specific security resources to achieve compliance (SC15T, SC2D, SC3D, SC3E, SC4D and SC5D). The second configuration indicates that it is also sufficient that a firm outsources, at the same time that it merges, its security resources to existing business operations. It seems that the two firms with this causal configuration (SC4E&T and SC5E) needed the external expertise for the development of their internal security resources. Therefore they rely on external organisations' resources to merge internal resources to develop new security resources or routines. This has further implications in terms of the relationships and interactions required between the external organisation and the compliant firm. In other words, compliant firms may require that external organisations collaborate closely and embed their services or products (resources) within the firm.

The firms SC4E&T and SC5E have seen larger increases in their investments in security resources development, and (as will be shown in the following empirical section) have also seen important investments for capability building, in order for them to be able to align external and internal resources.

Stage 7: Regulatory evaluation

Figure 25, monitoring and evaluation for compliance, shows two configurations in the regulatory evaluation stage associated with compliance. Firstly, it was sufficient that the personnel were involved in the evaluation of the security resources to relate to compliance (SC1&5T), as they may be able to self-enforce the CTPAT regulatory measures, and they would have to be capable of applying corrective measures in real-time.

It was also sufficient that compliance managers evaluate the compliance process, so that firms could be associated with compliance; however it was necessary that food safety certifiers were not part of the security evaluation process. An interpretation may be that food safety certifiers, with respect to security matters, may not generate enough value to the firms in terms of compliance; they may undermine the ability of compliance managers to evaluate, monitor and apply corrective measures on a daily basis, which seems to be fundamental for any security programme.

It is important to bear in mind that food safety certifiers popped up in the case studies every once in a while. Although they are perceived as positive factor, our results show that in fact they are not, at least in terms of feedbacks for security purposes (Figure 25 below).

Figure 25: Monitoring and evaluation for compliance

Tosmana Report
Algorithm: Graph-based Agent
Model Settings:
Minimizing Value 1
including C R
Variable Settings:
Crisp Set (No Thresholds)
Truth Table:
v1: P.E.CEO v2: P.E.CO
v3: P.E.Per v4: P.E.SC
v5: P.E.FSC v6: P.E.CTPAT
v7: P.E.CBP v8: P.E.Consul
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	v8	O	id
1	0	1	0	0	1	0	0	1	SC15T
1	0	0	0	0	0	0	0	0	SC1D
1	1	0	0	1	0	0	0	0	SC1E
0	1	0	0	0	1	0	0	1	SC2D
0	0	0	1	0	1	0	0	0	SC2ET
0	1	0	0	0	1	1	0	1	SC3D
0	1	0	1	0	0	0	0	1	SC3E
1	0	0	1	0	0	0	0	0	SC3T
1	1	0	1	0	1	1	1	1	SC4D
0	1	0	1	0	0	1	0	1	SC4ET
0	1	0	1	0	1	0	0	1	SC5D
0	1	0	1	0	1	0	1	1	SC5E

Result: (all)
P.E.PER + P.E.CO * p.e.fsc
(SC15T) (SC2D+SC3D+SC3E+SC4D+SC4ET+SC5D+SC5E)
Created with Tosmana Version 1.301

mvQCA: compliance processes remarks

In summary, there are two relevant sources of regulatory information: Customs Border Protection (CBP), and the Fresh Produce Association of the Americas (FPAA). After firms take the decision to comply, and focus their security resources to meet the CTPAT guidelines, they may set up formal communications systems to pass on information about compliance plans and progresses. The implementation requires not avoiding specific security resources (e.g. CCTV, GPS), and finally engaging the compliance managers in the evaluations of the firm's compliance process to CTPAT.

The following sections expand upon the implementation stage of the regulatory process. The previous analyses focused on compliance strategies (avoiding, merging, adding, outsourcing, trial and error, design and implementation of security resources), whilst the following analyses stress the role of capabilities; specifically which capabilities were built, and how.

6.2. Capability building

Putting the implementation stage under the microscope helps to understand whether there is a relationship between the sophistication of the capabilities built by firms and their compliance level. The first part of this section describes and summarises the capabilities built at each compliance level. Later it presents the mvQCA for the identification of causal configurations, or the bundle of capabilities supporting the move of firms towards higher compliance. The third part presents my attempt to make sense of the results of the mvQCA.

6.2.1. Summary of capabilities building processes

Compliance levels

It was previously explained that conformance is the notion of developing resources to meet regulation, in this case CTPAT guidelines, whilst compliance refers to adherence to the CTPAT regulation. The three compliance levels are: 1) low, for firms which have not applied yet for a CTPAT membership, 2) middle, for firms that applied for a CTPAT membership (submitted application and confirmed of receipt by CTPAT department), but had not yet been verified in situ, and 3) high, for verified firms in situ (certified)[89]. The classification of firms by conformance and compliance levels shows no apparent patterns between them (Table 6.2.1.1, p.225).

[89] An accepted application suggests that a firm had supposedly developed security resources conforming to the CTPAT guidelines; however, at this stage the firm had still not been verified. Furthermore, in fact, their security resources may not be conforming to the guidelines, as with the cases SC1&5T and SC2E&T. Once the firm is verified in situ, it is given the certification in situ; or it can be given recommendations for upgrading their security resources, and a new schedule for in situ verification.

Table 6.2.1.1: Compliance and conformance levels

Compliance / Conform[90]	Low	Middle	High	Sample size (n)
Low	SC2E&T	SC1&5T		**2**
Middle	SC1D			**1**
High	SC1E, SC3T	SC3D, SC3E, SC4D, SC4E&T, SC5D	SC2D, SC5E	**9**
Sample size (n)	**4**	**6**	**2**	**12**

Although conformance is important, in this section the analysis moved from resources (related to conformance) to capability building. Thus the next section explores the types of capabilities used to develop the security resources, and classifies them according to their degree of sophistication.

Sophistication degrees of Capabilities

To develop security resources firms had to build up and exploit their capabilities. Although a capability cannot be seen or be measured in a straightforward way, there are indications of its presence and of where it was built (assembled).

A capability is present when a new function for a security is discovered in an existing resource, or when it is designed and developed in a new resource. The degrees of sophistication of the capabilities depend on the sources of learning and knowledge that combine to build up such capabilities.

---

[90] See Table 6.2.1.1, CTPAT Security Resources Development for the datasource of the classification in low, middle and high conformance. Although SC2E&T and SC1&5T have similar resources to SC1D, SC2E&T is an exporter and transport provider, and would therefore be expected to have more guidelines covered. SC1&5T on the other hand, although possessing similar resources, do not have them in their own facilities, and they have declared they have no special leasing arrangements regarding security installations in the facilities that will belong to the transport provider. Therefore when SC1&5T move to the new facilities, all security installations in the previous facilities will stay there, which means that SC1&5T are subject to developing and building all security measures in the new facilities. This is a weak aspect pointed out by the CTPAT inspectors.

As shown previously we have six sets of capabilities: 1) organisational competencies; 2) managerial systems; 3) internal coordination; 4) stakeholders'[91] support in the strategy and implementation stages; 5) supplier development; and 6) vertical alignment[92], according to how learning occurred and knowledge was sourced. The capabilities built with internal learning and knowledge are considered 'basic' in this investigation. The capabilities built with bilateral learning, knowledge interchange with stakeholders, unilateral learning, or knowledge transfer with supply chain partners, are considered 'intermediate'. Capabilities built with bilateral learning or knowledge exchange with supply chain partners are considered 'advanced'.

In the case studies we presented summaries (capabilities-resources matrix) of the type of capabilities built and the security resources developed (e.g. Table 5.2.1, p.120). The following table contains the count of capabilities built by firms rated by sophistication level (See Table 6.2.1.2, p.227).

The table shows the number of times that a given capability was built to develop a security resource. In general, the more sophisticated capabilities have the lower counts. Nevertheless, capabilities built with learning and knowledge transfers with stakeholders are frequent.

Although the analysis will focus on the capability building only, it is worth presenting the CTPAT security resources developed with those capabilities (See Table 6.2.1.3, p.228). The most frequent resource developed was procedural security, whilst the least frequent were information technology systems and the investigation of business partners. This does not mean these resources were not important, but during this period they were not being developed, whether they were needed or not.

In addition, the total count in capabilities is higher than the total count in resources. It was shown in the case summaries of capability-security matrixes that in some cases one single capability would be enough to develop more than one resource, whilst in other instances

[91] Stakeholders comprise: network of suppliers (excluding the supply chain partners) and external organisations not directly related to the firms' normal operations.

[92] Capabilities built in coordination with supply chain partners (exporter, transport provider and distributor). Capabilities built with other actors (network of suppliers or unrelated organisations) were classified in stakeholders' support or suppliers' development. For instance the GPS traceability system development by SC4E&T was classified as stakeholder support; as a result of adopting the software developed by a non supply chain partner, and adapting its setting for the needs of the firm.

more than one capability would be needed to develop a single capability. In general, these results suggest that developing single resources in our cases required, on average, more than a single capability.

Table 6.2.1.2: Summary of capabilities building

	Basic			Intermediate		Advanced		
Firm	Organisational Competencies	Managerial systems	Internal coordination	Stakeholders support	Supplier development	Vertical Alignment	**Total Count**	**Share**
SC1D	3	1		1			**5**	**3.9%**
SC1E	1	2	3	1			**7**	**5.5%**
SC1&5T	1	1	3	3			**8**	**6.3%**
SC2D	4	2	2	2	1	1	**12**	**9.4%**
SC2E&T	3	2		3			**8**	**6.3%**
SC3D	5	1	2		3		**11**	**8.6%**
SC3E	2		2	3	1		**8**	**6.3%**
SC3T	3	3	1	3		1	**11**	**8.6%**
SC4D	2	1	1	5	3		**12**	**9.4%**
SC4E&T	5	3	1	5		3	**17**	**13.3%**
SC5D	3	3	2	2			**10**	**7.8%**
SC5E	3	2	1	5	1	7	**19**	**14.8%**
Total	**35**	**21**	**18**	**33**	**9**	**12**	**128**	**100%**
Share	**27.3%**	**16.4%**	**14.1%**	**25.8%**	**7%**	**9.4%**	**100%**	
Average count	**2.9**	**1.9**	**1.8**	**3**	**1.8**	**3**		

Table 6.2.1.3: CTPAT Security Resources Development

Firm	Business Partner	Physical security	Access controls	Personnel security	Procedural security	Information technology	Container and Trailer	Conveyance	Awareness Training	Total Count	Share
SC5E	1	1	2	1	4	1	3	2	1	**16**	**14.41%**
SC5D		1	1	1	1	1	1			**6**	**5.41%**
SC4E&T		1	1	1	3	1	3	1	2	**13**	**11.71%**
SC4D		1	2		3		2	2	1	**11**	**9.91%**
SC3T		1	1	1	3		1	2		**9**	**8.11%**
SC3E	1	2	2		2		1			**8**	**7.21%**
SC3D	1	4	2		2		1			**10**	**9.01%**
SC2E&T	1		2		4		1			**8**	**7.21%**
SC2D	1	4	2	1	4					**12**	**10.81%**
SC1&5T		1	1		2			1	1	**6**	**5.41%**
SC1E		1	2		3		1			**7**	**6.31%**
SC1D		1			1		1	1	1	**5**	**4.50%**
Total	**5**	**18**	**18**	**5**	**32**	**3**	**15**	**9**	**6**	**111**	**100%**
Share	**4.5%**	**16.2%**	**16.2%**	**4.5%**	**28.8%**	**2.7%**	**13.5%**	**8.1%**	**5.4%**	**100%**	
Average count	**1.0**	**1.6**	**1.6**	**1.0**	**2.7**	**1.0**	**1.5**	**1.5**	**1.2**		

Compliance capabilities

Hypothesis 2a[93] states that higher levels of firm compliance correlate with higher degrees of capabilities sophistication. In the following paragraphs, we show how the basic capabilities, which are predominant in low compliant firms, were increasingly absent in middle and high compliant firms, whilst the sophisticated capabilities were less present in low compliant firms compared to high compliant firms. This trend is measured based on capabilities types count by compliance levels[94].

Table 6.2.1.4 (p.229) shows an increase of sophisticated capabilities according to higher compliance levels. Low compliant firms show a higher share of basic capabilities, 71%, compared to the total sample average, 57%. Middle compliant firms on the other hand, show a higher share of intermediate capabilities, 37%, compared to the total sample average, 32%. Finally, high compliant firms show higher share of advanced capabilities, 25%, than the total sample average, 9%.

Table 6.2.1.4: Compliance levels and capabilities sophistication

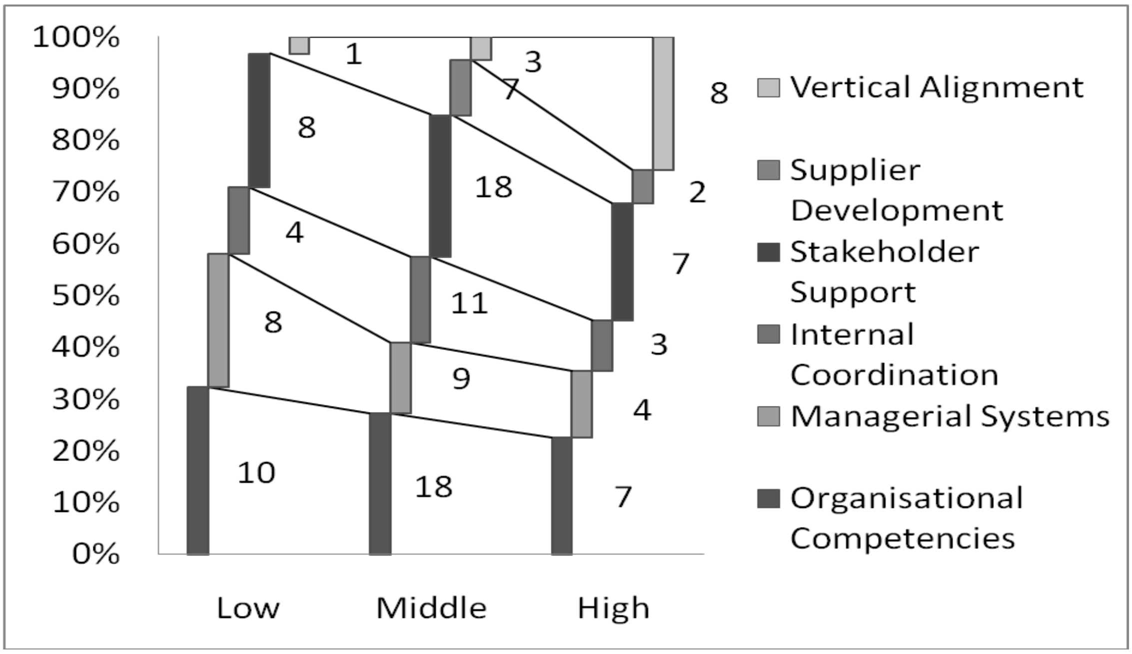
Compliance	**Capabilities** Basic	Intermediate	Advanced	Total	n
Low	22	8	1	31	4
Middle	38	25	3	66	6
High	14	9	8	31	2
Total	74	42	12	128	
Share of total capabilities by compliance level					
Low	71%	25%	3%	100%	4
Middle	57%	37%	4%	100%	6
High	45%	29%	25%	100%	2
Total	**57%**	**32%**	**9%**	**100%**	
Share of total capabilities by sophistication					
Low	29%	19%	8%	**24%**	4
Middle	51%	59%	25%	**51%**	6
High	18%	21%	66%	**24%**	2
Total	100%	100%	100%	**100%**	

[93] See section 3.2 Research questions and hypotheses testing roadmaps.

[94] Although the different capabilities require variegated degrees of knowledge, and each capability is built differently, we are not taking a value to represent them. At most, we are indicating how many capabilities the firms built. This is like the traditional patent counts, in which each patent represents completely different technologies, sectors, knowledge, value, time to register it, and so on, yet the purpose is just to say that it exists at a given time in a given context.

Error! Not a valid bookmark self-reference. (p.230), presents the specific capabilities that firms built according by compliance level. In general, it shows that basic capabilities building lowers at higher compliance levels. Moreover, the stakeholders based capability building seem to be important for most of the firms, regardless of their compliance levels. On the other hand, vertical alignments, which are advanced capabilities, are predominantly built by high compliant firms, i.e. 8 counts, versus 3 and 1 count by middle and low compliant firms respectively. Our interpretation of these results is that learning and knowledge transfer, and exchange from supply chain partners and stakeholders may be needed to progress in compliance, whilst basic capabilities relatively less important. These results seem to support hypothesis 2a, which states that higher compliance levels associates with sophisticated capabilities, i.e. intermediate and even more on advanced capabilities[95].

Figure 26: Capability building by compliance level



[95] These results from the descriptive statistics should be taken as preliminary, as a more systematic analysis follows ahead with the mvQCA.

The next section explores in more detail how these intermediate and advanced capabilities were built, with the intention of identifying patterns of capability building.

Intermediate vs. advance compliance capability building

This exploration of capability building will examine the differences between sets of firms that possess different compliance levels. As we assume that there is progress from first low to middle, and then eventually to high compliance; and then taking into account and focusing on the shares of intermediate capabilities in the transition from low to middle and to high compliance (See Table 6.2.1.4, p.229), the next section explores how intermediate capabilities were built by low and middle compliant firms. Applying the same logic, we then compare the advance capabilities building between middle and high compliant firms.

Intermediate capabilities building

Low compliant firms build up intermediate capabilities characterised by three main aspects (See Table 6.2.1.5, p.233). Firstly, there are considerably enhancements of the security applications of their security systems; firms were driven to adoption and adaptation of technologies or processes[96].

Secondly, to gain access to security-related expert knowledge without producing it internally, firms agreed with stakeholders to accumulate it and exploit it internally. The firm's concern would be about realising the potentials of expert knowledge. The role of the stakeholder was supporting the capabilities building of the firm, in whatever manner the firm considered necessary. The firms were not concerned about whether the stakeholders' capabilities evolved or not.

Thirdly, in some instances the stakeholders' capabilities would be a concern for the firms, but only because they required that stakeholders incur single capability upgrading, such as

[96] These capabilities resemble what in the literature has been argued as critical to enhance a firm's performance, innovation and absorptive capacity (Cohen & Levinthal, 1990).

ensuring that the service provided by stakeholder was of good quality. These stakeholders were not in the core business of moving the fresh produce, unlike their supply chain partners (exporters, transport and distributors)[97].

The middle compliant firms added two additional characteristics to those previously explored. Firstly, they had to learn practically how to transfer knowledge to their suppliers and clients, so that they (the partners) were able to exploit the security resources developed by the firm. In other words, in order for the firm's resources to deliver the security functions and conform to CTPAT, they had to tutor their supply chain partners in how to utilise and adapt security resources, which implies the building up of the supply chain partner's resources and capabilities. This is exploiting externally what is developed internally[98]. Secondly, driven by the need to meet security regulations, they engaged in joint designs and planning with their stakeholders. At that point it was not enough to transfer knowledge or to accumulate it internally. They created systems that provided the security functions that were available neither internally nor externally, but which could potentially be created by merging stakeholders' resources with the firm's internal resources (See Table 6.2.1.6, p.234).

[97] In relation to the resource networks, von Tunzelmann and his colleagues (2003, 2007) suggested that firms needed to align their resources and capabilities with a network of suppliers and clients. Alignments of capabilities between the network of suppliers of resources for the business operations are called resource network alignments, whereas the subset of resource network alignment between the main suppliers of inputs for production and the users/clients of their products are called vertical alignments (von Tunzelmann, 2003, p. 379; von Tunzelmann & Wang, 2007, p. 200).

[98] This is a complementary feature of the absorptive capacity, only it resembles the opposite direction of the knowledge transfer, from the focal firm to its suppliers or clients, and it requires identification of the potential uses of the own technologies (and processes) in their partners' operations, establishing the transaction and the appropriate knowledge transfer to the external firm; this outward knowledge transfer had been called 'desorptive capacity'. More specifically, desorptive capacity is the firm's ability to externally (outside the boundaries of the firm) exploit knowledge (Herzog, 2008, p. 43; Lichtenthaler, 2009, p. 842; Lichtenthaler & Ernst, 2007, p. 44).

Table 6.2.1.5: Inventory of intermediate capabilities by low compliant firms

Firm	*Capabilities building*	*Intermediate capabilities*	*Coding*
SC1D	Adoption and adaptation of SC1E traceability system	Adoption and adaptation	C.SH
SC1E	Agreement on the coordination strategies with the State Preventive Police with trained personnel and dogs to detect drugs and other chemicals at the facilities access point.	Agreement and coordination with Unrelated organisations (SH)	C.SH
SC2E&T	1) Coordination between SC2E&T (driver), customs brokers, and insurance providers for traceability and electronic manifest.	Coordination with network of suppliers (SH)	C.SH
	2) Reliance in electronic transmission by the customs broker.	Exploiting Network of suppliers' resources (SH)	C.SH
	3) Trailers inspection and hauling in the Mexican customs broker or Maymar.	Exploiting Network of suppliers' resources (SH)	C.SH
SC3T	1) Personal CEOs' networks with drivers with good reputation through experience in other firms.	Exploiting Network of suppliers' resources (SH)	C.SH
	2) An external company performs the electronic manifest and the prior notice.	Coordination with Unrelated organisations (SH)	C.SH
	3) Trust building and coordination with other drivers for conveyance security.	Coordination with Unrelated organisations (SH)	C.SH

Table 6.2.1.6: Inventory of intermediate capabilities by middle compliant firms

Firm	*Capability building*	*Capabilities*	Coding
SC1&5T	1) GPS and electronic manifest integrated software by the developer, in coordination with the SC1&5T.	Adoption and Adaptation	C.SH
	2) Following procedural security as defined by exporter and distributor.	Adoption	C.SH
	3) Awareness sessions developed by CTPAT, and practical session with the US Department of Transport.	Adoption	C.SH
SC3D	1) Recommendations and security profiles developments for the SC3E and SC3T in physical security.	Desorptive capacity	C.SD
	2) Recommendations and security profiles developments for the SC3E and SC3T in access controls and procedural security.	Desorptive capacity	C.SD
	3) Recommendations and security profiles developments for the SC3E and SC3T in procedural security.	Desorptive capacity	C.SD
SC3E	1) Coordinated service with outsourced private security provider.	Agreement with Network of suppliers	C.SH
	2) Implementation adopted and adapted from the SC3D on Physical, access controls, and procedural securities.	Adoption and adaptation	C.SH
	3) Assessing the trailer security of the transport provider and issuing the recommendations given by the SC3D.	Desorptive capacity	C.SD
	4) Designing access controls in coordination with the private security service provider.	Joint design: firm-Unrelated organisation	C.SH
SC4D	1) Development of security profiles with CBP officials.	Joint design: firm-Unrelated organisation	C.SH
	2) Development of security profiles for the SC4E&T in procedural security and agreeing with customs brokers for better coordination of SC4E&T.	Desorptive capacity	C.SD
	3) Development of security profiles for the SC4E&T in conveyance security.	Desorptive capacity	C.SD
	4) Analysis of drivers' behaviour with information provided by SC4E&T's traceability systems.	Adoption	C.SH
	5) Consultant inducing the security awareness in the firm.	Adoption	C.SH
	6) Customs broker specialised personnel for electronic manifest for all their clients, not only for SC4.	Desorptive capacity	C.SD
	7) SC4E&T support in trailer security (GPS and inspection reports).	Adoption and adaptation	C.SH
	8) SC4E&T support in conveyance security (GPS and inspection reports).	Adoption and adaptation	C.SH
SC4E&T	1) Procedural security enhanced by incorporating and training on the electronic monitoring of the surveillance practices (TouchProbe).	Adoption	C.SH
	2) Trailer security procedures developed internally but authorised and inspected by SC4D, US and Mexican Customs Brokers.	Agreement and coordination with network of suppliers	C.SH
	3) Agreements on anti-doping and background checks with State Police Department.	Agreement with Unrelated organisation	C.SH
	4) Adoption of the GPS convoy traceability system and adaptation of the settings to the needs of firms SC4E&T.	Joint design: firm-Unrelated organisation	C.SH
	5) HACCP training by CIAD for procedural security and trailer security.	Adoption and adaptation	C.SH
SC5D	1) Adoption of IT systems developed by SC5E.	Adoption	C.SH
	2) Implementation by SC5E and information sharing from SC5E to SC5D on how to analyse the management of the seals and their monitoring forms.	Adoption	C.SH

The previous capabilities building inventories seem to provide three general patterns. Firstly, Table 6.2.1.5 shows that most low compliant firms build capabilities to exploit and coordinate with their stakeholders (SC1E, SC2E&T, SC3T), and with little efforts made to build up absorptive capacity (SC1D). Secondly, Table 6.2.1.6 shows that middle compliant firms make serious efforts to try to build up absorptive capacity (SC1&5T, SC3E, SC4D, SC4E&T, and SC5D). And thirdly, middle compliant firms build up capabilities with their stakeholders and supply chain partners (SC3E- 4th capability; SC4D-1st, 2nd, and 3rd capabilities; SC4E&T-2nd and 4th capabilities).

Advanced capabilities

The advanced set of capabilities will be explored in middle and high compliant firms (Table 6.2.1.7, p.236).

To start with, it is important to highlight that there was only one middle compliant firm that built up advanced capabilities. The capabilities were used to jointly design security resources between the SC4E and SC4T. The capabilities evolved through learning by experience. The increasing knowledge stocks were expected to be realised within the firm SC4E, whilst the firm SC4T played the supportive role in the joint design processes. Although the SC4T's capabilities may evolve, the expected outputs were only appropriable by SC5E, and were not shared.

High compliant firms, on the other hand, not only jointly developed security resources with various internal departments, stakeholders and supply chain partners, but also made efforts to coordinate the supply chain, which appears to be 'the key' for high compliance.

It seems therefore that low compliant firms try to build up capabilities based on acquiring external knowledge for internal exploitation, whilst medium compliant firms have engaged in unilateral knowledge transfers from the firm to their partners, or from their partners to the firm. And finally, high compliant firms have prioritised the coordination of security systems along the supply chain.

Table 6.2.1.7: Inventory of advanced capabilities (Vertical alignment) by middle and high compliant firms

Compliance	Firm	*Capability building*	*Advanced capabilities* *(Vertical alignment-C.VA)*
Middle	SC4E&T	Mixed knowledge of surveillance systems by SC4T with complex packing facilities operations by SC4E for physical security, access control and awareness.	Joint design with SC
	SC2D	Information sharing (assessment) and coordination on the ways to conduct trailer inspections upon visits by SC2D to the SC2E&T facilities.	Coordination with SC
High	SC5E	Capability cogeneration during formal meetings, joint design exercises, joint planning, joint strategising, and coordination. It required the involvement of packing departments, the compliance manager, the SC5D CEOs, transport providers, consultants, and other stakeholders. The efforts translated into procedural, information technology, container and trailer, conveyance, and threat awareness security resources. All for a total of seven different resources.	Joint design and coordination with SC, supplier development, stakeholders and internal departments involvement and coordination.

Remarks on intermediate vs. advanced capabilities

All in all, based on the capabilities inventory by low (Table 6.2.1.5), middle (Table 6.2.1.6), and high (Table 6.2.1.7) compliant firms, it seem that firms require sets of capabilities ad-hoc to the compliance level.

The first transition, from low to middle compliance, may have required transcending from exploiting and coordinating with stakeholders to jointly design and plan the development of security resources with their stakeholders, or by developing desorptive capacity to support the supply chain partner's absorptive capacity in order to exploit the firm's security resources outside its own boundaries (by their supply chain partners), rather than inside their boundaries (the individual firm).

The second transition, from middle to high compliance, may have required building up the capability to coordinate the supply chain partners' resources implementation and, very importantly, developing their suppliers capabilities in order to enable the functionality of the firm's resources in the supply chain partners' security practices and operations. This suggests that there may be specific capabilities required to progress up the compliance ladder. The following section analyses more systematically the capabilities required by compliance level using the mvQCA.

6.2.2. mvQCA of the compliance capabilities building

The second research question is about how firms acquired or built up their capabilities and developed their resources to become compliant. In the previous section we mentioned two transitions towards higher compliance: intermediate capabilities building from lower to middle compliance, and advanced capabilities building from middle to high compliance.

The following sections present the analyses with mvQCA to identify the causal configurations of capability building that drove firms towards compliance. A later section attempts to evaluate the results and draw conclusions from them.

mvQCA: model specifications

To proceed with the analysis of the capability building process and determinants of compliance, we must specify the model. Similar to the compliance process, the outcome of the model is always compliance. In this analysis, due to the limitations of the QCA with TOSMANA of treating the output variable as binomial rather than multinomial, following the same procedures as with traditional statistical analyses like ANOVA, and the use of simple control variables in any type of regression, the dataset was split up to generate two groups; one group containing low and middle compliant firms, the other group containing middle and high compliant firms. The output variable takes value 0 if there is no compliance and 1 if there is compliance.

The causal conditions (independent variables) of compliance are the 6 capabilities:

1. Organisational competencies (ORGCAP=C.OC)
2. Managerial systems (MANSYS=C.MS)
3. Internal coordination (INTCOORD=C.IC)
4. Stakeholders support (STAH=C.SH)
5. Suppliers' development (SUPDEV=C.SD)
6. Vertical alignment (ALIGN=C.VA)

These causal conditions are not crisp sets yet (0, or 1), but multi-value sets. Consequently, thresholds had to be created. The threshold setting rule was the same for all causal conditions: 'if the firm had counts equal or over the median' in the particular causal condition, then that causal condition takes value 1; otherwise it takes value 0.

There was one exception in the thresholds settings; vertical alignments caused contradictory results within such a threshold. To correct this, the threshold for this capability was changed from 0.5 to 2, which eliminated the contradiction. With this we obtained straightforward results. This decision has implications, however. For all other conditions (capabilities) it was assumed that having built at least 1 capability was already intensive compared with those not having such a capability at all. The threshold slightly modified the interpretation for vertical alignments. Firms with 0 or 1 vertical alignment capabilities built are not intensive, and they need to have built twice or more their vertical alignments to be considered intensive.

mvQCA: the compliance capability building

The analysis was divided into three stages. In Stage 0 we identified the causal configurations leading to low compliance, comparing against middle compliance firms. In Stage 1 we identified the causal configurations of middle compliance, comparing against low compliant firms. In Stage 2 we identified the causal configurations of high compliance, comparing against middle compliance firms. As in the analyses of the compliance process, the models also tried to identify reminders and contradictions, to enhance parsimony and inclusiveness. However, we found no more contradictory results.

Table 6.2.2.1: Causal configurations of the compliance capability building*

Stages	Causal configurations
0. Low compliance	orgcap*[MANSYS$_s$+stah$_s$]+intcoord*align[ORGCAP$_s$+supdev$_s$] *(SC1E)* + *(SC1D, SC2ET, SC3T)*
1. Middle compliance	[ORGCAP*INTCOORD]$_s$+ALIGN$_s$+[STAH*(orgcap$_s$+mansys$_s$)]+[orgcap*mansys]$_s$ *(SC3D, SC5D)* + *(SC4ET)* + *(SC15T, SC3E,SC4D)*
2. High compliance	[MANSYS*SUPDEV$_n$]$_s$ + [SUPDEV$_n$*ALIGN]$_s$ *(SC2D, SC5E)*

*The model was run with Tosmana 1.301 (Cronqvist, 2009). Minimise =1 or 0, Including=C(Contradictions)+R(Reminders).
** Minimising=C, Including=R+1(Compliance levels).
ORGCAP=intensive in organisational competencies;
MANSYS=Intensive in managerial systems;
INTCOORD=Intensive in internal coordination;
STAH=Intensive in stakeholders support;
SUPDEV=Intensive in supplier development;
ALIGN=Intensive in vertical alignment;
CAPITAL LETTERS INDICATE AN INTENSIVE CAUSAL CONDITION (CAPABILITY)
Lowercases indicate the a non-intensive causal condition (capability)
Subscripts: s=sufficient condition; n=necessary condition; ns=necessary and sufficient conditions; no subscripts indicate that the condition is neither necessary nor sufficient.
+ in the model results denotes 'or', in set theory represents 'Union'
* in the model results denotes 'and', in set theory represents 'Intersection'

At first glance, the compliance capability building configurations suggest that low compliant firms use basic capabilities rather than intermediate or advanced to develop security resources. On the other hand, middle compliant firms diversify the capabilities building as much as possible for the development of security resources. And finally, there is a more focused approach in the capabilities built by high compliant firms, with a key role played by knowledge transfers to supply chain partners (supplier development) (Table 6.2.2.1, p.240).

In the following section the causal configurations detail the three compliance levels and propose some interpretations of the results.

mvQCA: evaluation and interpretation of the model results

Stage 0: When firms do not want to climb up the compliance ladder

It was mentioned in previous sections that although some firms were not explicitly seeking compliance, they were all trying to conform to some degree with CTPAT guidelines. This analysis therefore tries to identify capabilities building by all firms, even when they are not looking for compliance.

Low compliance is associated with various causal configurations. Firms tried to build up managerial systems for the development of security resources, but without the support of organisational competencies. Also, the lack of organisational competencies was followed by a lack of stakeholder support (SC1E). Where there has been an attempt to build up organisational competencies for security resources developments, it has been done in isolation from other basic and advanced capabilities (SC1E, SC2ET, and SC3T). Hence, the only instances where low compliant firms have tried to build up security-related capabilities have focused on isolated efforts either in managerial systems or organisational competencies (See Figure 27, p.242).

Figure 27: Capability building in low compliance

```
Tosmana Report
Algorithm: Graph-based Agent
Model Settings:
            Minimizing Value    1
            including           C R
Variable Settings:
Truth Table:
v1:         orgcap      v2:     mansys
v3:         intcoord    v4:     stah
v5:         supdev      v6:     align
O:          lowcompliance       id:     firm
v1          v2          v3      v4      v5      v6      O       id
0           0           1       1       0       0       0       SC15T
1           0           0       0       0       0       1       SC1D
0           1           1       0       0       0       1       SC1E
1           1           0       1       0       0       1       SC2ET,SC3T
1           0           1       0       1       0       0       SC3D
0           0           1       1       1       0       0       SC3E
0           0           0       1       1       0       0       SC4D
1           1           0       1       0       1       0       SC4ET
1           1           1       0       0       0       0       SC5D
Result: (all)
            orgcap * MANSYS +           ORGCAP * intcoord * align
            (SC1E)   (SC1D+SC2ET,SC3T)

            orgcap * MANSYS +           intcoord * supdev * align
            (SC1E)   (SC1D+SC2ET,SC3T)

            orgcap * stah +     ORGCAP * intcoord * align
            (SC1E)   (SC1D+SC2ET,SC3T)

            orgcap * stah +     intcoord * supdev * align
            (SC1E)   (SC1D+SC2ET,SC3T)
Created with Tosmana Version 1.301
```

Stage 1: The first and steady steps

Compared to the low compliant firms, the middle compliant firms show greater diversity of capabilities, given that low compliance is mainly based upon managerial systems or organisational capabilities (Figure 27, p.242), whilst middle compliance is based upon vertical alignments, organisational capabilities, internal coordination, and stakeholders support (Figure 28, p.243). However, the capabilities for middle compliance are bundled into three configurations: 1) vertical alignment capabilities, 2) combinations of organisational competencies and internal coordination capabilities, and 3) stakeholders support.

The first configuration, vertical alignment capabilities (ALIGN), shows that the development of security resources based on vertical alignment is a valuable on its own, as it alone positions the SC4ET in middle compliance (Figure 28, p.243).

The second configuration, organisational capabilities and internal coordination, on the other hand, imply that the capabilities alone are not sufficient to drive companies, SC3D and SC5D, to middle compliance, as the results show only combining them (ORGCAP*INTCOORD), rather than individually, firms position themselves in middle compliance. This means the value of the capabilities derives from complementing each other (Figure 28, p.243).

The third configuration, stakeholder involvement is valuable, as long as the firms (SC15T, SC3E and SC4D) do not divert their attention on organisational competencies (orgcap*STAH) or managerial systems building (mansys*STAH), as they risk to be identified as low compliant, and lose their status as middle compliant. Thus, full attention may be required in acquiring and exchanging knowledge with their stakeholders for middle compliance (Figure 28, p.243).

Figure 28: Capability building for middle compliance

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:
Name Thresholds
Truth Table:
v1: orgcap v2: mansys
v3: intcoord v4: stah
v5: supdev v6: align
O: middlecomplianc id: firm

v1	v2	v3	v4	v5	v6	O	id
0	0	1	1	0	0	1	SC15T
1	0	0	0	0	0	0	SC1D
0	1	1	0	0	0	0	SC1E
1	1	0	1	0	0	0	SC2ET,SC3T
1	0	1	0	1	0	1	SC3D
0	0	1	1	1	0	1	SC3E
0	0	0	1	1	0	1	SC4D
1	1	0	1	0	1	1	SC4ET
1	1	1	0	0	0	1	SC5D

Result: (all)

ALIGN + orgcap * mansys + ORGCAP * INTCOORD
(SC4ET) (SC15T+SC3E+SC4D) (SC3D+SC5D)

ALIGN + orgcap * STAH + ORGCAP * INTCOORD
(SC4ET) (SC15T+SC3E+SC4D) (SC3D+SC5D)

ALIGN + ORGCAP * INTCOORD + mansys * STAH
(SC4ET) (SC3D+SC5D) (SC15T+SC3E+SC4D)

Created with Tosmana Version 1.301

Stage 2: Compliance leadership

Previously, a progression in the sophistication of capabilities needed to increase compliance levels seemed to be present. Nevertheless, for high compliance rather than focusing on advanced capabilities, resources were developed based on intermediate capabilities, 'Supplier Development'.

On the other hand, building up these capabilities is still not enough for high compliance, as they have to be accompanied by management systems or by vertical alignment to position the firms (SC2D and SC5E) in high compliance. Furthermore, these two capabilities taken individually are neither necessary nor sufficient for high compliance.

Paying closer attention to the two high compliant cases, it is possible to illustrate that firms with high compliance may request that their supply chain partners build up security-related capabilities in ways that align these partners' security functions with those developed using the firm's resources so that they can be efficiently utilised by their supply chain partners; this is a process we refer to as desorptive capacity. Consequently, the whole supply chain may conform to the CTPAT guidelines, and may be granted certification, thus eventually collectively appropriating regulatory benefits.

The presence of managerial systems as a complement of desorptive capacity suggests that supply chain learning and knowledge sourcing may be accompanied by internal systems for high compliance, either to trigger such learning processes or to exploit internal knowledge, and the product of that learning.

This is similar to Winter and Szulanskis' (2001) propositions about replications as strategies. The use of templates (following step-by-step procedures) is used to replicate systems and operations to avoid repetition of errors; however, such templates should follow periods of experiential learning (Winter & Szulanski, 2001, pp. 733, 737). In our context, desorptive capacity may be one of the forms of experimental learning, and managerial systems one of the forms of replication systems, or templates.

When the firm does not complement desorptive capacity with managerial systems, it is still possible to make the association to high compliance if vertical alignments are the complement. This implies that, upon upgrading of the supply chain partners' capabilities, new potential security functions may be identified by the firm. This may trigger the firm's intention to re-adapt their resources to deliver new security functions. Such re-adaptations may be called a capability, i.e. desorptive capacity, to the extent that their supply chain partners exploit the newly developed security functions.

Figure 29: Capability building for high compliance[99]

Tosmana Report
Algorithm: Graph-based Agent
Model Settings:
Minimizing Value 1
including C R
Truth Table:

v1:	orgcap	v2:	mansys
v3:	intcoord	v4:	stah
v5:	supdev	v6:	align
O:	highcompliance	id:	firm

v1	v2	v3	v4	v5	v6	O	id
0	0	1	1	0	0	0	SC15T
1	1	1	0	1	1	1	SC2D
1	0	1	0	1	0	0	SC3D
0	0	1	1	1	0	0	SC3E
0	0	0	1	1	0	0	SC4D
1	1	0	1	0	1	0	SC4ET
1	1	1	0	0	0	0	SC5D
1	1	0	1	1	1	1	SC5E

Result: (all)
MANSYS * SUPDEV + SUPDEV * ALIGN
(SC2D+SC5E) (SC2D+SC5E)
Created with Tosmana Version 1.301

[99] Due to having no contradictions in this stage, the threshold was reset to .05 in vertical alignment. This slackens the conditions for high compliance.

mvQCA: compliance capabilities building remarks

In summarising the previous discussion the following observations can be made. Overall, the compliance capability building may follow various pathways from low to middle, and from middle to high compliance.

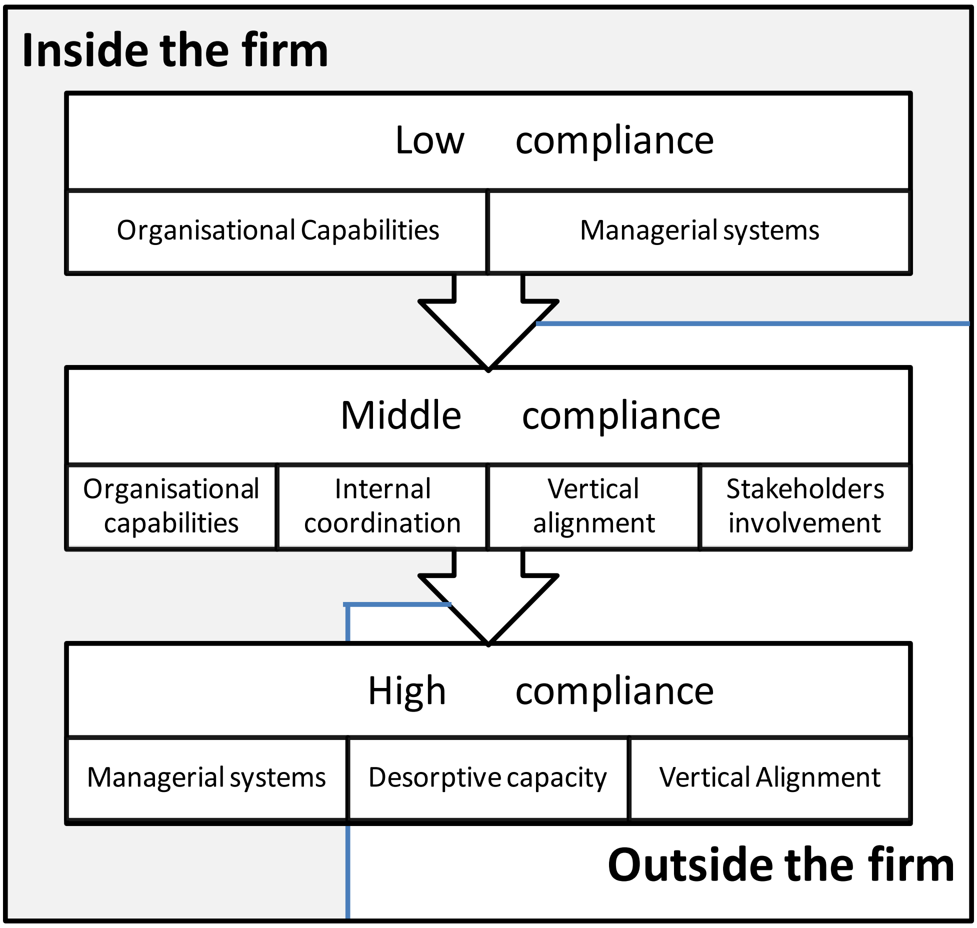
Firstly, when firms are low compliant, they try to develop security resources based on their organisational competencies (SC1E), or set up managerial systems (SC1D, SC2ET and SC3T) to do so. It seems that intermediate and advanced capabilities are still prohibitive at this stage of play.

For middle compliant firms there were three capability-building pathways. The first was based upon basic capabilities and the building up of organisational capabilities together with internal coordination capabilities (SC3D and SC5D). The second was based upon intermediate capabilities; when firms did not have either managerial systems or organisational capabilities, they supported their capability building of their stakeholders (SC15T, SC3E and SC4D). The third was based upon advanced capabilities; vertical alignments were used to support their capability building for compliance at middle level (SC4ET).

An interesting element related to the capabilities bundle is that managerial systems may have different importance at different compliance levels, given that for low compliance it was a valuable capability (Figure 27, p.242), for middle compliance it was needed not to be present (Figure 28, p.243), and for high compliance, it was also needed in combination with desorptive capacity (Figure 29, p.245). Moreover, in the absence of organisational capabilities, managerial systems capabilities have a negative impact in terms of compliance, positioning firms like SC1E in low compliance (Figure 27, p.242); but it is combined with desorptive capacity, it may have great complementary value, positioning firms like SC2D, SC5E in high compliance.

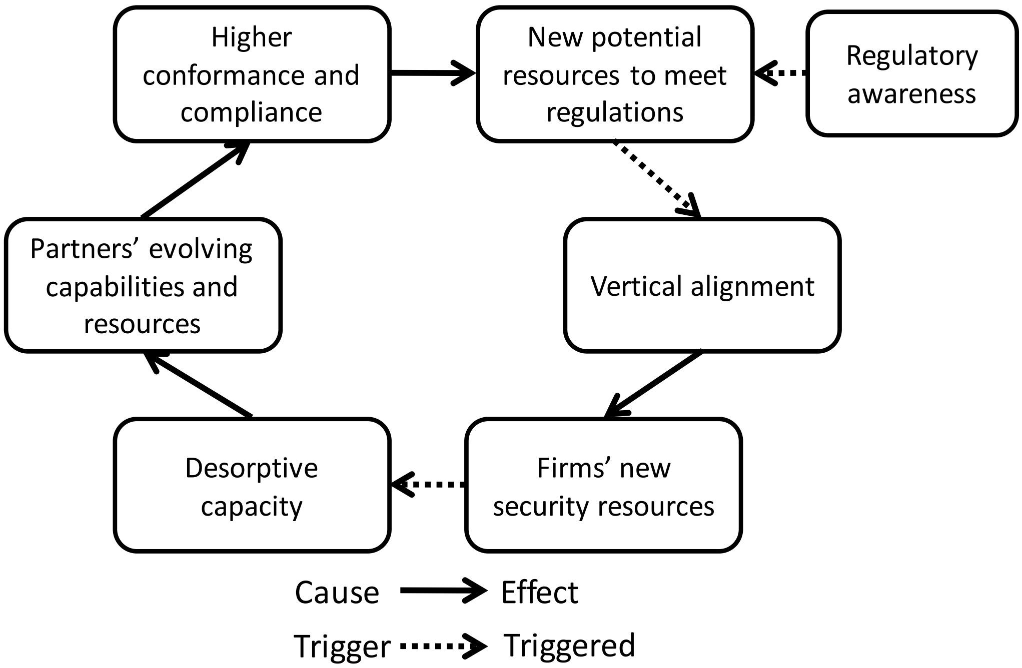
Similarly, desorptive capacity, vertical alignment and managerial systems have only complementary value for high compliance. However, to develop security resources with enough value to gain high compliance, the necessary condition was building up desorptive capacity. Although these results are not supportive of **hypothesis 2a**, they are revealing, since it was an intermediate capability what contributes to a high compliance level, rather than an advanced capability (See Figure 30, p.247). Rejecting the hypothesis highlights the value of a systematic assessment based upon mvQCA compared to using simple descriptive statistics (p. 236) which suggested accepting the hypothesis.

Figure 30: Compliance capability building



The compliance capabilities building processes resemble the evolutionary processes described by Teece (1986, p. 289) for complementary assets. Basic capabilities may relate to resources and capabilities that are neither complementary nor very difficult to protect outside the firm. Stakeholder support implies the unilateral dependency of the firm to their suppliers, whilst vertical alignment may relate to bilateral dependency.

Figure 31: Evolutionary compliance capability building



Desorptive capacity deserves special treatment. It is a case of bilateral dependency; one firm depends on the capabilities of the partners to exploit security resources, rather than to appropriate knowledge or assets (Lichtenthaler & Lichtenthaler, 2009, p. 1321). In this case, the value of resources is not only not intrinsic, but is also given by a non-market player, the regulator, and mediated by the supply chain partners' capabilities. To the best of our knowledge, this is a new understanding of bilateral dependency, in comparison to the traditional vertical alignments view of bilateral dependency which consist on the firm's capacity to acquire knowledge and profit from suppliers or and clients, whilst our understanding of bilateral dependency consist on the firm's capacity to enable the knowledge of the suppliers and clients to be able to profit not directly from them, but from the regulatory benefits.

Lastly, Teece (1986) analysed complementary assets under partial integration. It would have been useful know how complementary assets are managed under different types of governance structure. The next section explores the relationship between capability building and supply chain governance, the governance structures associated with capabilities building for each compliance level.

6.3. Supply chain relationships

It was shown above that basic capabilities are built upon efforts within the firm, whilst intermediate capabilities are built upon unilateral capability building in relationship with supply chain partners and/or stakeholders, and advanced capability building required substantial efforts and interaction between supply chain partners and, expectedly, with bilateral dependency. The present section analyses the governance structures on which development of security resources and capabilities is based. It is worth stressing that governance structures relate to the overall supply chain relationships, not only for security purposes, but also for business relations as a whole. Therefore, the analysis will seek to identify the overall governance of the supply chain business relationships that are conducive of capability building for security purposes.

Initially in this section we try to identify the governance structures contributing to individual capabilities for high compliance, i.e. managerial systems, desorptive capacity, and vertical alignment. Later, we identify the governance structures contributing to capabilities configurations for high compliance, i.e. the pairing of managerial systems and desorptive capacity, and desorptive capacity and vertical alignment.

The main constructs under examination are: power asymmetry, dependency, vertical integration, and vertical coordination.

Before we move onto the analysis, it is necessary to remind ourselves of the meaning of each component of the governance structure, as described in the methodological chapter (Table 3.2.4, p.64).

6.3.1. Summary of supply chains governance structures

Supply chain relationships are structured and governed by their parties. The structure is here defined by whether or not the firms are vertically 'integrated' and/or 'coordinated' with their supply chain. These are neither mutually exclusive nor inclusive, and they both need to be individually analysed.

The governance of the supply chain relationships can be seen as a power relation, related to the degree of dependency of the firm to the supply chain. Similarly, these are neither exclusive nor inclusive, but they must be individually analysed to try to draw meaningful conclusions. The following lines summarise the constructs for governance structures:

- *Vertical integration* refers to unified: 1) ownership, and 2) hierarchies (or some kind of authority) across various supply chain stages.
- *Vertical coordination* refers to harmonising and interacting: 1) investments, and 2) capabilities and skills building across supply chain stages.
- *Power asymmetry* refers to who in the supply chain decides whether the firm should comply or not with regulations, standards, norms, and so on.
- *Dependency* refers to: 1) the extent to which the firm have developed assets that are specific to the supply chain, 2) the time span of the firm's relationship with its supply chain partners, in terms of the time they have been in business and the time they expect to continue doing business, and 3) the degree of business transactions concentrated in its supply chain partners.

The governance structures are investigated in three ways: 1) the distributor's perception of the governing and structure in relation to the exporter, 2) the exporter's perception of the governing and structure in relation to the distributor, and 3) the transport provider's perception of the governing structure in its relations with both distributor and exporter.

The following Table 6.3.1.1, p.251, shows the summary of the values for each one of the constructs used to assess each firm's governance structure.

Table 6.3.1.1: Supply chain governance structures

Firm	Governance				Structures			
	Power Asymmetry	Dependency			Coordination		Integration	
	Decision making[1]	Asset specificity[2]	Relationship length[3]	Market Concentration[4]	Activities[5]	Investments[6]	Hierarchies[7]	Ownership[8]
SC15T	6	-3	19	30	0	2	0	0
SC1D	5	-1	15	100	3	1	0	0
SC1E	1	1	25	100	5	0	1	0
SC2D	1	0	23	20	0	4	0	0
SC2ET	1	0	23	70	5	4	2	3
SC3D	1	1	18	20	4	4	1	3
SC3E	1	2	20	90	5	4	1	2
SC3T	10	1	5	18	1	0	0	0
SC4D	10	1	30	60	5	4	0	0
SC4ET	9	6	28	100	4	4	0	3
SC5D	5	0	30	80	1	3	0	3
SC5E	4	2	25	80	2	4	0	0
Mean[9]	4.5	0.8	22	64	2.9	2.8	0.4	1.2
Median	4.5	1	23	75	3.5	4	0	0

1. Power asymmetry: scale from 1 to 10, where 1 means that decisions are made by supply chain partners, 10 decisions made by the firm, and 5 shared decision making between the firm and supply chain partners.
2. Asset specificity: scale from -6 to 6, where -6 denotes that assets are not specific, (i.e. 1) Geographic location, 2) infrastructure, 3) human capital, 4) brand, 5) technology and processes, and 6) marketing windows), and 6 means that assets are highly specific.
3. Relationship length. Scale from 0 to 30 years, where 15 years corresponds to the time the firm has spent with the supply chain partners, and 15 more years corresponds to the time the firm expects that its relationship with the supply chain partners will last. Any time frame was constrained to 15 years; therefore firms with 20 years were classified as 15 years.
4. Market concentration: scale from 0 to 100, where for the distributor this represents the share of volume of produce distributed for its main exporter in the study (SC1D-SC1E); for the exporter this represents the share of volume of produce exported throughout the main distributor (SC1E-SC1D); and for the transport provider this represents the share of the movement of cargo for the exporter and distributor in the total movement of cargo (SC14T-SC1E and SC1D).
5. Activities: scale from 0 to 5, where 0 represents no activities coordination with the supply chain partners and 5 represents complete coordination of activities with the supply chain partners, i.e. 1) systems of skills and capabilities (synergies between projects), 2) skills and capability building roadmaps (information sharing), 3) joint capabilities and skills development planning, 4) exchange (temporal) of human resources for skills and capability building between the firm and supply chain partners, and 5) shared (continuous) skills and capabilities building teams.
6. Investments: scale from 0 to 4, where 0 means that no efforts to coordinate investments between the firm and supply chain partners have been made, and 4 means that maximum coordination efforts of investments between the firm and its supply chain partners have been made, i.e. 1) systems of assets (synergies between projects), 2) roadmaps for investments, 3) parallel and interacting investments across units among firms; and 4) loans and financing the client/supplier.
7. Hierarchies: Scale from 0 to 2, where 0 indicates that the firm manages the skills formation and capability building activities only within its boundaries; 1 indicates that the firm also manages the skills formation of other stages of the supply chain; and, 2 indicates that the firm also manages the entire capability building activities of other stages of the supply chain.
8. Ownership: scale 0 to 3; where 0 means separate ownership between the firm and other supply chain partners; 1 means the presence of minority investments by the firm in their supply chain partners business; 2 means the presence of joint ventures (resulting in creation of new entities) between the firm and the supply chain partners; and 3 means that the firm is under unified ownership (acquisition/merger) with other supply chain partners.
9. Although it is useful to make broad comparisons by using averages it may also be misleading, since for instance in ownership, in our sample, there is no case with minority investments in the supply chain partners, while the average is suggesting that there is.

The Table 6.3.1.1, p.251 shows firms (e.g. SC3E) under power relations concentrated in the supply chain partners rather than in their own firm (SC3E power asymmetry=1), with a high degree of dependency due to high asset specificity (SC3E asset specificity=2), relationship length below the average (SC3E relationship length=20 years) their market concentration is far above the rest of the firms in the study (SC3E concentration=90%). This indicates that the firm may be falling under unilateral dependency in favour of their supply chain partners.

There are also cases of firms concentrating the decision making power (e.g. SC4D power asymmetry=10) yet still being dependent on their supply chain partners (SC4D asset specificity=1, relationship length=30, and market concentration=60%).

In terms of structures, there are firms which are vertically coordinated and integrated (SC2E&T Activities=5, Investments=4, Hierarchies=2, and Ownership=3). There are other firms which are vertically uncoordinated and disintegrated (SC3T Activities=1, Investments=0, Hierarchies=0, and Ownership=0), and various degrees in between.

The combination of the previous elements helped identifying various supply chain governance structures. Averaging and dichotomising the values for the four constructs (symmetric-asymmetric power, dependent-independent, coordinated-uncoordinated, and integrated-disintegrated) it is possible to devise 16 different combinations of governance structures, which lead to Table 6.3.1.2, p.253.

The following Table 6.3.1.2, p.253, shows that among 12 cases in our investigation, there are 10 different types of governance structures under which security-based capabilities were built.

In the searching of patterns of governance structures we plot the 4 constructs of the governance structure into a four-dimensional graph. Hence the following (Figure 32, p.254) is a graph rotated along different angles in order to facilitate the search for patterns across firms.

Table 6.3.1.2: Summary of supply chain governance structure[100]

Firm	Power asymmetry	Dependency	Coordination	Integration	Governance structures types count
SC15T	Symmetric	Independent	Uncoordinated	Disintegrated	1
SC1D	Symmetric	Independent	Uncoordinated	Disintegrated	1
SC1E	Partners	Dependent	Uncoordinated	Disintegrated	2
SC2D	Partners	Independent	Uncoordinated	Disintegrated	3
SC2ET	Partners	Independent	Coordinated	Integrated	4
SC3D	Partners	Independent	Coordinated	Integrated	4
SC3E	Partners	Dependent	Coordinated	Integrated	5
SC3T	Firm	Independent	Uncoordinated	Disintegrated	6
SC4D	Firm	Independent	Coordinated	Disintegrated	7
SC4ET	Firm	Dependent	Coordinated	Integrated	8
SC5D	Symmetric	Dependent	Uncoordinated	Integrated	9
SC5E	Symmetric	Dependent	Coordinated	Disintegrated	10

The first dimension in the graph (Figure 32, p.254), power asymmetry, has a scale of 0 to 4. 0 and 4 do not have meaning, as they were used for graphical convenience, 1 means that the decision-making power is located within the firm, 2 means that the decision making power is shared between the firm and the supply chain partners, and 3 means that the decision making power is held by the supply chain partners.

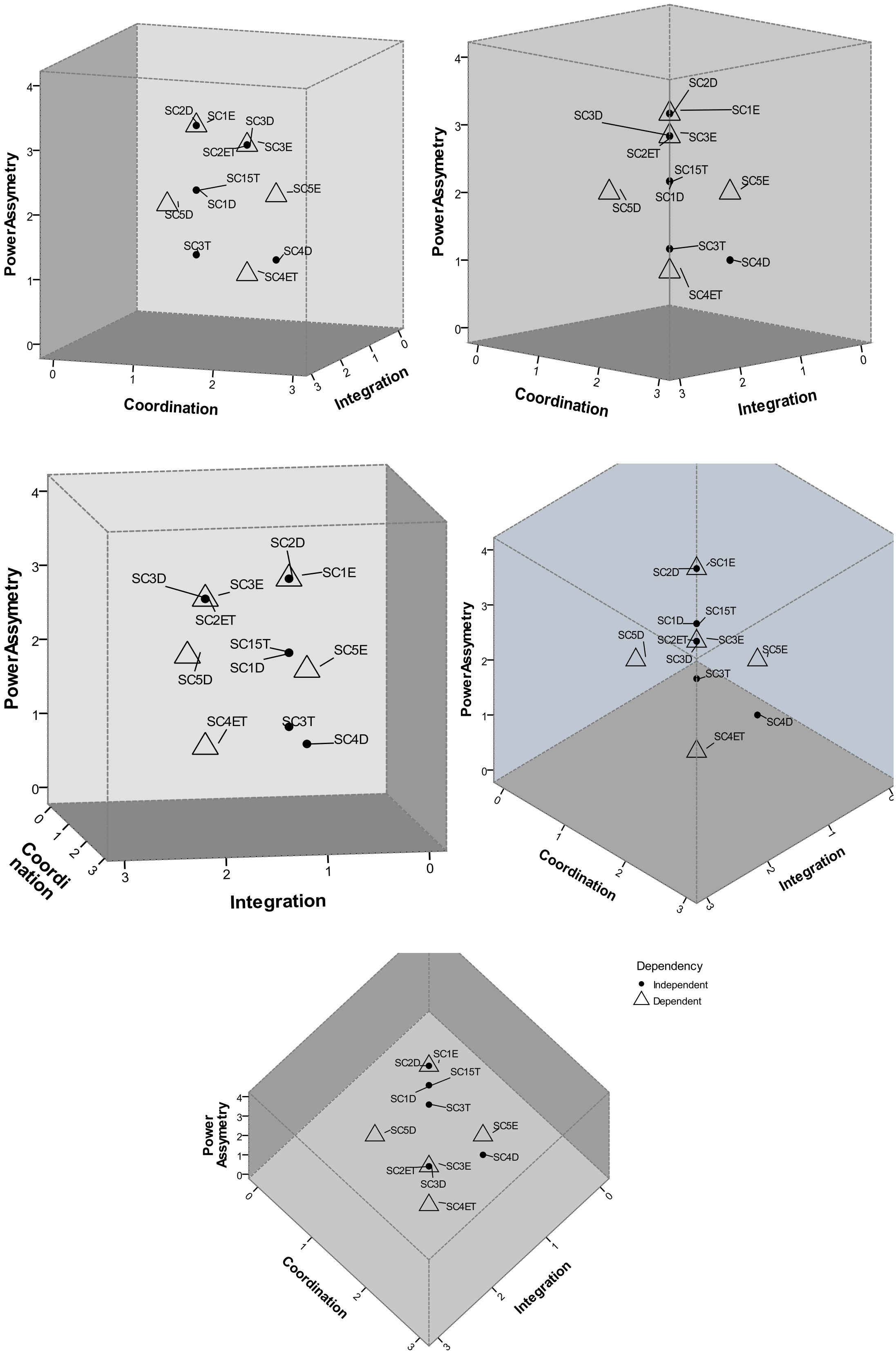
The second dimension, coordination, has a scale of 0 to 3. 0 and 3 do not have meaning, as like previously they were introduced for graphical convenience, 1 means that the firm is uncoordinated, and 2 means that the firm is coordinated with the supply chain.

The third dimension, integration, has a scale of 0 to 3. 0 and 3 do not have meaning, as the previous variables, 1 means that the firm is disintegrated from the supply chain, and 2 means that it is integrated with the supply chain.

The fourth dimension, dependency, is represented with two key shapes (Δ and ●). ● means that the firm is independent from its supply chain, whereas Δ means that the firm is dependent on its supply chain. (See Figure 32, p.254).

[100] The thresholds to categorise governance structures as asymmetric or not, dependent or independent, coordinated or uncoordinated, and integrated or disintegrated, were based upon thresholds set by TOSMANA software (mvQCA software). This is explained further below (Figure 33).

Figure 32: Visual representation of the governance structures



From the previous graphs (Figure 32, p.254), it is difficult to identify an underlying pattern of governance structures. Hence, it is not possible to associate governance structures with the types of capabilities that led firms (SC2D and SC5E) to compliance. Thus the following section tries to identify such patterns based on the mvQCA.

6.3.2. mvQCA of the Supply chains governance structures

This section initially demonstrates how specific capabilities (i.e. managerial systems, desorptive capacity, and vertical alignment) link with the firms' governance structures. It then demonstrates the configurations that contributed to firms (SC5E and SC2D) building up joint managerial systems and desorptive capacity, as well as joint desorptive capacity and vertical alignment.

As in the previous mvQCA analysis, the model specifications are presented first, to be followed by a summary of the results, and finally some interpretations of them.

mvQCA: Model specifications

In previous sections, the mvQCA was intended to identify compliance processes and capabilities for each compliance level; in other words, compliance processes and capabilities were the independent variables, whilst compliance was the dependent variable. In these sections, we follow a different strategy; we will try to identify the structural and governance conditions under which capabilities were built. This means that governance structures are the independent variables and capabilities are the dependent variables.

Hypothesis 3a is that increasing capability sophistication may drive integration, coordination, power asymmetry, and bilateral dependency. Hence, to test for this hypothesis, we applied the mvQCA to identify the causal configurations 4 times, for: 1) managerial systems, 2) desorptive capacity, 3) vertical alignment, and 4) joint managerial systems and desorptive capacity, and joint desorptive capacity and vertical alignments.

The governance structures (causal conditions) of security-based capability building include 8 variables. These causal conditions may be crisp (binomial) or multi-value (ordinal) sets. Therefore, various thresholds had to be created. The threshold setting rule was similar for all causal conditions: 'if the count was close to the median' the causal condition took a value of 1. Otherwise, it took a value of 0. The threshold however, had to be adapted to each causal condition, to have balanced and analytically justifiable groups, which also helped reducing contradictory results (See Table 6.3.1.1, p.251; and Table 6.3.2.1, p.260).

The justification and the implication of these adjustments is explained in the following paragraphs.

In general, the mvQCA acknowledges that setting thresholds may not necessarily be a sensibly practice, due to the structure of the data, which in some cases may not allow for homogenous subsets (Cronqvist, 2005, p. 3); hence, given that all variables have different structures and analytical implications, it may be as non-sense setting random thresholds as well as setting the same threshold for all variables. For some variables it may be necessary to dichotomise setting one threshold (e.g. it would be acceptable to classify firms according to the time span of their relationship, as long or short), whilst for others to trichotomise setting two thresholds (e.g. it would be better to classify firms according to the decision making power held by the supplier, or by the exporter, or by both).

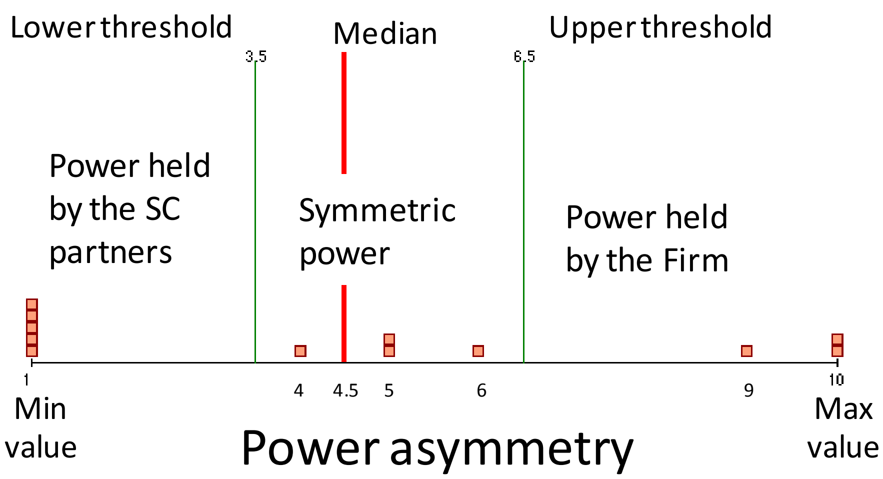
For instance, the variable power asymmetry, lends itself to be clustered in three 'relatively homogeneous' subset of firms, 1) the subset of firms which declared that the decision making power rested in the supply chain partner, 2) the subset of firms which declared that the decision making power rested in themselves, and 3) the subset of firms declaring that the decision making power was so some extent similar or shared between the themselves and their supply chain partners. These thresholds intend to capture the correlation between the distribution of the decision making power along the supply chain and the compliance capabilities building. In this case, the lower threshold was set on 3.5 of the power asymmetry scale, whilst the upper threshold was set on 6.5. Note that there would be no difference in the analysis if the lower threshold was set in the region between 1 and 4 (excluding these values), or if the upper threshold was set in the region between 6 and 9 (excluding these values), because it would not change the classification of the firms, as they remain in the same cluster (see Chart 5, p.258, and Table 6.3.2.1, p.260)[101].

Another example is the variable asset specificity, which although it might be possible to set two thresholds, the analysis tries to differentiate firms with specific assets from the rest (the ones with generic assets), which means setting only one threshold (1.5 of the asset specificity scale). So, firms over the 1.5 threshold are the ones with compliance capabilities and resources specific to their supply chain partners (see Chart 6, p.259 and Table 6.3.2.1,

[101] However, if we had a larger sample size, it is likely we would have firms in the currently empty region and results could have changed; hence it is important that thresholds make analytical sense and they are very fine tuned.

p.260). If the previous threshold had been put somewhere in the region between 0 and 1, it would had some of the firms (not all) with middle degree of asset specificity would have been classified together with the high specific assets, and then we would only distinguish between generic assets and slight asset specificity vs. middle and high asset specificity. Similarly, placing the threshold between -1 and 0 would have differentiated between firms with generic assets from the rest[102]. Thus, the threshold reflects our interest in differentiating firms with high asset specificity form the rest.

Chart 5. Threshold setting for power asymmetry



102 Again, it is important setting thresholds that make analytical sense, as it has implications in a potential context of larger sample sizes, where one may potentially find firms in one or the other side of the threshold with potentially different results.

Chart 6. Threshold setting for Asset specificity

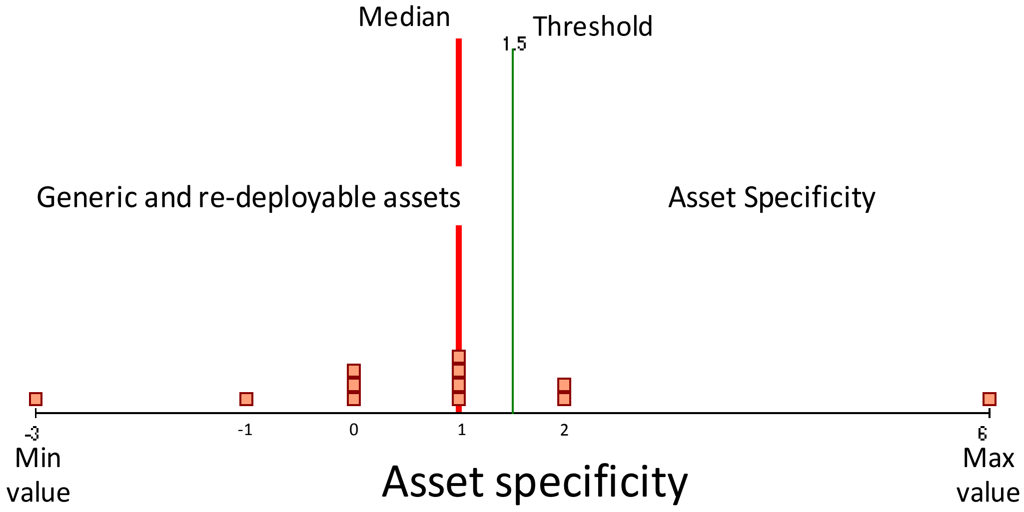


Table 6.3.2.1. Causal conditions, thresholds, and interpretations of governance structures

Governance structure conditions	Values and Thresholds	Interpretation
Power asymmetry (Decision making)	Value=0 if < 3.5 Value=1 if ≥ 3.5 and < 6.5 Value=2 if ≥ 6.5	Power concentrated in the SC partners Symmetric power Power concentrated in the Firm
Asset specificity	Value=0 if < 1.5 Value=1 if ≥ 1.5	Generic or re-deployable assets Specific assets
Relationship length	Value=0 if < 24 Value=1 if ≥ 24	Low time span of SC relationship High time span of SC relationship
Market concentration	Value=0 if < 75 Value=1 if ≥ 75	Low market concentration in the SC High market concentration in the SC
Activities coordination	Value=0 if < 3.5 Value=1 if ≥ 3.5	Uncoordinated activities with the SC Coordinated activities with the SC
Investment coordination	Value=0 if < 3.5 Value=1 if ≥ 3.5	Uncoordinated investments with the SC Coordinated investments with the SC
Hierarchies	Value=0 Value=1 Value=2	Disintegrated authorities between SC partners Integrated authorities for skills and capabilities building between SC partners Integrated authorities for control over all activities between SC partners
Ownership	Value=0 if < 1 Value=1 if ≥ 1	Disintegrated ownership between SC partners Integrated (unified) ownership between SC partners

mvQCA: model results

mvQCA: evaluation and interpretation of model results

Governing and structuring security-based managerial systems

The governance structures that contributed to building up security-based managerial systems were: 1) vertical integration in the form of hierarchies controlling all the operations of the supply chain parties; 2) asymmetric power in combination with lack of coordination of activities between supply chain partners; and 3) (bilateral or unilateral) dependency relationships, characterised by long term relationships and high market concentration of the firms in the supply chain (Figure 33, p.263).

Hence security-based managerial systems require either vertical integration (SC3ET), asymmetric power between firms (SC2D and SC3T), or dependency relationships (SC1E, SC4ET, SC5D and SC5E). Among all the causal conditions, there is only one that is individually sufficient to build up the capability, which is the presence of hierarchies (SC2E&T), as it is shown in results in Figure 33, p.263, the rest of the governance structures constructs are combined with at least another one, which means that the rest of the causal conditions are sufficient only in combination with others. These governance structures suggest strong intervention and control of the processes across firms in the supply chain, rather than freedom of choice among SC partners.

Table 6.3.2.2: Governance and structure configurations of capability building*

Capabilities	**Causal configurations**[1]
Managerial systems (MS)[1]	Hierarchies(2)$_s$+[PowerAsymmetry(0,2)*CoordActivities(0)]$_s$+[RelationshipLength(1)*Concentration(1)]$_s$ *(SC2ET)* + *(SC2D, SC3T)* + *(SC1E, SC4ET, SC5D+SC5E)*
Desorptive capacity (DC)	[RelationshipLength(0)*Hierarchies(1)]$_s$+[CoorInvest(1)*Ownership(0)]$_s$ *(SC3D, SC3E)* + *(SC2D, SC4D, SC5E)* [CoorInvest(1)*Hierarchies(1)]$_s$ + [Hierarchies(1)*Ownership(1)]$_s$ *(SC3D, SC3E)*
Vertical alignment (VA)	[PowerAsymmetry(0,2)*CoordActivities(0)]$_s$ + [PowerAsymmetry(1,2)*AssetSpecificity(1)]$_s$ *(SC2D, SC3T)* + *(SC4ET, SC5E)* [AssetSpecificity(1)*RelationshipLength(1)]$_s$ + [AssetSpecificity(1)*Hierarchies(0)]$_s$ *(SC4ET, SC5E)* + *(SC4ET, SC5E)*
MS ^ DC; and DC ^ VA	[CoordActivities(0)*CoordInvest(1)]$_s$ *(SC4ET, SC5E)*

*The model was run with Tosmana 1.301(Cronqvist, 2009). Minimise =1, Including=C(Contradictions)+R(Reminders).

[1] Hierarchies (2)= Integrated authorities for control over all activities between SC partners. PowerAsymmetry (0,2)=(Power concentrated in the supply chain partner for SC2D, and Power concentrated in the firm SC3T). The values of all the causal conditions are given in (Table 6.3.2.1, p.260).

Subscripts: s=Sufficient condition; n=Necessary condition; ns=Necessary and sufficient conditions; no subscript indicates that the condition is neither necessary nor sufficient.

+ in the model results denotes 'or', in set theory represents 'Union'.

* in the model results denotes 'and', in set theory represents 'Intersection'.

Figure 33: Governance structures for security-based managerial systems

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds	
PowerAsymmetry	3.5	6.5
AssetSpecificity	1.5	
Relationshiplenght	24	
Concentration	75	
CoordActivities	3.5	
CoorInvest	3.5	
Hierarchies	--	
Ownership	1	

Truth Table:
v1: PowerAsymmetry v2: AssetSpecificity
v3: Relationshiplenght v4: Concentration
v5: CoordActivities v6: CoorInvest
v7: Hierarchies v8: Ownership
O: mansys id: firm

v1	v2	v3	v4	v5	v6	v7	v8	O	id
1	0	0	0	0	0	0	0	0	SC15T
1	0	0	1	0	0	0	0	0	SC1D
0	0	1	1	1	0	1	0	1	SC1E
0	0	0	0	0	1	0	0	1	SC2D
0	0	0	0	1	1	2	1	1	SC2ET
0	0	0	0	1	1	1	1	0	SC3D
0	1	0	1	1	1	1	1	0	SC3E
2	0	0	0	0	0	0	0	1	SC3T
2	0	1	0	1	1	0	0	0	SC4D
2	1	1	1	1	1	0	1	1	SC4ET
1	0	1	1	0	0	0	1	1	SC5D
1	1	1	1	0	1	0	0	1	SC5E

Result: (all)
Hierarchies{2}+ PowerAsymmetry{0,2}CoordActivities{0}+ Relationshiplenght{1}Concentration{1}
(SC2ET) (SC2D+SC3T) (SC1E+SC4ET+SC5D+SC5E)
Created with Tosmana Version 1.301

Governing and structuring desorptive capacity

Conversely, building up desorptive capacity is free of issues of dependency relationships and asymmetric power in the supply chain. This does not mean that there is a need for the absence of governance of the supply chain, but that upon integration and/or coordination the governance fashion does not make a difference whatsoever (Figure 34, p.265).

Building up desorptive capacity certainly requires coordinated and integrated structures in the supply chain (SC3D and SC3E). Yet there are cases where vertical disintegration is a condition for desorptive capacity, as long as there are coordinated investments between supply chain partners (SC2D, SC4D and SC5E).

There are also governance structures that require the presence of hierarchies structuring the development of skills and capabilities across supply chain partners; however, this will only contribute to desorptive capacity building if the relationship is relatively new, or if the firms are independent from each other. So firms may still be able to build up the capability in the initial stages when they are still freely adapting to one another (SC3D and SC3E).

Figure 34: Governance structures for security-based desorptive capacity

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds	
PowerAsymmetry	3.5	6.5
AssetSpecificity	1.5	
Relationshiplenght	24	
Concentration	75	
CoordActivities	3.5	
CoorInvest	3.5	
Hierarchies	--	
Ownership	1	

Truth Table:

v1:	PowerAsymmetry		v2:	AssetSpecificity	
v3:	Relationshiplenght		v4:	Concentration	
v5:	CoordActivities		v6:	CoorInvest	
v7:	Hierarchies		v8:	Ownership	
O:	supdev	id:	firm		

v1	v2	v3	v4	v5	v6	v7	v8	O	id
1	0	0	0	0	0	0	0	0	SC15T
1	0	0	1	0	0	0	0	0	SC1D
0	0	1	1	1	0	1	0	0	SC1E
0	0	0	0	0	1	0	0	1	SC2D
0	0	0	0	1	1	2	1	0	SC2ET
0	0	0	0	1	1	1	1	1	SC3D
0	1	0	1	1	1	1	1	1	SC3E
2	0	0	0	0	0	0	0	0	SC3T
2	0	1	0	1	1	0	0	1	SC4D
2	1	1	1	1	1	0	1	0	SC4ET
1	0	1	1	0	0	0	1	0	SC5D
1	1	1	1	0	1	0	0	1	SC5E

Result: (all)

Relationshiplenght{0}Hierarchies{1} + CoorInvest{1}Ownership{0}
(SC3D+SC3E) (SC2D+SC4D+SC5E)

CoorInvest{1}Hierarchies{1}+ Hierarchies{1}Ownership{1}
(SC3D+SC3E) (SC3D+SC3E)

Created with Tosmana Version 1.301

Governing and structuring vertical alignments

Vertical alignment seems to be favoured by presence of dependent relationships among supply chain partners (See Figure 35, p.267).

There are various governance structures under which vertical alignments may evolve. The first causal configuration seems to support the idea that synergies and coordinated activities for SC2D and SC3T are not required. Vertical alignments occurred under vertically uncoordinated relations and unilateral decision-making. The firm SC2D reported that the exporter had the power to decide what SC2D should comply with; whilst SC3T reported that the power was retained in-house.

However, the firm SC2D and its partner SC2E&T reported that their power was not held within their own firms, but by their partners. Similarly, the firm SC3T reported that they had the capacity to set the norms and regulations for their supply chain, which they only had a one-year relationship with. On the other hand, SC3E and SC3D reported that the power was held by their partners, and not by SC3T. This suggests that these firms have more symmetric power than they perceive.

Therefore it seems that these supply chains (SC2 and SC3) do not have a clear idea as to who sets the norms and regulates the supply chain, and the extent to which these norms and regulations are binding. It appears to be more the case that a supply chain partner may issue a recommendation that could benefit their security capabilities and resources for compliance; the firm may then believe it is a binding norm, and will adapt their processes and systems accordingly. However, because there is not a binding norm, there are hardly any timeframes or control mechanisms to support the transformation of the firm's processes and systems; hence, there are no coordinated transformations of the firm's capabilities according to the supply chain partner's capabilities; nonetheless ad-hoc vertical alignments may still happen.

Another causal configuration suggests that regardless of the structure of the chain, it is sufficient to be in a dependent relationship (SC4E&T and SC5E: asset specificity=1), no matter if that dependency is bilateral (SC4E&T=power asymmetry=1) or unilateral (SC5E: power asymmetry=2). As expected, it seems that firms who build up specific assets are able to align better vertically to their partner's evolving capabilities.

Furthermore, according to the final causal configuration, hierarchical controls are not necessary for dependency to favour the presence of vertical alignments (SC4E&T and SC5E), which supports the notion of issuing recommendations by supply chain partners rather than forcing or structuring transformations along the chains.

All in all, vertical alignments will evolve eventually within the firm, as long as there is a need expressed by the supply chain partner.

Figure 35: Governance structures for security-based vertical alignments

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds	
PowerAsymmetry	3.5	6.5
AssetSpecificity	1.5	
Relationshiplenght	24	
Concentration	75	
CoordActivities	3.5	
CoorInvest	3.5	
Hierarchies	--	
Ownership	1	
Dependency	0	

Truth Table:
v1: PowerAsymmetry v2: AssetSpecificity
v3: Relationshiplenght v4: Concentration
v5: CoordActivities v6: CoorInvest
v7: Hierarchies v8: Ownership
O: align id: firm

v1	v2	v3	v4	v5	v6	v7	v8	O	id
1	0	0	0	0	0	0	0	0	SC15T
1	0	0	1	0	0	0	0	0	SC1D
0	0	1	1	1	0	1	0	0	SC1E
0	0	0	0	0	1	0	0	1	SC2D
0	0	0	0	1	1	2	1	0	SC2ET
0	0	0	0	1	1	1	1	0	SC3D
0	1	0	1	1	1	1	1	0	SC3E
2	0	0	0	0	0	0	0	1	SC3T
2	0	1	0	1	1	0	0	0	SC4D
2	1	1	1	1	1	0	1	1	SC4ET
1	0	1	1	0	0	0	1	0	SC5D
1	1	1	1	0	1	0	0	1	SC5E

Result: (all)
PowerAsymmetry{0,2}CoordActivities{0} + PowerAsymmetry{1,2}AssetSpecificity{1}
(SC2D+SC3T) (SC4ET+SC5E)

AssetSpecificity{1}Relationshiplenght{1} + AssetSpecificity{1}Hierarchies{0}
(SC4ET+SC5E) (SC4ET+SC5E)

Created with Tosmana Version 1.301

Governing and structuring managerial systems and desorptive capacity, and desorptive capacity and vertical alignment

The previous analysis aimed to identify the governance structures favouring the individual capability building, whereas the present analysis is specifically intended to identify the conditions for capabilities building for high compliance which we have identified as involving paired capabilities, i.e. managerial systems and desorptive capacity, and desorptive capacity and vertical alignment. Although these two paired capabilities are different, they were present in the same sets of firms (SC2D and SC5E). Therefore, the governance structures will be the same for the configuration consisting of managerial systems and desorptive capacity, and desorptive capacity and vertical alignment. Consequently, the analysis is primarily run to identify the governance structures favouring either capability building configuration.

Additionally, the analysis is run in three phases identifying: 1) the governance conditions for compliance capabilities, 2) structural conditions for compliance capabilities, and 3) the governance structures conditions for high compliance capabilities (i.e. managerial systems and desorptive capacity, and desorptive capacity and vertical alignments).

Firstly, the governance conditions for high compliance capabilities building show that bilateral dependency (power asymmetry=1 and asset specificity=1) (SC5E) is sufficient for building up high compliance capabilities. Alternatively, high compliance capabilities are also built under independent governance relationships, with generic or re-deployable assets (asset specificity=0) and with low market concentration of the firm (market concentration=0) (SC2D). Interestingly, this points towards loose supply chain relations, characteristic of market transactions (See Figure 36, p.269).

Figure 36: Governance conditions for security-based compliance capabilities

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds	
PowerAsymmetry	3.5	6.5
AssetSpecificity	0	
Relationshiplenght	24	
Concentration	25	75
CoordActivities	3.5	

Truth Table:
v1: PowerAsymmetry v2: AssetSpecificity
v3: Relationshiplenght v4: Concentration
O: ManagerialSystems and SupplierDevelopment; SupplierDevelopment and Alignment
id: firm

v1	v2	v3	v4	O	id
1	0	0	1	0	SC15T
1	0	0	2	0	SC1D
0	1	1	2	0	SC1E
0	0	0	0	1	SC2D
0	0	0	1	0	SC2ET
0	1	0	0	0	SC3D
0	1	0	2	0	SC3E
2	1	0	0	0	SC3T
2	1	1	1	0	SC4D
2	1	1	2	0	SC4ET
1	0	1	2	0	SC5D
1	1	1	2	1	SC5E

Result: (all)
PowerAsymmetry{1}AssetSpecificity{1}+ AssetSpecificity{0}Concentration{0}
(SC5E) (SC2D)
Created with Tosmana Version 1.301

Secondly, the structural conditions suggest that rather than vertical integration, coordination in the form of investment mechanisms (coordinated investments=1) may sustain high compliance capabilities. It is also necessary that firms 'do not' coordinate skills and capabilities building between them (coordinated activities=0), in order to set the structural conditions for high compliance capabilities (SC2D and SC5E). It seems that skills and capabilities coordination may divert the efficient investment coordination across firms, which sets the conditions for more relevant or valuable high compliance capabilities (See Figure 37, p.270).

Figure 37: Structural conditions for security-based compliance capabilities

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds
CoordActivities	3.5
CoorInvest	3.5
Hierarchies	--
Ownership	1

Truth Table:
v1: CoordActivities v2: CoorInvest
v3: Hierarchies v4: Ownership
O: ManagerialSystems and SupplierDevelopment, SupplierDevelopment and Alignment
id: firm

v1	v2	v3	v4	O	id
0	0	0	0	0	SC15T,SC1D,SC3T
1	0	1	0	0	SC1E
0	1	0	0	1	SC2D,SC5E
1	1	2	1	0	SC2ET
1	1	1	1	0	SC3D,SC3E
1	1	0	0	0	SC4D
1	1	0	1	0	SC4ET
0	0	0	1	0	SC5D

Result: (all)
CoordActivities{0}CoorInvest{1}
(SC2D,SC5E)
Created with Tosmana Version 1.301

The individual assessment of governance and of structures showed that no matter the integration type of the supply chain, firms needed to operate in a coordinated fashion (Figure 37, p.270) and a bilaterally dependent manner, if not independently (Figure 36, p.269).

However, the integrated analysis of the governance and structures is consistent with the structure analysis. This means that high compliance capabilities will emerge from the vertical coordinating of investments, and not from forcing the development of capabilities across firms (SC2D and SC5E) (Figure 38, p.271). Henceforth, vertical integration or hierarchical control over the supply chain may not be supportive of high compliance capabilities.

Figure 38: Governance structures for security-based compliance capabilities

Tosmana Report
Algorithm: Graph-based Agent
Settings:
Minimizing Value 1
including C R
Variable Settings:

Name	Thresholds	
PowerAsymmetry	3.5	6.5
AssetSpecificity	1.5	
Relationshiplenght	24	
Concentration	75	
CoordActivities	3.5	
CoorInvest	3.5	
Hierarchies	--	
Ownership	1	

Truth Table:
v1: PowerAsymmetry v2: AssetSpecificity
v3: Relationshiplenght v4: Concentration
v5: CoordActivities v6: CoorInvest
v7: Hierarchies v8: Ownership
O: Managerial Systems and DesorptiveCapacity, DesorptiveCapacity and Alignment;
id: firm

v1	v2	v3	v4	v5	v6	v7	v8	O	id
1	0	0	0	0	0	0	0	0	SC15T
1	0	0	1	0	0	0	0	0	SC1D
0	0	1	1	1	0	1	0	0	SC1E
0	0	0	0	0	1	0	0	1	SC2D
0	0	0	0	1	1	2	1	0	SC2ET
0	0	0	0	1	1	1	1	0	SC3D
0	1	0	1	1	1	1	1	0	SC3E
2	0	0	0	0	0	0	0	0	SC3T
2	0	1	0	1	1	0	0	0	SC4D
2	1	1	1	1	1	0	1	0	SC4ET
1	0	1	1	0	0	0	1	0	SC5D
1	1	1	1	0	1	0	0	1	SC5E

Result: (all)
CoordActivities{0}CoorInvest{1}
(SC2D+SC5E)
Created with Tosmana Version 1.301

In other words, there is more need of investment coordination mechanisms with collaborative and cooperative (self-regulated), rather than integrated or governed (enforced), capabilities and resources development across firms in the supply chains.

mvQCA: governance structures for compliance capabilities, remarks and conclusions

The previous analysis may be summarised as follows. Building up managerial systems (internal knowledge) requires strong control mechanisms and interventions through asymmetric, dependent, integrated and uncoordinated supply chains. The development of desorptive capacity (external knowledge: learning internally, transferring knowledge to the suppliers for their exploitation by the suppliers/clients) requires mainly vertical integration or vertical coordination. The vertical alignments, on the other hand (external knowledge: learning together, exploiting it internally), require loose structures, but dependency based upon developing specific assets to the supply chain. This means that internal knowledge requires supply chain control and integration, external knowledge for external exploitation requires supply chain integration and coordination, and external knowledge for internal transformations requires supply chain specific assets.

In conclusion, it seems that internal transformations relate to supply chain governance mechanisms to controls the supply chain partners, such the case of SC2E&T with its overarching hierarchies over the export and the transportation, or the asymmetric power that the supply chain partners have over SC3T (see Figure 33, p.263), whilst external transformations relate to supply chain structural mechanisms, such the cases SC2D, SC4D, SC5E, which based their supply chain relationship more on investment coordination and not much hierarchies (see Figure 34, p.265). Clearly, these results should be seen in light of the small sample size, thus the need to corroborate this result with more empirical investigations.

Going back to hypothesis 3a, it was suggested that a transition from basic to sophisticated capabilities would be associated to: 1) increased controls or asymmetric power, 2) increased bilateral dependency, 3) increased coordination, and 4) increased integration. However, we found that moving from basic (managerial systems) to intermediate (desorptive capacity) and advanced (vertical alignment, and desorptive capacity and vertical alignment), the only consistent pattern was in increasing coordination, whilst we found the opposite trend for control and power asymmetry, and for dependency and integration we found no patterns. Hence, overall hypothesis 3a was rejected by our cases.

Yet, elaborating on the only construct that supported hypothesis 3a, we suggest that high compliance requires capability building to be supported by supply chain structural mechanisms, vertical coordination. Hence, compliance capability building is reinforced by: 1) establishment of synergies between projects; 2) sharing firms' investment plans; 3) parallel, alternating, and interacting investments across units between firms; and 4) exchanging loans and financial supports between supply chain partners.

All in all, the importance of these results lies not in the 'enabling' but in the 'non-enabling' conditions for high compliance capabilities, such as: governance and integration. Hence, regardless of the dependency of the supply chain, the power asymmetries, the degrees of vertical integration, what matters is whether the supply chain investments are vertically coordinated, and that capability building is not constrained into a supply chain programme, but it is allowed to evolve at the supply chain will.

7. CHAPTER 7 Discussion of results

This chapter proposes a way to use the Resource-Based View to understand how capabilities, driven by regulations rather than market norms, are built. The structure of the discussion follows the research questions stated in the methodological chapter. Firstly, it addresses the organisational processes that firms follow in relation to their compliance, inferring that rather than a single 'compliance model' there are multiple 'pathways to compliance'.

Secondly, it addresses capability building and resource development, and how their value is leveraged, showing that rather than 'cumulative capabilities models' (i.e. basic, intermediate or advanced), we may see multiple trajectories, and that different values may be associated with each one of them. A key element addressed here is how resources and capabilities are leveraged to bring benefits for complying firms. In this section, the traditional view of resources and capabilities is revisited. It argues that firms create value when they find, build and exploit meaningful capabilities configurations, in light of the consumer's (regulator's) needs, rather than simply accumulating capabilities and resources.

Thirdly, it addresses supply chain governance structures and the role of supply chain integration and coordination in the compliance-capabilities building processes. It shows the benefits of measuring integration and coordination separately, so that coordination may be identified as the key driver of higher compliance. This connects the discussion back to the issue of the value of resources and capabilities, and suggests that competitive advantage may come from long term supply chain relationships, and also from realising the value of security resources and capabilities of the firms involved as quickly as possible. Value emerges here from the appropriation of regulatory benefits and risk reductions that come from compliance.

7.1. Business regulation and the compliance process

This section discusses the complexity of the compliance processes to highlight that understanding compliance (and its absence) requires paying attention to the role of capability building, rather than just 'willingness', which has been the main focus in previous regulatory studies. Thus, the argument suggests that responsive and 'really responsive' regulation scholars may benefit by deepening the analysis of willingness and capabilities as causes of compliance and noncompliance by moving from just organisational theories to include the RBV, in other words, paying attention to the firms' resources and capabilities building. Such distinctions may also inform regulators seeking to develop and implement better regulations.

This may enable regulators to show in which cases noncompliance is the result of lack of willingness, or lack of capabilities, and the processes by which firms may be incentivised to comply from either starting point, firms' unwillingness or incapability. Further, although this discussion derives mainly from an impact assessment of a public-private regulatory partnership (i.e. CTPAT), we previously explained that it was not possible to find cases exclusively complying with PPPs, Public, and Private regimes. Hence, this discussion may, in theory, have similar implications for public and private social regulations, since our cases have not only built up security resources in response to CTPAT, but also in response to other regulations independently, i.e. to public and their self-regulations.

As mentioned beforehand, the notion of compliance processes was introduced by Sproull (1981), enriched by French *et al.* (1992), and furthered by Henson and Heasman (1998). This investigation conducted an empirical investigation to identify the causal conditions of conformance and compliance[103], which are typically implicit, but more often neglected in empirical regulatory studies.

In general, the results show heterogeneous processes (Table 6.1.1.6, p.211), yet with distinctive behavioural patterns of compliance and non-compliance (See Table 6.1.2.1, p.215). More specifically, there were distinctive compliance patterns between compliant and non-compliant firms: 1) differences in regulatory awareness, 2) differences in their compliance methods, and 3) differences between compliance leadership and delays.

[103] As explained in page 200, compliance relates to the adherence of a firm to a regulation, and conformance relates to the actual implementation and processes that meet the regulatory guidelines and standards (Gilliland & Manning, 2002, p. 322; Scharfeld, 2003, p. 11; R. Wilson, 1997, p. 48)

Differences in regulatory awareness

On the basis of the evidence gathered here, it seems that only well known, reputable and legitimate institutions can regulate firms in this context. Customs Border Protection (CBP) and the Fresh Produce Association of the Americas (FPAA) are the institutions that make firms aware of regulations. Surprisingly it was not sufficient to have CTPAT as a reference institution, given that it is the CTPAT certifying agency. A possible explanation is that CTPAT lacks sufficient enforcement and prosecution powers and needs to refer back to the CBP when potential wrongdoing by firms is identified. Consequently, it is the CBP that gets identified as the most important source of awareness for countering terrorism. These results are consistent with other regulatory studies that argue that hegemony, power and legitimacy are necessary to trigger responses from regulated parties (Braithwaite & Drahos, 2000, p. 398; Scott, 1987, p. 451).

Another explanation relates to Baldwin and Black's (2008) suggestion that complex regulatory regimes, with regulatory functions such as information, inspections, certification, and enforcement being dispersed across different sectors, can add uncertainty, confusion and interferences between the regulator and the regulated. As a result, firms may not have a clear idea as to who is demanding what, and which regulator they should be listening to (Baldwin & Black, 2008, p. 63). This may limit the possibilities regulators have to effectively drive firms towards compliance.

Interestingly, CTPAT had been a source of regulatory awareness only in the absence of industry associations' regulatory information (Figure 22, p.217), suggesting that for this public-private regulatory regime, a multiplicity of actors and duplicity of roles may make effectively changing the behaviour of firms more difficult, even after they have decided to comply.

Regulatory competition and multiple compliance processes

Previous investigations in the software, chemical and financial sectors argued that compliance with a given regulation is influenced by previous compliance processes to other regulations and by the presence of competing compliance processes (Blount, 2007; EPA, 2000, p. 10; Vlachos, 2004, p. 5).

For regulatory studies, regulatory competition is a relevant issue. In fact, Meidinger (2009) persuasively argued that governments have regained authority in recent years, yet find themselves competing with private sector safety regulatory programmes (Meidinger, 2009, p. 242). Regulatory competition is important because, to meet regulatory aims, firms require resources and capabilities that adhere to the norms (Yapp & Fairman, 2006, p. 44) at a precise time (Williams & Edge, 1996, p. 873). Thus, a regulatory regime whose compliance processes attract more resources and capabilities from the firm, is assumed to be more authoritative than other regulatory regimes not attracting as many resources and capabilities.

Our empirical results on the other hand suggest that this is not the case here. Although having multiple compliance processes simultaneously on-going does not seem to have a positive influence, it also does not seem to have a negative effect. In the implementation stage, the new security-based operations merged into the pre-existing operations of external organisations (supply chain partners mainly, i.e. SC4ET, SC5E). The learning processes for capability building and their related investments were split between the firms' and the external organisations' operations. It is therefore possible that in a mixed regulatory regime like CTPAT it may not be given that resources and capabilities are incompatible. In our cases they co-exist, and can even merge.

Therefore, conforming to PPPs seems to allow for the coexistence of multiple regulatory regimes; achieving social aims, responding to consumer needs, and reducing the burdens and discriminatory conditions as Garcia-Martinez *et al.* (2007) suggested previously for food safety standards. There must be limits to this sharing and overlapping of resources between compliance processes involving multiple regulatory regimes, but it is also possible that such limits may be mainly set by the capabilities of the firms.

Compliance leadership and delays

The results in this investigation do not seem to support the notions of first mover advantage advocated by Ashford *et al.*, (1979) and Porter and van der Linde (1995). Most of the early movers (SC5D, SC3T, SC2D and SC1E), rather than attempting to increase the resource barriers as Wernerfelt (1984) suggests, focused on understanding how to secure their facilities and supply chains through open knowledge exchange and collaborations with other stakeholders. This approach was the same with on time movers and newcomers, many of whom ended up conforming highly to CTPAT. As a result, resources and capabilities were accessed by latecomers, which implies that there were no major resources barriers, opposite to Wernerfelt's (1984) hypothesis, and that they faced intense periods of learning and capabilities upgrading, and perhaps leapfrogging.

These processes are not uncommon; Kim (2004) showed how Asian firms with low knowledge bases invested heavily in absorptive capacity building, with intense periods of continuous and discontinuous learning, eventually driving up their knowledge base (Kim, 2004, p. 348). Hence, there is a strong relationship between intensity of effort and commitment, and long-term learning and competitiveness. Yet firms may fail to comply, at least temporarily, when they miss out on a critical knowledge base.

Hence, regulatory scholars interested in delays in regulatory compliance and leadership may want to take into account the idea that, after willingness has been established, firms may depend on their knowledge base and capabilities. The research suggests two reasons why building early security resources and capabilities did not raise barriers. Firstly, CTPAT regulators do not continuously, publicly and transparently update the guidelines for compliance with CTPAT. Secondly, CTPAT does not maintain fluent bilateral communication systems to nurture and support firms' early engagement.

Hence, there may be more to non-compliance than just unwillingness to comply, or violation of the law or norms. Non-compliance is also influenced by who regulates and how, and with implementation strategies, rather than whether a firm is early, on time, or delayed. Yet regulatory studies keep focusing on issues of willingness, reluctance or attitudinal settings to explain compliance.

Capabilities: the missing link between willingness and compliance

Regulatory scholars generally consider that "non-compliance is, first of all, a violation of the law" (Lai et al., 2007, p. 539). Such violations may be due to lack of: 1) enforcement capacity, 2) rewards systems, 3) organisational expectations of regulatory benefits, or 4) adequate institutional arrangements, or management tactics opening up planning legislation to the public and stakeholders.

A step forward in the acknowledgement of the importance of competencies and capabilities in the regulatory studies was made by scholars such as Parker (2006), Nielsen and Parker (2008), and Baldwin and Black (2008).

In 2006, Parker stressed that enforcement was about regulators persuading businesspeople of the value of compliance, and regulators understanding the motivational complexities that lead to non-compliance, and learning how to improve regulation to enforce it in fair and non-stigmatising ways. For her, non-compliant behaviour leads to conflict, particularly when management is responsible, because their *willingness* (norms of compliance) does not match up to their *behaviour* due to, among other reasons, 'incompetence' (Parker, 2006, p. 610). Under such conditions, regulators fall into a "compliance trap dilemma" because they lack political and cultural support for their views. As a result, the regulator can 1) accept the firm's views, 2) enforce harder, or 3) change businesspeoples' views about the morality of their own behaviour, in order that the enforcement method is seen as legitimate, and compliance is seen as normal (Parker, 2006, p. 611).

Interestingly, in Parker's anti-cartel case study, firms were willing but not able to comply. After enforcement, the agency had broken the intrinsic motivations of the firms to comply, leading to resistance, defiance or disengagement (Parker, 2006, p. 611). Similar responses were seen in firms SC4E&T and SC4D, the supply chain that list certification, and which in non-structured interview information, suggested that they were waiting for the benefits that come from the upgrading of the traditional cross-border infrastructure to emerge, so that they can disengage from CTPAT.

Nielsen and Parker (2008) showed that firms' internal resources (such as research and development, legal knowledge, economic knowledge and technical knowledge relevant to compliance) drove compliance in Australian firms (Nielsen & Parker, 2008, pp. 330-332). It is therefore encouraging that our results resemble findings from criminologists scholars, calling for larger scale and more widespread confirmatory research of out thesis.

Baldwin and Black (2008, p. 69), drawing on institutional theories of organisations, also understand compliance in terms of firms' operating and cognitive frameworks and how resources are distributed between organisations, or what they called 'attitudinal settings'. In relation to the operative and cognitive frameworks, they describe organisational **responses** as structured strategic **actions** driven by rational and institutional pressures. However, the authors later turned responses and actions (processes) into 'cultures and understandings' (structures), which operate within regulated organisations (Baldwin & Black, 2008, p. 70). Interestingly, the authors moved from the understanding of processes to the understanding of structures, leading to a focus on 'stocks of resources' or 'attitudes' among organisations rather than the processes by which these resources and attitudes are created.

Although non-compliance may be a violation of the law, it is worth putting this into context and differentiating between firms that are unwilling to comply and those that are unable to develop the knowledge base, the resources and the capabilities needed for compliance. Moreover, because errors are normal in any learning process, firms may unwittingly follow paths that lead to non-compliance. Regulators may want to take that into account when deciding what enforcement strategy to follow, by for instance allowing self-regulations for willing firms with capabilities, incentive-based regulations for unwilling firms with capabilities, voluntary capacity building programmes for willing firms without capabilities, and incentive-based regulations and capacity building programmes for unwilling firms without capabilities; however, such conditions and the corresponding regulatory strategies are not yet clearly captured in the literature. On the other hand, it is not so easy to measure the intent which is what willingness is about. And finally, command-control regulations may ultimately be required after persuasion and capacity building are not effective for reluctant firms.

The next section discusses how capabilities acquire value in the compliance process.

7.2. Leveraging value from compliance capabilities

This section highlights the importance of interaction between internal and external sources of knowledge. The idea is that compliance may not need incremental or linear capability building processes, nor incremental injections of money as argued, for example, in regulatory studies of the value of death (Viscusi, 1995, p. 46). Instead, it is a rather complex process, with patterns of external sourcing and internal application, and patterns of internal development and external exploitation. Such complex processes derive from the heterogeneity of resources and capabilities, and from the attempts of the firm to leverage the value of compliance, which is often externally given.

Earlier sections showed how the RBV sees resources as (tangible or intangible) things and capabilities as ways (even potentially) of doing or producing things. These resources and capabilities may be complementary, or they may have their own intrinsic value.

The question being addressed here is whether the same will hold for capabilities and resources created for compliance. Eisenhardt and Martin (2000) suggest that capabilities are dynamic when they respond to changing environments, and that they can be built from many starting points both inside and outside the firm (Eisenhardt & Martin, 2000, p. 1116). In practical terms, this means that dynamic capabilities have intrinsic value that may be carried over to wherever they are applied to.

Based on this interpretation, the summary of capabilities by compliance level (Table 6.2.1.4, p. 229) suggests that at low compliance levels, the most advanced (i.e. dynamic) capabilities are only just emerging, and that they evolve, grow and multiply during the transition to higher compliance. As advanced capabilities develop, the role of more basic capabilities diminishes at higher compliance levels.

The problem with this interpretation is that it does not address the role of each type of capability in the compliance process, or the difficulties of identifying patterns of compliance-capability building. The application of qualitative comparative analysis (mvQCA) shows that desorptive capacity with vertical alignment, and desorptive capacity with managerial systems, are associated with high compliance. The remaining capabilities, although they may be present, may not be crucial (for the time being) for high compliance (See Figure 29, p.245).

So although heterogeneity is good, it is more relevant in terms of compliance to discover the patterns of capabilities building under different environmental pressures. If the value of capabilities is not intrinsic but exogenous, perhaps a firm needs capabilities configurations capable of leveraging the value of compliance for the firm, rather than a variety of capabilities. Heterogeneous capabilities therefore are, at most, preconditions to enable what are important and valuable capabilities configurations. But how can a capabilities configuration leverage value for the firm in a compliance context?

Just as technological 'mutations' are offered to the markets, which are far from random (Nelson, 1994, p. 50), capabilities mutations may be offered to regulators. The individual (and bundles of) capabilities embedded in security resources offered to CTPAT may be 'systematically selected', creating patterns of surviving capabilities and resources configurations. These configurations capture the regulatory benefits, leveraging the value of compliance by the firm.

The following sections show the patterns of capabilities and resources configurations systematically selected by CTPAT regulators.

Compliance: a transition to limited diversity of capabilities

In the present investigation, we have discovered three paths of compliance capability building relating to each compliance level or to environmental pressure, and two paths from low to middle and from middle to high compliance (Table 6.2.2.1, p.240). Initially, low compliant firms focused largely on internal capabilities. There was no sourcing of knowledge or learning from outside their own boundaries for compliance, suggesting a lack of either absorptive or exploitive capacities. But then, how do these firms progress towards compliance?

The RBV scholars Buysse and Verbeke (2003) suggested that a shift from reactive to preventive, and to compliance leadership[104] requires the engagement of a broader range of stakeholders. Their general suggestion is greater stakeholder involvement for higher compliance and conformance (Buysse & Verbeke, 2003, p. 454). However, our investigation only reflects the similar pathways from low to middle compliance, not from middle to high.

In our case, the low compliant (reactive) firms built up single capabilities that could have the potential to internally exploit the security resources (Figure 27, p.242). The pathway to middle compliance complemented internal learning sources with a broader range of sources

[104] It corresponds to a shift from low to middle and high compliance in our case.

of knowledge from stakeholders and supply chain partners (Figure 28, p.243), and we suspect that this also required higher investment. On the other hand, the pathway to high compliance required narrowing down the sources of knowledge and learning to intra firm (managerial systems) and supply chain partners (vertical alignment), whilst stakeholder support does not play a key role; hence the diversity of capabilities building is more limited than that which Buysee and Verbeke (2003) predicted for high compliance.

The pathway to high compliance consists of two configurations: 1) managerial systems and desorptive capacity, and 2) desorptive capacity and vertical alignments (Figure 29, p.245).

For the first configuration, firms developed security resources out of their own managerial systems, and later enabled their suppliers understanding and the exploitive capacity of the firm's resources. This is similar to recent findings in open innovation frameworks for information and communication technologies (see Lichtenthaler & Lichtenthaler, 2009, pp. 1321-1322).

For the second configuration, firms coordinated the development and timely deployed their security resources along their supply chains, rather than their capabilities building. Perhaps scheduling investments for security resources deployment between firms may have been the trigger for inter-firm learning and knowledge exchanges. This looks like the 'internally facing' and 'externally oriented' capabilities building theorised by von Tunzelmann and Wang (2007), for which until now little empirical evidence has been provided, and which according to the authors the dynamic interactive capabilities may be important to advance the theory of production, given that productivity of technology may lie in its ability to generate more technology (2007, p. 202). Our investigation aligns with such view, in addition to highlight that the new technology does not only generates in the firm building up the capabilities and knowledge for it, but also in their supply chain partners or stakeholders firms.

The value of capabilities and resources

A key point towards understanding compliance relates to whether the capabilities and resources are seen as valuable by the regulators. There are questions as to whether or not such value is intrinsic, whether or not the RBV falls into a tautology. Some short answers are yes, their values have been assumed intrinsic, yet the RBV is not tautological, and we provide empirical contributions to dispute the RBV tautology argument.

There are two main criticisms of the tautology of the RBV. First, not questioning what makes capabilities and resources valuable (Porter, 1991, p. 108). This has been mostly truth; however, without a clear notion of how capabilities and resources are translated into value we have a weak theory but not a tautological (self-evidentially true). Likewise, there is a criticism the RBV assumes the presence of value in resources and capabilities, making the theory tautological (truth by assumption) (Priem & Butler, 2001, p. 64). The second criticism is the lack of empirical investigations to assess the presence of value in resources and capabilities (Foss, 1998, p. 147), however, this makes it speculative, not tautological, which may not contribute to the falsification of theories. This thesis is a small empirical contribution to remove the assumptions that resources and capabilities have value intrinsically, by showing that the value depend on the ways capabilities or resources are combined to satisfy a client, in our case the client being the CTPAT regulators.

Barney (2001) responded to Priem and Butler (2001) by recalling that resources and capabilities are valuable according to the market context in which a firm operates (Barney, 2001), because it is ultimately the market that values and pays a price for the resources and capabilities.

The present investigation not only supports Barney's assertion, but also reinforces it. Here, values differ even within the same market contexts, because capabilities and resources were created for regulatory compliance, therefore the value assigned by the regulator may differ across firms competing in the same markets according to each compliance level (Table 6.2.2.1, p.240). In other words, the capabilities and resources at low compliance may be less valuable than at high compliance in the eyes of the regulators.

Foss (1998, p.146) also argues in favour of the non-tautological character of the RBV, suggesting that the value of resources and capabilities positively feed on each other, making such values not given. This investigation not only complements Foss' (1998) argument, but also provides evidence of organisational learning not always feeding security capabilities and resources creation positively, but sometimes negatively, with feedback loops in the compliance decision making processes (Figure 21, p.202). This interrelationship between capabilities and resources suggests that the value is not leveraged in individual capabilities or resources; hence, their value is not always intrinsic.

What is more, such value may actually be lost in combination with other types of capabilities and resources, or it may be valuable only in the absence of other capabilities; hence, capabilities are not always complementary, they may also be substitutes (Figure 28, p.243). Therefore, like other goods, it is not given that the value of capabilities and resources is intrinsic, complementary or substitute in nature. A reason for this may be that the value of the security capabilities and resources is assigned externally by the regulator, in an exercise of comparing against what the regulator knows about the rest of the industry's security capabilities and resources.

All in all, the possibility of intrinsic value is small, whilst the possibility of complementary and substitute value is higher. Also, although the firm may make efforts to leverage value by making capabilities and resources appealing to the regulators[105], it is the later that ultimately decides whether or not they are worthy of certification.

For instance, if the firm does not complement vertical alignments with desorptive capacity, the capabilities and their newly created resources may not yield the value as defined by CTPAT regulators (e.g. fast cross-border clearance, customs payment accounts, reduced inspections rates, and so on). The example of managerial systems is even more drastic, since removing desorptive capacity and leaving managerial systems alone may drive regulators to classify the firm as low compliant (Table 6.2.2.1, p.240).

All in all, removing the assumption that knowledge, assets, capabilities and resources are always complementary or that they always have intrinsic value, and testing for configurations (heterogeneous patterns) rather than mere diversity (heterogeneity), counters criticisms that argue the RBV to be imprecise, untested, or tautological. Even more important, it may contribute insights about how to propose better strategies to the firm to leverage value after compliance has been achieved.

In cases in which the value of such configurations requires the combination of resources and capabilities located in different firms along a supply chain, the analysis of the inter-firm

[105] In a market context, the firm invests in advertisements to appeal to consumers, and in a regulatory context the firm invests in lobbying to appeal to regulators.

relationship may be paramount, since these can regulate and govern the capability building and resources development across firms.

7.3. Supply chain relationships for capability building

The previous discussions about the compliance process and compliance capabilities showed that supply chains are determinant upon the individual firms' capacity to comply; on the one hand because the implementation strategies consist of outsourcing security measures to their supply chain partners and stakeholders without relocating those activities outside the firm, and on the other because capability building and resources allocation leads firms to source knowledge from, and enable, their supply chain partners. These strategies and patterns of capabilities building suggest that supply chain relationships play important roles, and the following section discusses the results of governance structures.

The first part of the following section discusses the results of supply chain structures, taking into account and separating the effects of integration and coordination. The second part discusses the role of the supply chain governance to attempt to understand whether asymmetric or symmetric powers in the supply chains dominate the capabilities building. It concludes with the interaction effect of the supply chain governance and structure.

Overall, it will be shown that although compliance requires relevant knowledge transfer and collective capabilities building, which should happen with selective and justified information sharing (Lamming, Caldwell, Harrison, & Phillips, 2001, p. 7), the risk of over-reliance on just one or two suppliers that may not comply with regulation (Cousins et al., 2004, p. 557) such as Supply Chain 3 and Supply Chain 4, was tackled by compliant firms (SC2D and SC5E) using collaborative strategies (Cousins et al., 2004, p. 556) (vertical coordination) rather than vertical integration.

Supply chains structure

This part of the discussion contributes to the removal of the assumption that supply chain governance structures are holistic systems, i.e. integrated or disintegrated (markets, hierarchies, and intermediate points). Considering that more detailed analysis of the supply chain relationships is needed, the discussion focuses on both integration and coordination mechanisms, and the ways in which they mediate the firms' capabilities building and resources development for compliance.

Given that firms need to at least interact with other firms to exchange and transfer knowledge for capability building, and that they are exposed to hierarchical inter-firm controls (Delmas, 1999, p. 663; Williamson, 1971, p. 113), we now turn our attention to the supply chain governance structures, which we have argued mediates such inter-firm interactions (Arshinder et al., 2008, p. 318; Frank & Henderson, 1992, p. 942; Jaspers & van den Ende, 2006, p. 819; Patnayakuni et al., 2006, p. 15; Sirmon et al., 2007, p. 277).

Following Williamson (1971), and Delmas (1999), it should be possible to predict that firms with access to knowledge from their supply chain partners possess this knowledge because they are integrated, i.e. the different organisations are owned by the same entity. If the firm is not situated in vertically integrated supply chains, for capabilities to be exchanged between organisations (because they are not marketable) the least that can happen is that the organisations engage in an alliance; this is due to a mixture of equity sharing and a lack of hierarchical control (Delmas, 1999, p. 639), or there may also be pressures to integrate the chain.

On the contrary, the Resource-Based View predicts that vertically disintegrated firms lead to heterogeneous external knowledge, which is later incorporated into the firm by means of coordination mechanisms. In these cases, Lorenzoni and Lipaparini (1999) argued that may be as a result of lowering the costs by introduction of trust and other relational capital, which may eliminate the need for the exogenous safeguards devised by Transaction Costs Theory (Lorenzoni & Lipparini, 1999, pp. 332-333). However, there is the underlying argument that trust and relational capital are cheaper than exogenous safeguards.

Similarly, the food value chain and supply chain literatures closely relate to the Resource-Based View. Even without the need of trust and social capital, they argue that global food supply requires coordination economies for competitiveness (Henson & Humphrey, 2009, p. 9) and performance (Arshinder et al., 2008, p. 317). Thus, if a firm is situated in a vertically disintegrated supply chain, then knowledge may be transferred across firms in a vertically coordinated fashion.

Although recent supply chain contributions acknowledge that coordination is a separate issue from integration (Jaspers & van den Ende, 2006, p. 821; Patnayakuni et al., 2006, p. 15; Robertson & Langlois, 1995, p. 547), there have been only a few attempts to capture their individual and interactive effects.

For instance, the literature on economies of speed, scope and scale suggests that the creation of organisations that have the capacity to coordinate and control (integration) within and between large firms is what drives economies of speed (Chandler, 1973, pp. 6-7). Yet in this analysis coordination is not independent from, but a by-product of, disintegration. The underlying assumption is that coordination follows the corporate disintegration into largely specialised subdivisions. On the contrary, a resource-based and evolutionary view argues that coordination is a by-product of integration, at least in complex systems industries (Prencipe, 2004, p. 129). These arguments seem to be concerned with deciding whether or not coordination and integration are different sides of the same coin.

A literature strain that considers coordination and integration to be two different subjects is that of the 'Global Production Networks' (GPN). Yet they are not so much concerned with the relationship with capability building, but with how coordination efficiency may lead to reduce incentives of integration, which in turn drives supply chains into disintegration (Ernst & Kim, 2002, p. 1422; Rugman, 1997, p. 183). This is the inverse causality stated by Chandler (1973, pp. 6-7). The GPN scholars seem to be more interested in issues of economic development, industrial organisation and general business transactions, than they are in the capabilities in the context of coordination and integration.

Our investigation shows the results of analysing integration and coordination individually, and their interaction effects on capability building.

The main result is that capability building among supply chain partners may not require full integration of the supply chain, merely coordination (Table 6.3.2.2, p.262). The implication is that integration does not follow coordination, and that coordination does not follow integration. More specifically, knowledge exchange between supply chain partners may occur on an ad-hoc basis, and investments need to be coordinated between the firms for the development and deployment of security resources (Figure 37, p.270). What we discovered is that no control (integration) over the supply chain was required, but rather a 'commitment' from the firms to 'engage' with the whole supply chain to develop and deploy their security resources in due course.

This suggests that elements of trust or relational capital, i.e. commitment and engagement, eliminate the need for the safeguards set up by the Transaction Costs theory, and therefore do not cause integration. This is similar to what Lorenzoni and Lipparini (1999) found, where relational capital drove not only increased coordination among supply chain partners, but also disintegration (Lorenzoni & Lipparini, 1999, pp. 332-333). In fact, their findings are closely related to Chandler's predictions (1973, pp. 6-7), which state that disintegration is associated with coordination. Our results, on the other hand, support the relationship between relational capital and coordination, but not of relational capital and integration in the supply chain.

Furthermore, our results showed that firms with high compliance did not coordinate their skills and capabilities development with their supply chain partners (Figure 38, p.271). This seems contradictory in light of the presence of vertical alignment and desorptive capacity for high compliance (Figure 29, p.245), and of outsourcing and merging strategies with stakeholders and supply chain partners in the sixth stage of the compliance processes (p.221 and Table 6.1.2.1, p.215). Nevertheless, it does not mean that firms did not interact for the purposes of knowledge exchange and exploitation at all, or that they did not use informal inter-firms skills and capability-building. In fact, the very presence of vertical alignment and desorptive capacity is evidence of informal coordination mechanisms[106]. These mechanisms are not unusual; Baden-Fuller & Winter (2005) have shown that through trial and error and experience, successful principles (e.g. guidelines and good practices) may be reproduced to enable organisational change and learning (Baden-Fuller & Winter, 2005, p. 52).

Moreover, our results suggest that learning and knowledge exchange between supply chain partners required close collaboration, commitment and engagement. These informal exchanges and knowledge flows may occur via either trial and error or design-implement

---

[106] The results may represent coordination mechanisms such as: 1) systems (synergies between projects), 2) roadmaps (information) sharing, 3) joint planning, 4) exchange of human resources, and 5) shared teams. On the other hand, stakeholder support, desorptive capacity and vertical alignment may imply more informal coordination mechanisms.

strategies, but these are not formalised between firms. What we seem to have here are evolutionary and unplanned processes.

Hence formal coordination mechanisms cannot precede capability building, but may precede resources development and deployment. No specific resources need to be in the minds of the compliance managers to collaborate with partners, only the intention to discover the potentials of their capabilities[107]. Once a potential security resource is in the pipeline, investment coordination may take place for the relevant development and deployment of resources. This is important in more general terms, because such discoveries for compliance with CTPAT may bring about ancillary benefits, which is not unusual in regulatory compliance (Ashford et al., 1979, p. 179).

All in all, our results suggest that regulators tend to select firms with security resources developed after vertical alignments and desorptive capacity, or managerial systems and desorptive capacity. Hence regulators are an important part of the 'selection environments' (Nelson & Winter, 1975, p. 340), and supply chain structures are 'selected systems' throughout certifications. Therefore regulators may be driving the informal coordination for compliance capabilities building and formal coordination for resources development, whilst integration or disintegration remains unaffected.

The following section presents a discussion about how supply chain structures are governed.

Supply chain governance structures

The previous section demonstrated some of the ways in which the supply chains are governed; this section is a more comprehensive discussion of supply chain governance and structured compliance capability building.

[107] This is also consistent with the compliance process, which seems to disregard the avoiding of resources if compliance is the target.

Supply chain governance

The Resource-Based View (RBV) and Supply and Value Chain literatures state that the interaction of capabilities across firms is influenced by the ways relationships between them are governed. Two important elements of such governance are dependency and power asymmetry in the relationships (Cousins, 2002, p. 79; Gereffi et al., 2005, p. 88; Monteverde & Teece, 1982, p. 324; Strange, 2009; Teece, 1986, p. 289).

This investigation identified 10 combinations of supply chain governance (Table 6.3.1.2, p.253). For instance, there is unilateral dependency (Supply Chain 1, 3 and 4), bilateral dependency (Supply Chain 5) and independent (Supply Chain 2) relationships (Table 6.3.1.2, p.253). There are also relationships with symmetric power (Supply Chain 5) and asymmetric power (Supply Chain 1).

Unlike previous studies, our investigation did not assume that a dependent firm has less power in the relationship. A firm may be mainly fitted for transactions with a given partner, but such a partner may also have transactions with several other firms, which indicates that the firm is dependent on the partner, but not the other way around. But this not to say that dependent firms are also norm takers and those independent firms are norm setters.

For instance, an exporter (SC2ET) may be independent from a distributor (SC2D), because the volume of produce traded through said distributor is less than the median of the rest of the surveyed firms. Their relationship length is also expected to be less than that expected in the rest of the cases. Finally, because their operations are not specific enough to trade only with the distributor (SC2D), they can switch with relatively ease compared to the rest of the cases under investigation. Yet the exporter (SC2ET) reports that it may find itself taking the norms and standards set by the distributor.

Similarly, an exporter (SC4E&T) may be dependent, because 100% of its transactions are through a single distributor (SC4D). Their relationship length is expected to be the maximum possible, which acts as a deterrent to switch distributor, and its assets are highly specific to the operations with its distributor, which means that it is very difficult (and is therefore unlikely) to find another distributor that matches the exporters' specific operations. Yet the exporter (SC4E&T) may find itself setting the norms that its supply chain needs to follow (Table 6.3.1.1, p. 251).

Griffith and Myers (2005) explain that even discrepancies may be caused by different expectations of the supply chain partners in how to govern their relationships. Power struggles and negotiations may be at will then, and these may even translate into hybridised norms among partners in a single chain (Griffith & Myers, 2005, p. 257). Hence assuming that supply chain governance is the same across partners may negate the possibility that power asymmetry and struggles for compliance capability building exist, and this is an assumption difficult to sustain, in this investigation at least.

Our analyses, rather than focusing on one or the other elements of governance, i.e. dependency or power asymmetry, look at both, independently and interactively.

Compliance capability building may occur either way: 1) with bilateral dependency and symmetric power relations, or 2) with independent and asymmetric power relations (Figure 36, p.269).

The first type of governance, bilateral dependency, is similar to other studies' results. Intense exchanges of knowledge and complementary assets between the firms may lock both parties into the relationship (Cousins, 2002, p. 79; Monteverde & Teece, 1982, p. 324; Strange, 2009; Teece, 1986, p. 289); however, our results also show that the power in such relationships is usually symmetric, so both firms (SC5E and SC5D) tend to be able to set norms for the supply chain. This may contribute to the free mobilisation of knowledge across firms' boundaries.

The second finding is more puzzling, but also more interesting. It seems to prove the opposite of the previous argument. Compliance capability was also possible between firms with lower market concentration and without specific assets (SC2D). This type of governance is similar to what the Value Chain Governance studies call market transactions. Following Gereffi, Humphrey and Sturgeon's (2005) framework, it is possible to explain that increasing firms' capabilities drives a value chain to disintegration, and that governance will be driven by market transactions (Gereffi et al., 2005, p. 87). However, our analysis also takes into account issues of power asymmetry.

Firms (SC5E) capable of setting norms and collaborating with supply chain partners may be able to build up their compliance capabilities, i.e. by first finding. But when firms are not able to set norms (SC2D), they may need to be able to shift volumes of produce transacted with different partners, as well as to re-use their assets in ways that allow them to meet the norms set by their partner. For instance, if a distributor (SC2D) with production lots from a given exporter (SC2E&T) is not able to set the norms, and the norms that the exporter (SC2E&T) sets are entirely compatible with the distributor (SC2D), then at least the distributor (SC2D) should be able to source production from other exporters. On the other hand, if the new norms set by the exporter make the distributor's current assets obsolete, the distributor may need to adapt and re-deploy part of its assets according to the needs of the new sets of norms. Part of the assets, those adapted and redeployed, may be those applicable for transactions with the exporter that has concentrated its power and adjusted its norms. The other part of the assets, that which is not adapted, remains for transaction from exporters that did not modify their norms, and which do not have power over the distributor.

All in all, capability building may need some degree of freedom, either in terms of the freedom to switch partners (market transactions or re-deployable assets) or if that is not possible, then to set norms (bilateral dependency).

Supply chain governance structure

The interaction effects of the governance structures show that vertical coordination, and more precisely investments coordination of the supply chains. Although for some scholars who advocate that dependency and power in the supply chain is main driving element for capability building (Aust, 1997; Moreno-Luzon & Lloria, 2008; Nefussi & Priolon, 1997; Patnayakuni et al., 2006; Sherman, 2004), it may be surprising that what seems more novel in our results is 'what is not there', such as power relations, dependency and integration. This is, the high compliant firms in our investigation, SC2D and SC5E, rather than forcing the capabilities development throughout in their supply chains, the capability building emerged from coordinating investments with their supply chain partners (Figure 38, p.271), thus trial and error, experience and learning, together with formal investment coordination mechanisms to deploy newly developed security resources may be driving the compliance capability building processes for the Mexican fresh produce supply chain to the United States.

So, although compliance requires relevant knowledge transfer and collective capabilities building, which should happen with selective and justified information sharing (Lamming et al., 2001, p. 7) (which in turn runs a risk of overreliance on one or two suppliers that may fail to comply (Cousins et al., 2004, p. 557) (SC3 and SC4), the strategy of compliant firms (SC2D and SC5E) seems to have tackled such risks by favouring more collaborative and flexible supply chain relationships (Cousins et al., 2004, p. 556) (vertical coordination) over vertical integration.

To meet the objective of the thesis of building up a framework to analyse compliance, The following section integrates the previous discussions on compliance processes, capability building and supply chain governance structures, as a way of meeting the objective of the thesis; explaining the behaviour of firms towards compliance and the role played by the supply chain relationships.

7.4. Compliance capability building's governance structures

In our framework, regulations, standards and norms are given; yet the framework allows for an assessment of the impact in terms of resources and capabilities building to different regulatory settings, because regulators are important parts of the selection environment of the firms (Nelson, 1994; Nelson & Winter, 1975). There are three categories to select firms according to their compliance levels: 'low' for firms not aiming for CTPAT selection; 'medium' for firms building up resources and whose application for certification is on-going or pending with the CTPAT regulator; and 'high' for firms that have been granted the certification by the CTPAT regulator (CTPAT/CBP, 2006).

After identifying the environment selecting criteria (CTPAT voluntary program), some firms may decide to adhere to the norm, and although there is a general model that firms may follow for compliance (Henson & Heasman, 1998), the process is rather complex and iterative. Nevertheless, cases of the Mexico-US fresh produce supply chains have followed some patterns of compliance. The two most important patterns were: firstly, although they are not necessarily complementary, firms complying with multiple-regulations simultaneously, without conflicting results derived from limited resources availability, perhaps because each compliance regime may yield ancillary benefits anyway (Ashford, 2001; Ashford, Ayers, & Stone, 1985; Ashford et al., 1979; Sproull, 1981). The second pattern was the need for merging resources at the same time that external knowledge is required (outsourcing) in the context of the firm's supply chain relationship, as expected (but not completely proven) by Buysse and Verbeke (2003).

The need for interaction with the supply chain as a consequence of the compliance process seems to be driving the agri-business to build up dynamic capabilities. This may be surprising considering that dynamic capabilities are usually associated with highly changeable, uncertain, but hugely valuable technologies or products (Eisenhardt & Martin, 2000; Hoopes & Madsen, 2008; Lee & Slater, 2007; Petroni, 1998; Richey, 2003; Teece et al., 1997), whilst our cases are fairly stable and certain commodities industries.

Building up these dynamic capabilities for compliance, or what we call compliance capabilities (i.e. managerial systems together with desorptive capacity, or vertical alignment together with desorptive capacity), was proven to require close intervention of their supply chain partners to source knowledge internally and externally, and to exploit it correspondingly, similar to more technologically advanced industries (Harris & Li, 2009; Lichtenthaler, 2007; Lichtenthaler & Lichtenthaler, 2009; Malhotra, Gosain, & El Sawy, 2005; Mowery, Oxley, & Silverman, 1996).

A necessary element of the compliance process was the desorptive capacity, which means supporting the capability building of the firms' partners. This implies that governance structures should condition the way these capabilities are built. However, contrary to previous investigations in which either vertically integrating, or exercising asymmetric power over the supply chain, or taking advantage of the dependency of the supply chain partners would have been suggested as the possible mechanisms to put pressures to drive compliance capability building processes of the supply chain partners (Cousins, 2002, p. 79; Delmas, 1999, p. 663; Ernst & Kim, 2002, p. 1422; Gereffi et al., 2005, p. 88; Monteverde & Teece, 1982, p. 324; Rugman, 1997, p. 183; Strange, 2009; Teece, 1986, p. 289; Williamson, 1971, p. 113), in our investigation, we found that a more promising mechanism for promoting compliance capability building processes is tighter supply chain coordination, without modifying the degree of vertical integration of the firms, i.e. ownership. This is important because, it implies less hassle than expected if supply chain compliance capabilities want to be promoted.

Similarly, recent contributions on discontinuous innovation and the role of supply chain relationships show that strategic dalliances and non-committal supply chain relationships for activities that last very short periods and which allow flexibility, agility, freedom, and rapid adaptations, are necessary for obtaining crucial technologies and competencies, reducing the need for mergers and acquisitions, or in-house capability development (Phillips et al., 2006, p. 455)[108]. Hence, firms did not need to dismantle or assemble the firm, but were able to run parallel relationships with new temporal partners, along with their already established supply chains partners.

There are similarities and differences in our results and those of Phillips, Lamming, Bessant & Noke (2006). The similarities are the presence of flexibility, adaptability and freedom for the acquisition of supply chain knowledge, without increasing integration. The differences are that the relationships parallel to their supply chain partners were not necessary, and the strong commitment to the project, i.e. compliance, led to firms developing new relationships with the same supply chain partners, without switching from long-term to short-term relationships.

A possible reason for such differences may be that compliance encourages and requires that systems be run within the supply chain stages. Consequently, it may be difficult to run parallel business relations for compliant firms when the systems need to be deployed with their long-standing supply chain partners.

All in all, CTPAT has signalled firms about the need to comply with security regulations most effectively by means of CBP enforcement officers and the Fresh Produce Association of the Americas. Firms may have followed different pathways in their compliance process; those that align vertically and desorb capacity to their supply chain partners are able to develop the security-based resources that adhere better to the CTPAT guidelines, which grants them the certification from CTPAT regulators. Such compliance capabilities are facilitated by coordinated supply chains. Therefore, although it is not clear whether or not CTPAT certification will transform the governance and integration of the supply chains with which firms are building up compliance capabilities, it is clear that CTPAT certification drives firms to commit to tighter vertical coordination mechanisms with their supply chains for compliance capability building.

[108] Although the previous study raises the question of how to differentiate between short and long terms, a possible answer may be one that depends on the sector, region and so on.

8. CHAPTER 8 Conclusions

The objective of the thesis had been to build up and use a framework to analyse firms' behaviour when they are subject to regulations, particularly regarding the way compliance occurs. The results of the analysis in this thesis generated some policy implications of the Mexico-United States fresh produce supply chains. There are also methodological implications on how to analyse business compliance with regulations when supply chains, not only the individual firms, need to be involved.

The conclusion is divided into 5 sections: 1) addressing the research questions, 2) theory and methodological implications, 3) policy implications, 4) contributions, and 5) limitations and further research.

8.1. Answering the research questions

The thesis answered three research questions, and in the process it was possible to make additional findings.

Answering research questions and hypotheses

The ***first*** set of questions tried to understand the different firms' organisational compliance processes in response to supply chain security regulations. In particular, they asked: What compliance processes do firms follow to meet regulations for the prevention of accidental and intentional contamination of food? And, do differences in the compliance processes across firms explain the differences in their compliance levels with CTPAT? This question was not followed by a hypothesis, but it was promised to be raised in these conclusions.

Based on the analysis of the results with multi value Qualitative Comparative Analysis (mvQCA), we identified firms following variegated compliance processes when trying to reach compliance with CTPAT. Although we had identified some general patterns in various stages of the compliance processes, we could not identify a compliance process model, and in fact, the mvQCA had revealed various pathways at different stages of the compliance processes. First, high compliant firms' processes appeared to be triggered by the intervention of long established and reputable institutions more than by the regulatory agency administering the regulation (CTPAT). After initial assessment by firms (low, middle and high compliant), only the highest compliant firms have shown a decision to comply and the necessary compliance capability building. Low compliant firms have been exposed to multiple sources of regulatory information, which led us to infer that duplication of sources of regulatory awareness may hinder firms' understanding of the regulatory requirements, i.e. regulatory confusion, driving firms to non-compliance.

Between the decision to comply and actually complying, there were rather complex iterative processes that low compliant firms had not been able to manage, at least not to the full. Based on the results and the mvQCA we infer that one of the reasons for it is the increasing need of supply chain partners' engagement, which was not present among low compliant firms.

Middle and high complying firms not only used their supply chain partners but also their stakeholders support. The mvQCA results showed that some operations owned and controlled by low compliant firms, in the case of middle and high compliant firms were actually outsourced (losing ownership) to their stakeholders but with the operations remaining within the firm (without lost control over them). Thus we infer that in the course from low to high compliance, firms may have to disintegrate operations as a result of investment decision makings, but retaining control over them, as a result of coordination and collaboration decision makings.

Thus, we propose the following hypothesis: the compliance processes followed by firms may not be based on a compliance model or on heterogeneity of compliance processes, but on a limited diversity of pathways, of which may include a variety or combination of regulatory clarity, engagement, supply chain and stakeholders support, strong capability building, and internal and supply chain-based compliance process auditors.

The ***second*** set of questions tried to understand how firms build up compliance capabilities and developed security resources, as well as whether compliance capabilities correlated with different compliance levels. The hypothesis was that compliance was present among firms with more advanced capabilities.

After understanding how capabilities are built based upon case studies, although a first statistical description shows a direct correlation between capabilities and compliance, the mvQCA have actually rejected this hypothesis. The mvQCA showed that high compliance may be reached either by combining basic with intermediate capabilities, or intermediate capability with advanced capabilities. An intermediate capability was used to exploit in-house resources within the facilities of their supply chain partners, desorptive capacity. Such resources were developed from their managerial systems and from the firms efforts to match their supply chain partners' capabilities.

So, we deduce that substituting basic for advanced capabilities is not a sufficient condition to reach compliance. Compliant firms 'combined capabilities' (i.e. mixed basic, intermediate and advanced) to develop resources that met better the regulatory guidelines. These two statements are against our original hypothesis, 2a. Instead, we can now infer that, building and piling up heterogeneous capabilities is only a precondition for compliance, and the right combination of capabilities bring firms closer to compliance, and a necessary condition is that in such combinations, desorptive capacity is present.

All in all, regardless of the efforts firms pay to become compliant, there are specific conditions related to compliance capabilities building, to satisfy the regulator, and the certification to be granted.

The ***third*** set of questions tried to identify the supply chain governance structures that enable firms to build up compliance capabilities, and whether difference in governance structures would explain the presence of such capabilities. The hypothesis was that firms with more integrated, coordinated, dependent and asymmetric power supply chain would be able to build up compliance capabilities.

The basic statistics did not show any pattern in this respect, while the mvQCA was able to show patterns, they were only partially supporting our hypothesis. In terms of supply chain structure, the presence of compliance capabilities was common among firms with supply chain coordination, and not with integration. In terms of supply chain governance, the presence of compliance capabilities was common among firms sufficiently interdependent from their supply chains, or having complete freedom to switch supply chain partners when these were not able to build up compliance capabilities. So far so good; however, the interaction effect of supply chain governance and structures, showed that the common feature among firms with compliance capabilities was only the high degree of supply chain coordination.

Thus, overall three of our explanatory variables (power, dependency, and integration) were not supporting our hypothesis, whilst coordination was indeed. Interestingly, this goes in line with the results in capability building processes, and in the organisational compliance processes, whereby supply chain partners engagement seem to play an important part in assessment of the compliance process, exchanging knowledge, desorpting or aligning capabilities with them, for compliance. From this we infer that, although there may be various pathways firms may follow to compliance, the ones including supply chain-based organisational processes, capabilities building, and coordination may be closer to develop the security resources worthy of certification.

Yet, taking into account that this thesis is based on a small sample, we would like to encourage further investigations for enhancing the statistical representativeness and validity of our claims. Yet, we have no reasons to believe that our cases are too dissimilar to other fresh produce supply chain firms engaged cross border transactions between Mexico and United States, as described in the background chapter.

8.2. Theoretical contributions and implications

Business regulation and compliance

During the discussion, it was shown how the smartest regulatory regimes (such as 'responsive' and 'really responsive' regulations) consider that repetitive violations should be confronted by the use of harder regulatory tools, whilst those who comply with regulations require only softer regulatory tools. Although this is not to be rejected, our investigation has shown that non-compliance may not only be a matter of willingness, but also a matter of complex compliance processes, whose paths do not necessarily lead to compliance.

In relation to understanding compliance, we have shown, for this case, that it is a complex process one requiring substantial resources and capabilities. But more importantly, although we have shown that, for some types of regulation including the case offered, there may be no such thing as a compliance model, there are still 'compliance patterns', each one of them consisting of configurations of capabilities that aid in the development resources suitable for meeting the regulatory requirements.

Thus, if compliance requires more than just willingness, it may worth including in regulatory theories different prescriptions for enforcement tools, some of which may be suitable for firms lacking the commitment, and others suitable for firms lacking the capabilities, the intention being to inform policy making about smarter ways to enable compliance.

In fact, risk regulations have been criticised along similar lines because they "tend to under emphasise the need to understand why such a non-complier is not behaving as required and to identify better regulatory responses to that non-compliance" (Baldwin & Black, 2008, p. 67).

As discussed earlier, however, the tendency of regulatory studies to use institutional approaches to explain business behaviour fixes their analyses in attitudinal settings (Baldwin & Black, 2008, p. 69), and normative and calculative aspects (Dao & Ofori, 2010; Greer & Downey, 1982, p. 491). Furthermore, when scholars have captured the importance of the firm's knowledge base, resources and capabilities (Nielsen & Parker, 2008, pp. 330-332), they have turned to the institutional prescriptions of accepting or changing the firm's moral behaviour, or enforcing regulations harder (Parker, 2006, p. 611), failing to adapt their prescriptions to the new empirical evidence.

Rather than a contribution to regulatory theories, this is a call for using different tools for enforcing compliance. More refined theories would offer institutional prescriptions for firms whose common denominators are issues of willingness and commitment; whereas for those whose common denominators are issues of competencies and capabilities, scholars may want to work more on theories for capacity building enforcement strategies.

If capabilities are important drivers of compliance regardless of the willingness of the firm or of their attitudinal settings, then regulatory prescriptions may be adapted for "incompetent firms" so that they are subject to capacity building enforcement programmes according to their compliance levels, rather than just revoking their licences. This should not be taken, however, as denying the priority of the precautionary principle in any regulatory matter.

The Resource-Based View

It was questioned in this thesis whether the RBV would benefit from measures of performance that captured not only traditional profitability indicators, but also qualitative ones, such as compliance levels to given regulatory regimes.

Many empirical investigations omit from their performance measures the regulatory compliance indicators, although they acknowledge the importance of the regulatory environment. As a consequence, it remains a major challenge to understand capabilities and resources heterogeneity from the RBV. We have shown that Value-Price-Cost differences remain high in the context of regulatory compliance in our case. The argument here is, we are failing to inform regulatory scholars about how given regulations impact firms' behaviour, and what sort of remedies (capabilities) may be suitable to drive compliance. An important message to the regulatory scholars may be that heterogeneous capabilities and resources are preconditions (starting points) in a path towards compliance, but full compliance is conditioned by the presence of valuable capabilities configurations. Hence, different regulatory strategies may need to be fitted to firms at different stages of compliance capabilities building (i.e. limited capabilities, heterogeneous capabilities, and limited diversity of capabilities), so that compliance is achieved more effectively, and with fewer economic burdens.

At the moment, the RBV is only able to communicate that regulations impact positively or negatively, falling into the same trap as regulatory studies, measuring regulation as an input and compliance as an output, rather than explaining what is happening inside the firm. Hence, regulators may not have a clear understanding as to what the relationship between guidelines/standards, certification, and compliance resources is, with the value, price and cost of capabilities.

This investigation has tried open up a new perspective on the relevance of the RBV for Regulatory Studies, translating the value, price and cost of capabilities reflecting the actions of regulators. The regulator influences the value of capabilities by its capacity to grant or deny access to markets. The 'price,' viewed in terms of the enhancement in unit revenue, or longer term supply chain relationships, or lower biosecurity risks, that such capabilities garner, is determined by the regulator's decision, as well as market conditions (other channels for output as well as the extent and nature of demand (some buyers may be unavailable reducing the thickness of the market and subjecting the seller to buyer power or to excessive competition). Finally, the cost of capability building, although potentially less overloaded by the regulator's actions, can become more risky in situations where regulators are not transparent or where regulations are very difficult to interpret and, in all cases, require the accumulation and development of resources, processes that are themselves costly and subject to learning (knowledge accumulation).

Likewise, another contribution relates to issues of values of resources and capabilities. If it is true that the values of resources and capabilities are subject to dynamic changes between the firms supply of resources and capabilities and the regulatory demand for resources and capabilities, then RBV scholars may want to investigate how such values fluctuate, rather than assuming them to be given. Some indicators may then be provided to the markets, policy makers, regulators, society and stakeholders. However, we acknowledge that it may represent important methodological challenges for the RBV.

Yet, following Nelson on technological uncertainty and systematic selection (Nelson, 1994, p. 50) in the context of the present investigation, the value of capabilities may change according to whether the security resources offered to the regulators are indeed systematically selected and certified because they adhere to the regulatory requirements. However, this systematic selection may change according to the security resources offered by the industry in the future, and even according to the dynamic targets for compliance set up by regulators (CTPAT/CBP, 2006).

All in all, although there are grounds for systematically enhancing the value of firms and supply chains' capabilities, it may be subject to their capacity to continuously re-assess resources to meet such dynamic targets, based on: 1) security resources offered by the industry, and 2) regulatory policies.

Supply chain relationships

It was shown that resources and capabilities building within the firm are mediated by the supply chain relationships. However, this investigation disaggregated the effects of structures (integration and coordination) and governance (dependency and asymmetry).

The investigation identified that firms' innovative capabilities to prevent contamination of food are based upon knowledge flows and investment coordination between supply chain partners, as has also been implied in manufacturing and environment studies (Bowen et al., 2001; Buysse & Verbeke, 2003; Lawson, Petersen, Cousins, & Handfield, 2009; Sheffi, 2001; Squire et al., 2009). Nevertheless, what is new is the key role played by the desorptive capacity (Lichtenthaler & Lichtenthaler, 2009) in comparison with the absorptive capacity (Cohen & Levinthal, 1990) or the vertical alignment (von Tunzelmann & Wang, 2007), as an innovative capability needed by the supply chain to prevent contamination of food.

The rejection of the hypothesis that ever increasing sophistication of capabilities may be associated with higher compliance levels is intriguing. It indicates that innovative compliance capabilities require iterative processes of internal exploration and exploitation of knowledge, followed by external exploration and exploitation of knowledge. In this process, the exploration within the firm consists of organisational capabilities and managerial systems building. Internal exploitation may also involve internal coordination capabilities. External exploration may involve construction of vertical alignments and stakeholders support, and external exploitation may require desorptive capacity.

Therefore, the supply chain governance structures become crucially important for explaining external explorative and exploitive capabilities.

The analysis shows that vertical coordination, and more precisely investment coordination, of the supply chains enables such exploration and exploitation across supply chain partners, as is implied by other studies (Aust, 1997; Moreno-Luzon & Lloria, 2008; Nefussi & Priolon, 1997; Patnayakuni et al., 2006; Sherman, 2004). The novel results are, however, about 'what is not there'. Power relations, dependency, and vertical integration are 'not' determinants of supply chain innovative capabilities for the development of resources to prevent contamination of the food along the chain.

However, that does not mean that the situation is static with respect to supply chain relationships. The fact that tighter investment coordination between partners is required to build up capabilities in order to prevent contamination of food along the supply chain indicates that financial, security-based resources and organisational capability building are important. Although the recourse for meeting these requirements may not be rare, they may be costly, time consuming, and ever changing. These characteristics of the compliance capability building process and the role played by the supply chain in these processes may contribute to raising the entry barriers to trans-national fresh produce supply chains.

Those findings seem to replicate results of compliance with food safety standards preventing accidental contamination in Senegal (Maertens & Swinnen, 2009), where it was found that although compliance led to poverty reduction of the international supply chains' partners, it also led to 72% of contract farmers losing their contracts with such chains (Maertens & Swinnen, 2009, p. 165).

Hence further investigations are required in order to assess more fully the economic consequences, especially if developing countries are involved in international supply chains subject to compliance with regulations preventing intentional or accidental contamination of food.

8.3. Methodological contributions, limitations and implications

This research contributes with 12 case studies, including 16 firms grouped into 5 supply chains. The 5 supply chains included three stages (exporter, transport and distributor), which is a methodological approach that, although suggested as superior to other supply chain analysis in terms of validity and rigour through triangulation of information (Seuring, 2006, pp. 246, 248), is rarely performed (Seuring, 2006, p. 237). This allowed discussions about not only intra-firm behaviour, but also supply chain interactions.

This investigation employed the RBV concerning the analysis of the values of resources and capabilities. It contributed to the understanding of intrinsic, complementary, or substitute values of resources and capabilities. This analysis was only possible thanks to the use of the Qualitative Comparative Analysis (QCA), which captures individual and interactive effects of the causal conditions of compliance. We found that the language of necessity, sufficiency, presence, and absence associated with the QCA is compatible with the notions of independent, substitute and complementary values of resources and capabilities of the RBV.

Furthermore, the mvQCA proved that it is possible to test for the presence or absence of such values, based upon qualitative indicators, thus overcoming the limitations of traditional quantitative indicators such as profitability or other market-based indicators. Hence, it is possible to capture the value in qualitative and quantitative constructs assigned by multiple actors, e.g. regulators, NGOs, consumers, customers, shareholders, stakeholders, and so on.

Although advantageous, the limitation with such an approach is the same that applies to all case studies, which is the fact that any generalisation is theoretical, and not statistical. Our selection of case studies, implies that our generalisations were applicable only to fresh produce supply chains, leaving other agri-businesses on the margins. However, there is no reason to believe that securing the standard facilities and supply chain operations of a tomatoes exporter would be too dissimilar to securing those of a cucumber exporter or of other fresh produce exporters; or to believe that securing the transport operations of the exporter would be too dissimilar if the transport had been outsourced. Furthermore, the temporal dimension was captured by asking the CEOs to indicate when resources and capabilities were developed, rather than by following a panel-like investigation, and we therefore rely entirely on the informants for our understanding as to the dynamics of the capability building.

It is proposed that further investigations seek to tackle such statistical generalisation, by designing a methodology that replicates the fuzzy qualitative comparative analysis for the identification of the causal conditions of the prevention of food contamination along international supply chains. Furthermore, it may be relevant to standardise the data-gathering instruments to apply the study in a panel-like fashion, across regions and across agri-business activities, possibly assessing different types of regulations, such as environmental, social responsibility, food standards, and so on, as this investigation has not much to say about.

Proceeding in such a way, the investigators may attain a more dynamic and comprehensive understanding of firms' and supply chains' behaviour. On the other hand, it may lower their capacity to capture the dynamics of capability building and intra and inter knowledge flows between supply chain partners, which is the benefit of narrative case studies, another key component of the analysis offered here.

Finally, this thesis contributed with a methodological procedure of splitting the sample, following the example of traditional statistical analyses like ANOVA and the use of simple control variables in any type of regression. This procedure allowed dealing with the issue of having a trichotomic dependent variable (low, middle, and high compliance), transcending the problem of dichotomous dependent variables in the use of QCA with TOSMANA.

8.4. Regulatory implications

It was suggested that product attributes are valued differently by different consumers (Ashford, 2001). Extending Ashford's proposition, from products to resources and capabilities attributes, and from consumers to regulators and other stakeholders (NGOs, Research-base, International organisations, and so on), this thesis suggests the need to re-define and better articulate the value of capabilities and resources in relation to the degree that their attributes adhere to the demand of regulators and other stakeholders, or to the degree they help to achieve better social outcomes, such as security, threat reduction, and so on.

In this sense, unless there are clear benefits (derived from certification) to compliance, the resources produced by the firms will fail to meet the expectations of the regulator. In this respect, the CTPAT indicators are not very helpful, since the average number of firms reporting tangible benefits by holding a certification (high compliance) is 19% (CTPAT/CBP, 2007, p. 46).

It is clear that such results do not adhere to previous regulatory studies propositions that when firms make an effort and achieve significant but not complete compliance, they should still be rewarded with fail-soft strategies, and with adjustable sanctions (Ashford et al., 1985, p. 463). Possibly CTPAT regulatory policy is not sending the right message to the international supply chains. Perhaps this might limit firms' willingness to comply, hence failing to build up their own technological and organisational capabilities.

Other regulatory studies (Porter & van der Linde, 1995, p. 110) suggested that regulators should not try to influence innovation. For them, one of the foundations of the relationship between regulation and innovation is that the maximum opportunity for innovation occurs when it is left to the industry, and not the standard-setting agency. However, 'bad innovation' may also emerge from industry practices. An example of this is the way "High Security Seals ISO-17712" are sometimes handled. Secondary data in this investigation showed that there is no control over the distribution of High Security Seals ISO-17712 in Mexico; consequently, intentional intrusions and contamination of food in a container may be covered up by re-sealing with another seal, which are distributed on the open market unrestrictedly, and with no record of who is acquiring them. Thus, tight complementary controls and monitoring measures are required with the use of such seals, as required by the regulatory agency, CTPAT.

Regulators have at least some degree of understanding of compliance, and of the potential of their own regulatory strategies. In our investigation we found that firms may take regulatory prescriptions as ways of concentrating the efforts of the firms during basic and intermediate capabilities building, exploiting them for securing the supply chain. Such was the case of (SC5E) who engaged in developing the resources as stated by the CTPAT guidelines, and when their capabilities were enhanced, they engaged in designing their own resources.

During the initial stages of compliance capabilities building, avoiding the exploration of new technologies may reduce the need for supply chain knowledge and capabilities, lowering their efforts, while still contributing to compliance. On the other hand, firms may also need to divert away from the suggested technologies, opening up possibilities for new technologies also capable of meeting the regulatory requirements.

Thus, it is not given that prescriptive regulations are not good for innovation, yet in some cases they may not be enough or they may not be the only regulatory strategy capable of driving innovative compliance.

A similar argument was given by Ashford (1985), who stated that regulators should have desirable technologies in mind, leaving as little room for uncertainty as possible (Ashford et al., 1985, pp. 462-463). We add that such a strategy might give flexibility to the firm to develop their technologies as soon as their capabilities evolve, which may occur before or after prescriptive technologies have been deployed within the firm and along their supply chain.

As said above, bad innovations may also derive from prescriptive regulations. An example of this is the poor use of the High Security Seals ISO-17712; also the GPS conveyance traceability technologies, which are preferred instead of cheaper methods for risk identification like tolls receipts with mobile communications (SC5), or the traditional criminal record background checks against social networks in the transport industry to establish the reliability of truck drivers (SC3T).

If the above technologies contribute to compliance and are not abnormal in the fresh produce and food industries, then regulators may want to take into account that regulatory guidelines and enforcement practices may need some flexibility, by for instance allowing self-regulations for willing firms with capabilities, incentive-based regulations for unwilling firms with capabilities, voluntary capacity building programmes for willing firms without capabilities, and incentive-based regulations and capacity building programmes for unwilling firms without capabilities. On the other hand, command-control regulations may ultimately be required after persuasion and capacity building are not effective for reluctant firms, in order to encourage product and process changes to better utilise resources, at the same time as reducing risks in the early stages of compliance, rather than just forcing end-of-pipe technologies.

8.5. STI Security Regulation and Policy implications

A principal policy implication is the potential value of developing institutional mechanisms in developing countries to stimulate the dynamic capabilities of small farmers to adapt to the fast-changing regulatory environment in terms of security, safety, sustainability, social responsibility, inclusiveness, and so on. This in turn might enable new entrants to coordinate with international supply chains; it might also enable existing firms to strategically exit given supply chains to engage with other ones, say, reorienting exports from either the US or EU to other growing global markets (e.g. BRICs or MIST economies).

Therefore if higher compliance requires desorptive capacity and vertical alignment, as our own investigation suggests, there may be two alternative policies. The first would be to retain policies that supervise compliance competition and exclusion issues within international supply chains, and allow compliance efforts to focus on a few partners, potentially excluding some farmers from global chains and raising entry barriers. The second would be to develop policy instruments to identify what supply chain stages require capacity building support, in order that they are not excluded from the international supply chains.

A number of economic policies may follow on from this second option. If one of the most important supply chain issues for capability building is the coordination of investments, as suggested by our research, then policy makers may want to devise specific financial instruments to enable less able firms, and increase their likelihood of sustaining relationships with supply chain partners based upon compliance capability building and resources development.

Equally important are Science, Technology and Innovation Policies. This investigation identified that higher compliance required intermediate and advanced capabilities for the development of security resources. If this is replicated throughout the rest of the industry then the faster the supply chain needs to comply with dynamic regulatory requirements, the faster the transfers, exchanges and flows of knowledge should occur along the supply chains, together with tighter coordination of investments between supply chain partners.

STI policy makers may wish to deploy instruments to improve such processes, especially if knowledge needs to be transferred across countries, and even more so if one of them is a developing country. Under such circumstances, the internationalisation of security STI policies may become increasingly important.

Although such internationalisation is already a reality[109], these initiatives seem to promote innovations in science and technologies that enhance the capacity of the national institutions enforcement agencies in their counter-terrorism missions. So far, at least, they have not focused on international supply chain security itself.

One example of how STI research and policy would enhance the international supply chain security is given by understanding the trade-off between security and economic impact. Moreover, it has been argued that innovation involves doing things rather differently to increase efficiency or reduce costs. This investigation identified three supply chains (SC3, SC4 and SC5) that had applied operational security procedures that met the purpose of conducting risk assessments, and that if shared with the CBP may support automated cargo inspection decision making.

These systems may be better off compared to other less cost-effective systems such as COOLTRAX and ACR SmartButton ($880 USD per container), contrary to what has been suggested elsewhere (Nganje et al., 2009), which because it lacks GPS, the classification of the cargo as low or high risk is unreliable anyway, because inspection points along highway by Mexican Department of Defence (SEDENA) cause changes in the internal trailer environments that may not necessarily mean that the cargo is of high risk. Perhaps the opposite is possible, and lower risk ratings may be assigned if the cargo can be proven to have been inspected by SEDENA with re-sealing carried out at the inspection point under the supervision of the same agency. However, since there are no international research and policy programmes, comparisons between innovative, ad-hoc, and cost-effective technologies and systems have yet to be assessed.

There is also a question as to whether SEDENA practices can be aligned with industrial interests. Even though the Mexican Presidency throughout SEDENA may seem interested in the Mexican agri-business, as shown with the elimination and modernization of inspection points, it may be more in accord with US border agencies, because even if Mexican producers may have a diminished voice in influencing these agencies their customers in the US may be more effective in having influence, and still the main concern of an agency like SEDENA is national security. This goes to the question worthy of further

[109] See, for instance the International Cooperative Programs Office (ICPO) of the Department of Homeland Security, http://www.dhs.gov/xabout/structure/gc_1246475440457.shtm.

investigation (though not here) of the tradeoffs between security and economic objectives and (further) the interaction of these tradeoffs with political processes.

Another matter is that while the regulatory policy is increasingly transferring responsibilities to the industry to engage in protecting the people, it is necessary that international security-based STI policies devise mechanisms that enable the international supply chains to meet those responsibilities.

Therefore it may be advisable to enhance the Science and Technology's Human Factors/Behavioural Science Division of US Homeland Security by including Organisational Behaviour to its remit. Although it may be implicitly included already, the US security policy would gain presence and influence by not only extending the regulatory arm to the industry thus making it accountable for protecting the population, but also by extending the policy arm as a mechanism to enable such regulatory mandate, even if it is only on a voluntary basis.

Furthermore, the International Research in Homeland Security Science and Technology Mission Areas should include among its highest priorities science, technologies and innovation needs and the organisational behaviour studies for international supply chain security. This might support the change of the traditional concept of border from 'port of entry' to a more modern approach of mutually agreed security standards that create 'a border' within which international supply chains' may comply with the highest security guidelines and the distinction is not the geopolitical boundary but organisational.

Under such new approaches, delays in the certification processes after the firm is already in compliance are neither an incentive for innovative compliance, nor for a secure border. Regulatory certification processes may be designed to grant increasing certification according to the regulatory aims being implemented. Fully visible real time upgradable certification processes may be required to incentivise firms in compliance leadership. Full knowledge of their status and cross industry benchmarking may lead firms to undertake greater efforts for compliance, or to focus their resource allocation and capabilities on other compliance processes.

An important incentive for compliance with CTPAT is the use of the FAST lanes. However, secondary interview data shows that there are industry initiatives promoting the enhancement of the capacity of cross-border operations. This will promote faster clearance of trucks in cross-border operations, even in those that are not complying with CTPAT. This sends a message to the industry that using CTPAT/FAST may not be as important as increasing industry investments in the US and Mexican borders infrastructure to release cargo faster. Hence the acknowledgement of the trade-offs between cross-border infrastructure and CTPAT compliance for access to FAST Lanes is a matter that the US and Mexico may want to prioritise; they need to make a decision about whether to enhance security at the port of entry, or over the entire supply chain, and this is a decision that has to be made between traditional and modern views of security policies.

Currently there are approximately 250,000 trucks using the Nogales port of entry, against a total of 6000 firms certified in the US and Mexico. Assuming that the number of certified firms in Mexico increases, the number of cross-border operations may increase using FAST lanes; the pressure on the two FAST lanes may cause bottlenecks, reducing the current pressure of the normal lanes. Opening new normal lanes may release around 30% of the pressure, which would be equivalent to allowing around 70,000 operations without the need to implement any security measures[110]. Interestingly, this suggests a conflict between security regulations and the security policy of the Department of Homeland Security.

These policy recommendations attempt to bring new issues to the attention of homeland security and national security policy makers. They stress potential incompatibility between national security policy and homeland security, which may endanger the engagement of the supply chain in the wider aim of securing the food supply.

[110] The Arizona Department of Transportation (ADOT) is constructing two additional commercial vehicle lanes at the Mariposa Port of Entry (POE). These new lanes will be on the east side of the existing lanes to accommodate commercial traffic during peak flows. A fourth Super Booth for primary inspection will be added. The two existing commercial lanes will be designated as FAST lanes, although the design allows maximum flexibility to shift trucks among the four lanes according to demand. The design also facilitates the safe movement of oversize and HAZMAT loads. Status: Construction $4.19 Million. The federal compound will be totally redesigned: the existing passenger vehicle building and most of the commercial vehicle facilities will be replaced. The initial phase contemplates six passenger vehicle lanes (expandable to 12); four pre-primary lanes for commercial vehicles (expandable to six); six primary inspection booths for commercial vehicles (expandable to 10); 50 commercial docks (expandable to 100), of which 25 will be enclosed for climate control; a new export dock including auto export facilities; bus loading, unloading and inspection areas; an area for four X-ray or VACIS (gamma ray) inspection machines; and a new commercial building. Status: Design. $95 Million (www.bip.arizona.edu

Hence it is necessary to analyse the trade-offs between international security-based regulatory regimes and national security policies, at a time when allocation of public and private resources is dedicated to regulatory compliance and security policies.

This policy recommendation tries to call the attention of homeland security and national security policy makers to the potential incompatibility between the international security agenda to counter terrorism and attempts to improve boarder infrastructure, because of the impact of the later on firms' incentives to comply with security regulations. Hence, a question is raised about whether countering terrorism is a state or a public-private partnership responsibility. In either case, the global supply chains need to be informed in order to plan their next moves.

9. Appendices

9.1. Appendix A: Cover letter

Date:

Dear

We sincerely appreciate your precious time to assist us with this research. This PhD research related to Science and Technology Policy Studies, at SPRU, University of Sussex, United Kingdom. The purpose of this project is to understand how post 9/11 security regulations influence technological capabilities and affects global value chains governance structures.

You will receive a summary of results, but if you are interested in a full report, please indicate this, and as soon as the research is concluded and edited, it will be sent to you.

The information for the present research is to be collected from two persons in the firm. A questionnaire would be applied to one manager knowledgeable of the trajectory of the firm relationship with a particular client/supplier, and its perceptions about security measures related to post 9/11 anti-bioterrorism regulations.

An interview would be conducted to the manager responsible for securing the supply chain, to understand how security capabilities were acquired, used, changed, developed and/or made ready for commercialization.

If you wish the results to be held confidential, please state so during the questionnaire or interview, and only aggregate results will be used in the study. However not crucial financial information is required in this research, as you can check on interview and questionnaire samples attached with this letter.

As small way of saying thanks and to show you our appreciation, by completing the interview and questionnaire, you will enter into a lottery for a

$ 200 amazon.com gift certificate

Please do not hesitate contacting me at any time for questions and concerns at Private numbers +521 (662) 1400015, 2877013. Mail to CIAD, A.C., Carretera a la Victoria Km. 0.6, CP 83000, Hermosillo, Sonora, Mexico. Email: yb25@sussex.ac.uk ; yari_borbon@yahoo.com

Sincerely

Yari Borbon Galvez
PhD Researcher
Candidate number: 99486
SPRU, The Freeman Centre, University of Sussex, Brighton, East Sussex, BN1 9QE Tel: +44 (0)1273 686758 Fax: +44 (0)1273 685865

9.2. Appendix B: Interview COMCAP 2007-2008

University of Sussex
SPRU – Science & Technology Policy Research

Interview: Compliance Capability Building
along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo Nacional de Ciencia y Tecnología

Company name: ____

Respondent: ____

Job Title: ____

ANTI-BIOTERRORISM SECURITY MEASURES TECHNOLOGICAL CAPABILITIES

Please mention **WHAT HAVE THE COMPANY DONE** to acquired, use, modify, develop, or make ready for commercialization of its new operational capacity related to the new security measures.

1. 'Assessment' capabilities:

   a. Planning
   b. Diagnosing
   c. Inspecting
   d. Measuring performance
   e. Importance (relevance)

2. 'Visibility and monitoring' capabilities:

   a. Prior notice (FDA rule)
   b. Background checks
      i. Personnel
      ii. SC client/supplier
   c. Electronic manifest
   d. Records keeping
   e. Monitoring of loading and downloading
   f. Warehouse visibility
   g. Cargo condition in-transit (ripeness, biological and chemical agents in the container)
   h. Product id and tracking

3. 'Supply chain coordination and integration' capabilities:

   a. Resources and technologies (equipment, material, human, software) sharing
   b. Security investments (reduce duplication along the SC)
   c. Client/supplier involvement in SC security decision making
   d. Coordinated planning with client/supplier
   e. Skills allocation along the SC to reduce duplication of security measures.
   f. Joint setting with client/supplier of security standards
   g. Team building with client/supplier

University of Sussex
SPRU – Science & Technology Policy Research

Interview: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo nacional de Ciencia y Tecnología

4. 'Vulnerability reduction' capabilities:

a. Access control
b. Awareness
c. Smuggling and theft prevention
d. Problem solving on security breaches

5. 'Operations agility' capabilities:

a. Variability reduction on delivery time
b. Delivery (tack) time reduction
c. Delivery schedule

6. 'Learning and knowledge' capabilities:

a. In-house security research (studies)
b. Joint security research (studies) with client/supplier
c. Joint security research studies with business association
d. Interaction with higher education institutions
e. Interaction with research centers
f. Interaction with governmental agencies
g. Interaction with consultancies
h. Private certifying agencies
i. Public specialized seminars and courses.
j. Others (specify):

Thank you for your valuable time and information!

Yari Borbon-Galvez. PhD Researcher in Science and Technology Policy Studies. SPRU, University of Sussex. Yb25@sussex.ac.uk; yari_borbon@yahoo.com (MX)+521(6621) 877013, (UK)+44 07725996677

9.3. Appendix C: Questionnaire COMCAP 2007-2008

University of Sussex
SPRU Science & Technology Policy Research

Questionnaire: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo Nacional de Ciencia y Tecnología

Firm name: ____________________

Respondent: ____________________

Job Title: ____________________

SUPPLY CHAIN GOVERNANCE STRUCTURES

Creation of client-supplier relationship

Relationship Necessity

1. How did you meet your client/supplier?

2. Why did your firm establish a relationship with your client/supplier?

3. In order to initiate that relationship, did you and/or your client/supplier have to change or include new:

Dimensions (tick accordingly)	Your firm			Your client/supplier			
	Changed	New	No	Changed	New	No	Don't know
a. Organizational structures							
b. Operation management							
c. Business functions							
d. Logistics (activities)/Supply Chain (infrastructure)							
e. Other internal systems, processes, or operations							

a. If modifications were experienced, where these initiatives came from?

Initiative	Tick
a. Voluntarily	
b. Negotiated with the client/supplier	
c. Mainly my client/supplier set up the conditions	
d. Other (specify):	

Client/supplier capabilities prior setting up the relationship

4. What capabilities did your firm assess from your client/supplier before setting up the relationship?

Dimension	Tick
b. Production	
c. Planning/Management	
d. Client/supplier coordination	
e. Trading	
f. Post-harvest systems	
g. Logistics (activities)	
h. Security	
i. Quality and standard setting	
j. Other (specify)	

5. What resources did this firm assess from the client/supplier prior to establish the relationship?

Resources	Tick
a. Human	
b. Financial	
c. Technological	
d. Organizational	
e. Supply chain (infrastructure)	
f. Other (specify):	

6. What values and attitudes did this firm assess from the client/supplier prior to establish the relationship?

Values and attitudes		Tick
a.	Organizational	
b.	Commercial/trade	
c.	Environmental	
d.	Security	
e.	Workplace safety	
f.	Income/tax	
g.	Other (specify):	

Maintaining client-supplier relationship

7. Are there systems, procedures or mechanisms to maintain the relationship with the client/supplier?

No ( )
Yes( ) → Explain:

8. Are there mechanisms to coordinate investments and realign skills and capabilities between the firm and your client/supplier?

a. Investments coordination mechanisms

No ( )

Yes ( ) → Tick all that apply

Investments coordination mechanisms		Tick
a.	Systems of assets (synergies between projects)	
b.	Roadmaps for investments	
c.	Parallel and interacting investments across units among firms	
d.	Loans and financing the client/supplier	
e.	Minority investments in client/supplier	
f.	Joint venture (resulting in creation of new entity)	
g.	Acquisition of client/supplier	
h.	Other (specify):	

b. Skills and capabilities realignments mechanisms

No ( )

Yes ( ) → Tick all that apply

Capabilities alignment mechanisms	Tick
a. Systems of skills and capabilities (synergies between projects)	
b. Skills and capability building roadmaps	
c. Joint capabilities and skills development planning	
d. Exchange (temporal)of human resources for skills and capability building	
e. Shared (continuous) skills and capabilities building teams	
f. Hierarchies (authority) that control both firms skills and capabilities building	
g. Hierarchies (authority) that control entire activities for both firms	
h. Other (specify):	

c. If ticked yes to a) or b), please select the frequency of the coordinated investments, or skills and capabilities realignments:

Coordinated investments frequency	
Every	Tick
a. Day	
b. Week	
c. Month	
d. Three months	
e. Six months	
f. Year	
g. More than a year	

Capabilities realignments frequency	
Every	Tick
a. Day	
b. Week	
c. Month	
d. Three months	
e. Six months	
f. Year	
g. More than a year	

University of Sussex
SPRU – Science & Technology Policy Research

Questionnaire: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo Nacional de Ciencia y Tecnología

Client-supplier relationship duration/termination

9. For how long have the firm been related to the client/supplier and the rest of your clients/suppliers?

Please mark the number of years

This client/supplier	1	2	3	4	5	6	7	8	9	10	11-15	15+
Rest of clients/suppliers (average)	1	2	3	4	5	6	7	8	9	10	11-15	15+

10. What are the length of your contracts with the client/supplier, and the rest of your clients/suppliers?

Please mark the number of years

This client/supplier	1	2	3	4	5	6	7	8	9	10	11-15	15+
Rest of clients/suppliers (average)	1	2	3	4	5	6	7	8	9	10	11-15	15+

11. How many more years at least do you expect the relationship with your client/supplier will last, as well as with the rest of your clients/suppliers?

Please mark the number of years

This client/supplier	1	2	3	4	5	6	7	8	9	10	11-15	15+
Rest of clients/suppliers (average)	1	2	3	4	5	6	7	8	9	10	11-15	15+

Managing the client-supplier relationship

12. What are the means to specify the conditions, requirements and/or procedures for the relationship?

Means / Specifications	Formal					Informal					
	Client-supplier contract	Meetings or public audiences	Exhibits (demonstrations, printouts, homepages, etc.)	Information Technologies (telephone, fax, email, etc.)	Other (Specify)	Conversations with client/supplier	Rule of thumb	Own experience	On a daily basis	Other (specify)	Not specified
a. Product quality											
b. Certifications and norms (regulations to comply with)											
c. Postharvest treatments											
d. Packaging and shipping											
e. Estimated shipping quantity											
f. Delivery schedule											
g. Logistics and transport systems											
h. Post 9/11 security measures											
i. Parties responsibilities and liability											
j. Job and operations descriptions											
k. Training, skills and knowledge requirements											
l. Procedures to maintain and terminate the relationship											
m. Conflict resolution mechanisms											
n. Authority and responsibilities of the parties											
o. Decision making involvement (among parties)											
p. Other (specify):											

University of Sussex
SPRU – Science & Technology Policy Research

Questionnaire: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo Nacional de Ciencia y Tecnología

Asset specificity and structure

13. In order to initiate or maintain the relationship with your client/supplier, please indicate what highly specialized assets you had to introduce:

Asset specificity	Tick
a. Geographic location	
b. Infrastructure	
c. Human capital (skills, knowledge)	
d. Brand	
e. Technology and processes	
f. Marketing windows	
g. Other (specify)	

14. If the relationship with your client/supplier terminates, could you find another one you could establish easily a relationship with?

No ( ) → why not:

Yes ( )

15. If your relation with your client/supplier terminates, please indicate what highly specialized assets you could reuse or sell:

Asset specificity	Tick
a. Geographic location	
b. Infrastructure	
c. Human capital (skills, knowledge)	
d. Brand	
e. Technology and processes	
f. Marketing windows	
g. Other (specify)	

Relationship assessment

16. What proportion of sells/purchases is concentrated in your client/supplier? | %

17. What kind of information does the firm and your client/supplier share?:

Information sharing	Tick
a. Product specifications	
b. Logistics (activities) systems assessments	
c. Supply chain (infrastructure) conditions	
d. Trade conditions	
e. Market trends	
f. Regulations, norms, rules, standards, certifications (compliance issues)	
g. Other (specify):	

18. Who and in what degree sets (demands) the norms and regulations to be implemented along the supply chain (including this firm)?

Client/supplier				Shared		This firm			
1	2	3	4	5	6	7	8	9	10

19. Does your client/supplier get involved in research and development (R&D) projects in this firm?

Yes	No	No R&D activities

20. Does your firm exchange human resources to transfer technologies and/or knowledge?

Yes	No	No R&D activities

US University of Sussex
SPRU – Science & Technology Policy Research

Questionnaire: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo Nacional de Ciencia y Tecnología

REGULATORY AWARENESS AND ANTI-BIOTERRORISM REGULATIONS COMPLINACE CAPABILTIES

Knowledge complexity

21. Did new anti-bioterrorism regulations make prior technology and supply chains obsolete? If so, did you have to change it and/or introduce new one? Tick all that apply →

Security impacts on		Obsolete	Changed	New	No impact
Technology	a. Composition				
	b. Design				
	c. Functionality				
Supply chains and logistics	d. Organization				
	e. Functions and roles				
	f. Actors				

22. Suppose you are required to replicate the security measures of your firm in another one, what is the degree of difficulty of replication?, (Not difficult at all is 0, and highest degree of difficulty is 10):

23. How many middle and high position employees (not operators) are in the firm?

24. How many people hold security related responsibilities in the firm?

25. How many people, from each party, supported or are supporting the development of security capabilities of the firm?

Coming from	How many?
a. Customs Border Protection	
b. Other governmental agencies	
c. Clients	
d. Suppliers	
e. Custom brokers	
f. Transport providers	
g. Agribusiness network	
h. Business association	
i. Consultancy	
j. Academic institution (universities and technical schools)	
k. Research Centers	
l. Others (specify):	

26. In order to comply with the security regulations, have the firm had to introduce 'tailor made' of specially design?:

Tailored	Tick
a. Machinery	
b. Infrastructure	
c. Software	
d. Other (specify)	

27. How long did it take to the firm to develop the actual supply chain (logistics) security capabilities?

University of Sussex
SPRU – Science & Technology Policy Research

Questionnaire: Compliance Capability Building along Global Value Chains (COMCAP 2007-2008)

CONACYT
Consejo nacional de Ciencia y Tecnología

Knowledge codifiability

28. Please indicate the responsibilities, conditions and plans of your anti-bioterrorism security measures:

Supply chain sections (tick all that apply)	This firm is responsible for securing:	This firm actually secures:	This firm plans to secure in the future (5 years from now)
a. The supplier's facilities			
b. Transit between the supplier's facilities and this firm's facilities			
c. This firm's facilities			
d. Transit between this facilities and the client's facilities			
e. Client's facilities			
f. Transit between client's facilities final selling location			

29. Please indicate whether and where knowledge, technical skills and problem solving are available:

Tick all that apply	Memos	Posters	Printed or electronic manuals/handbooks	Software	Nowhere
a. Strategic knowledge on supply chain and logistics security capabilities					
b. Technical skills to develop supply chain and logistics security capabilities					
c. Security breach or malfunctioning problem solving mechanism					

a. If software is used to store knowledge and expertise for anti-terrorism security measures, please tick on its origin and whether or not is specialized:

Origin	Standard	Specialized
a. Own development		
b. Software developers		
c. Client		
d. Supplier		
e. Other firm same industry		
f. Business association		
g. Other (specify):		

30. Please indicate the systems to spread knowledge about anti-terrorism measures along the supply chain: tick all that apply →

Knowledge transfer systems	Tick
b. Manuals and handbooks	
c. Speeches	
d. Observation	
e. Informal interaction among people	
f. Face to face	
g. Electronic systems	
h. Other (specify):	
i. No transfer	

Relationship modification with client/supplier

31. To complying with the security regulations along the supply chain, did you experience or expect modification of your relationship with the client/supplier, in any of the following ways? Mark accordingly

	Experienced		Expectations		No change
Expected duration of the relationship	Increased	Reduced	Increase	Reduce	
Contract length	Increased	Reduced	Increase	Reduce	
Change client/supplier	Yes	No	Yes	No	
Vertical integration with client/supplier	Integration	Disintegration	Integration	Disintegration	
Vertical relation without formal integration	Closer	Distant	Closer	Distant	
Roles and activities previously belonging to the client/supplier	More	Less	More	Less	

Thank you for your valuable time and information!

Yari Borbon-Galvez. PhD Researcher in Science and Technology Policy Studies. SPRU, University of Sussex. Yb25@sussex.ac.uk; yari_borbon@yahoo.com (MX)+521(6621) 877013, (UK)+44 07725996677

9.4. Appendix D: Guide to Read TOSMANA Reports

Report on Regulatory awareness (Figure 22: mvQCA of regulatory awareness as causes of middle-high compliance, p.217)

Tosmana Report
Algorithm: Graph-based Agent
Model settings:
Minimizing Value 1
including C R
Variable Settings:
Crisp Set (No Thresholds)

Truth Table:
v1: P.RI.CTPAT v2: P.RI.Distributor
v3: P.RI.CBP v4: P.RI.FPAA
v5: P.RI.TPC v6: P.RI.MEX
v7: P.RI.EXP v8: P.RI.IA
v9: P.RI.IN
O: compliance id: firm

v1	v2	v3	v4	v5	v6	v7	v8	v9	O	id
1	0	1	0	0	0	0	0	1	1	SC15T
1	0	0	0	1	0	0	1	0	0	SC1D
0	0	1	0	0	0	0	0	0	C	SC1E,SC5E
1	0	0	1	0	0	0	0	0	1	SC2D,SC4D
1	1	0	0	0	0	0	0	0	C	SC2ET,SC3E,SC4ET
1	0	1	1	1	1	0	0	0	1	SC3D
0	1	0	0	0	0	1	0	0	0	SC3T
1	0	1	0	0	0	0	0	0	1	SC5D

Result: (all)
P.RI.CBP + P.RI.FPAA
(SC15T+SC3D+SC5D) (SC2D,SC4D+SC3D)
P.RI.CTPAT * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
p.ri.distributor * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
p.ri.exp * p.ri.ia
(SC15T+SC2D,SC4D+SC3D+SC5D)
Created with Tosmana Version 1.301

The algorithm

There are two types of algorithms for the identification of parsimonious causal conditions in TOSMANA, the Quine–McCluskey algorithm and the Graph-Based Agent algorithm (Cronqvist, 2007, pp. 244-258). The Quine–McCluskey algorithm minimizes, or isolates the conditions (e.g. capabilities) that produce the output (e.g. compliance) from those conditions (present of absent) that are do not (Rubenzer, 2008, p. 180). The Graph-Based Agent algorithm was developed for TOSMANA to have the capability to minimize or isolate conditions that produce the output, including 'logical remainders', which is not possible to do with the Quine–McCluskey algorithm (Cronqvist, 2007, p. 241).

Logical reminders are important as they are all possible combinations of the causal conditions that are not actually representing any case study. For instance, if we have 5 possible causal dichotomous conditions, there would be 2^5=32 possible configurations of causal conditions. If we have 12 case studies, and assuming their causal conditions configurations are not repeated, we would have 20 unrepresented configurations=32 possible configurations - 12 present cases. Those configurations not represented by any case study are the logical remainders.

The importance of the logical remainders is that by assuming that they produce the outcome (in our case compliance) they become a tool for the identification of the most parsimonious configurations; hence, their exclusion from the analysis produces too complex configurations (Schneider & Wagemann, 2010, p. 409). This means that rather than identifying A*b*c*D*E (complex causal configuration of 5 dichotomous variables), with logical reminders it is possible to obtain A*c (parsimonious causal configuration of 5 dichotomous variables) as the causal configuration of compliance. Therefore, in our analysis, we decided to include the logical reminders, hence all our TOSMANA reports show Agent-Based algorithms as it is the one that handle logical reminders.

The model settings

The model settings have two components, 'minimising value' and the 'including'. The first component –i.e. minimising value- indicates that whatever output is being explained (in our case compliance), 1 represent the presence of the output, while 0 represents the absence of the output. This is possible because TOSMANA is capable of identifying causal configurations of compliance (minimizing value=1), as well as causal configurations of non-compliance (minimizing value=0). In cases when there are contradictory results from same causal configurations, it is possible to identify the causal configurations of such contradictions, in which case, the model should be run with the 'contradictions' as the output.

The second component –i.e. including- indicates whether causal configurations that yield contradictory and logical reminders are included in the analysis.

Variable settings

This indicates whether the variables were set as Crisp Set (dichotomous variables) or multi-value set, this scale numbers. For instance, in case of Figure 22: mvQCA of regulatory awareness as causes of middle-high compliance (p.217) the variables were set to Crisp-Sets, whilst in Figure 23: Compliance decision and conformance decision as drivers of compliance (p.219) they were set to multi-value. As a consequence of having multi-value variables, TOSMANA reports where the thresholds for the variable were set, in order to indicate order. Setting thresholds implies transforming a scale variable to ordinal. And each interval of the newly converted ordinal variable becomes a category of the variable. In the example from Figure 23 (p.219), the variable month has two thresholds, 26 and 55. This means that the variable has three categories, '0' when the variable takes values under 26 months, '1' when the variable takes values over 26 and under 55 months, and '2' when the variable takes values over 55 months (values exactly on the thresholds are omitted from the analyses).

The truth table

This section of the report consists of 2 components. The first component of the section reports the independent and dependent variables of the model. The independent variables are coded and named -e.g. v1: P.RI.CTPAT, v2: P.RI.Distributor, and so on- also the dependent variable is coded and named only that it will always be coded 0 -e.g. 0: Compliance-, so that it is easily identifiable in the next component of the section, that is the truth table.

The component of the truth table shows the values that each variable take for each case study. Each case is identifiable in the column at the far right of the table headed 'id'. However, the truth table rather than reporting case by case, it shows all the causal configurations in the database, and at the id column reports the cases that present that particular configuration. For instance, in the Figure 22 (p.217), the fourth configuration – source of regulatory awareness are CTPAT and the FPAA (Fresh Produce Association of the Americas) and not from the rest of the organisations- is shared by two firms with regulatory compliance, SC2D and SC4D. The third configuration on the other hand, is also shared by two firms (SC1E and SC5E), however, one of them is compliant and the other not.

Results

The last section (e.g. Figure 22, p.217) shows the results of the analysis. It displays the configurations (complex if logical remainders are not included in the minimisation, or parsimonious if they are included, in this case remainders were included hence the parsimonious results) of causal conditions that produced compliance, as well as the firms that have such configurations. Note that the configurations represent the pathways to compliance, and the sign + indicates alternative pathways to compliance, whereas the sign * indicates that the causal conditions are connected (they need to be together to cause compliance).

Further, in case crisp-sets, the condition will change to 'CAPITAL LETTER' if the condition should be present, whilst it will remain 'lowercase' if the condition should be absent. So for instance, the first line of results show when the source of regulatory awareness was the Customs Border Protection (CBP), the firm -i.e. SC15T, SC3D, and SC5D- reached compliance; same for the firms whose source was the Fresh Produce Association of the Americas (FPAA). Similarly (second line of results), another pathway to compliance by firms (SC15T, SC2D, SC4D, SC3D, and SC5D) was having CTPAT and not their 'industry associations' as source of regulatory awareness. And so on.

10. References

Agiwal, S., Mohtadi, H., & Kinsey, J. (2008). Security-Preparedness of Firms in U.S. Food Supply Chain. Paper presented at the Industry Studies Annual Conference 2008. Retrieved 2 January 2011, from http://ssrn.com/paper=1135679

Aiken, R., Kock, N., & Mandviwalla, M. (2000). Fluency in information technology: a second course for non-CIS majors. SIGCSE Bull., 32(1), 280-284.

Alvarez, R. R. (2001). Beyond the Border: Nation-State Encroachment, NAFTA, and Offshore Control in the U.S.-Mexican Mango Industry. Human Organization, 60(2), 121-127.

American Apparel. (2009). Investor Presentation [Electronic Version]. Fact Sheet. Retrieved January 24 2009, from http://americanapparel.net/contact/2009_Fact_Sheet.pdf

Andersen, S. O., Sarma, K. M., & Sinclair, L. (2002). Protecting the ozone layer: the United Nations history. London: Earthscan.

Aragón-Correa, J. A., Hurtado-Torres, N., Sharma, S., & García-Morales, V. J. (2008). Environmental strategy and performance in small firms: A resource-based perspective. Journal of Environmental Management, 86(1), 88-103.

Arshinder, S., Kanda, A., & Deshmukh, S. G. (2008). Supply chain coordination: Perspectives, empirical studies and research directions. International Journal of Production Economics, 115(2), 316-335.

Aruoma, O. I. (2006). The impact of food regulation on the food supply chain. Toxicology, 221(1), 119-127.

Ashford, N. (2003). Innovation-The Pathway to Threefold Sustainability. In F. C. Lehner (Ed.) The Steilmann Report: The Wealth of People: An Intelligent Economy for the 21st Century. Leipzig: Bochum/Wattenscheid KSI.

Ashford, N., Ayers, C., & Stone, R. (1985). Using regulation to change the market for innovation. Harvard Environmental Law Review, 9(2), 419-466.

Ashford, N., Heaton, G. R., & Priest, W. C. (1979). Environmental, Health and Safety Regulations and Technological Innovation. In C. T. Hill & J. M. Utterback (Eds.), Technological Innovation for a Dynamic Economy (pp. 161-221). New York: Pergamon Press, Inc.

Aust, P. (1997). An Institutional Analysis of Vertical Coordination Versus Vertical Integration: The Case of The US Broiler Industry [Electronic Version]. Staff Papers. Michigan State University, Department of Agricultural, Food, and Resource Economics, from http://ideas.repec.org/p/ags/midasp/11670.html

Baden-Fuller, C., & Winter, S. G. (2005). Replicating Organizational Knowledge: Principles or Templates? SSRN eLibrary.

Baldwin, R., & Black, J. (2007). Really Responsive Regulation. Unpublished Working Paper. London School of Economics and Political Science. Law Department.

Baldwin, R., & Black, J. (2008). Really Responsive Regulation. The Modern Law Review, 71(1), 59-94.

Baldwin, R., Schott, C., & Hood, C. (1998). A reader on regulation. Oxford: Oxford University Press.

Barney, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, 17(1), 99.

Barney, J. (2001). Resource-based theories of competitive advantage: A ten-year retrospective on the resource-based view. Journal of Management, 27(6), 643-650.

Barratt, M., & Oke, A. (2007). Antecedents of supply chain visibility in retail supply chains: A resource-based theory perspective. Journal of Operations Management, 25(6), 1217-1233.

Bartle, I., & Vass, P. (2005). SELF-REGULATION AND THE REGULATORY STATE~ A SURVEY OF POLICY AND PRACTICE, Research Report 17. Bath, UK: Centre for the study of Regulated Industries (CRI). University of Bath School of Management.

Bartle, I., & Vass, P. (2007). Self-regulation within the regulatory state: Towards a new regulatory paradigm? Public Administration, 85(4), 885-905.

Bayazit, O., Karpak, B., & Yagci, A. (2006). A purchasing decision: selecting a supplier for a construction company. Journal of Systems Science and Systems Engineering, 15(2), 217-231.

Beamon, B. M. (1999). Measuring supply chain performance. International Journal of Operations & Production Management, pp. 275-292, from http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=1786575&site=ehost-live

Bednar, J. (2006). Is full compliance possible? Conditions for shirking with imperfect monitoring and continuous action spaces. Journal of Theoretical Politics, 18(3), 347-375.

Bell, M., & Pavitt, K. (1995). The development of technological capabilities. In I. Ul Haque (Ed.), Trade, Technology, and International Competitiveness (pp. 218). Washington, D.C.: The World Bank.

Berdegue, J. A., Balsevich, F., Flores, L., & Reardon, T. (2005). Central American supermarkets' private standards of quality and safety in procurement of fresh fruits and vegetables. Food Policy, 30(3), 254-269.

Bessant, J., Kaplinsky, R., & Lamming, R. C. (2003). Putting supply chain learning into practice. International Journal of Operations & Production Management, 23(2), 167-184.

Bitran, G. R., Gurumurthi, S., & Sam, S. L. (2007). The need for third-party coordination in supply chain governance. MIT Sloan Management Review, 48(3), 30-37.

Black, J. (2010). The role of risk in regulatory processes. In R. Baldwin, M. Cave & M. Lodge (Eds.), The Oxford Handbook of Regulation (pp. 302-348). USA: Oxford University Press.

Blomqvist, K., Kyläheiko, K., & Virolainen, V. M. (2002). Filling a gap in traditional transaction cost economics: Towards transaction benefits-based analysis. International Journal of Production Economics, 79(1), 1-14.

Blount, S. (2007). The role of security management in achieving "Continuous Compliance" [Electronic Version]. White Paper: Compliance. From http://image.tianjimedia.com/imagelist/2007/141/d1h3327mv8ec.pdf

Boehlje, M., Akridge, J., & Downey, D. (1995). Restructuring agribusiness for the 21st century. Agribusiness, 11(6).

Bongers, H. B. (2004). The increased cost of security to the food industry since the events of september 11, 2001. Unpublished Master Thesis, The University of Wisconsin-Whitewater, Wisconsin, US.

Borbon-Galvez, Y. (1998). Guia logistica de transportacion de productos hortofruticolas a Europa. Hermosillo, Mexico: Sonora Exporta Fase II. Bancomext, S.N.C. http://econpapers.repec.org/paper/pramprapa/16712.htm.

Borbon-Galvez, Y. (2000). La Influencia de los Intermediarios Comerciales en la Configuración Hortofrutícola de Exportación de la Costa de Hermosillo. Unpublished BA Thesis, Universidad de Sonora, Hermosillo.

Borbon-Galvez, Y. (2001). Sonora; un Estado agrícola exportador de hortofrutales? In L. Arredondo & A. Salido (Eds.), Economía Sonorense y sus Regiones. Hermosillo, Mexico: UNISON.

Borbon-Galvez, Y. (2004). Federal agencies slowed learning process: the case of food trucking industry between United States and Mexico. (Internship Report). Unpublished Internship Report. American Trucking Associations and Discovering North America Summer Institute 2004-American University.

Boske, L. (2006). Port and supply chain security in the United States and Abroad (No. 150). Austin, Texas: University of Texas at Austin.

Bowen, F. E., Cousins, P. D., Lamming, R. C., & Faruk, A. C. (2001). The role of supply management capabilities in green supply. Production and Operations Management, 10(2), 174-189.

Boyd, J. W. (1998). Searching for the Profit in Pollution Prevention: Case Studies in the Corporate Evaluation of Environmental Opportunities: SSRN.

Braithwaite, J., & Drahos, P. (2000). Global Business Regulation. UK, USA, Australia, Spain: Cambridge University Press.

Branigin, W., Allen, M., & Mintz, J. (2004, 3 December). Tommy Thompson Resigns From HHS. Washington Post. From http://www.washingtonpost.com/wp-dyn/articles/A31377-2004Dec3.html

Braun, E., & Wield, D. (1994). Regulation as a Means for the Social Control of Technology. Technology Analysis & Strategic Management, 6(3), 259.

Bullinger, H.-J., Kühner, M., & Van Hoof, A. (2002). Analysing supply chain performance using a balanced measurement method. International Journal of Production Research, 40(15), 3533-3543.

Busch, P.-O., Jorgens, H., & Tews, K. (2005). The Global Diffusion of Regulatory Instruments: The Making of a New International Environmental Regime. The ANNALS of the American Academy of Political and Social Science, 598(1), 146-167.

Buysse, K., & Verbeke, A. (2003). Proactive environmental strategies: A stakeholder management perspective. Strategic Management Journal, 24(5), 453-470.

Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: a new framework for analysis. US and UK: Lynne Rienner Publishers.

C-TPAT/CBP. (2004). Securing the global supply chain. Retrieved 5/18/2006. From www.cbp.gov.

C-TPAT/CBP. (2006). Supply chain security best practices catalog. Retrieved 5/18/2006. From http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/.

C-TPAT/CBP. (2007). C-TPAT Cost/Benefit Survey: Center for Survey Research, University of Virginia. Weldon Cooper, Center for Public Service, University of Virginia.

C-TPAT/CBP. (2010). C-TPAT 5 Step Risk Assessment Process Guide. Retrieved 3 August 2010. from http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/supply_chain/ctpat_assessment.ctt/ctpat_assessment.pdf.

CAADES/CIDH. (2007). Propuesta de modernizacion del puesto de revision militar de "El Desengaño". Retrieved 13/Oct/2008, from http://www.cidh.org.mx

Calvin, L., & Barrios, V. (1999). Marketing winter vegetables from Mexico. Journal of Food Distribution Research, 30, 50-62.

Caren, N., & Panofsky, A. (2005). TQCA - A technique for adding temporality to qualitative comparative analysis. Sociological Methods & Research, 34(2), 147-172.

Carlson, S. L., & Fernandez, F. A. (2006). The Costs of Compliance in the US Securities Industry, SIA Research Reports (Vol. 7, pp. 1–31). Securities Industry Association.

Carmeli, A. (2001). High-and low-performance firms: do they have different profiles of perceived core intangible resources and business environment? Technovation, 21(10), 661-671.

Cashore, B., Gale, F., Meidinger, E. E., & Newson, D. (2006). Knots in the wood: explaining the uneven emergence of forest certification in developing and transitioning countries. Paper presented at the 47th Annual International Studies Association Convention, panel on Global Forest Policy – International, Regional, and National Perspectives on a Contested Issue., San Diego, CA, USA, March 22, 2006.

CBP. (2010). C-TPAT Mutual Recognition. Retrieved 3 August 2010. From http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/mr/mutual_recog.ctt/mutual_recog.pdf.

Chaddad, F., R., & Cook, M., L. (2004). Understanding New Cooperative Models: An Ownership-Control Rights Typology. Review of Agricultural Economics, 26(3), 348-360.

Chan, F. T. S., & Qi, H. J. (2003). An innovative performance measurement method for supply chain management. Supply Chain Management, 8(3/4), 209.

Chandler, A. D., Jr. (1973). Decision Making and Modern Institutional Change. The Journal of Economic History, 33(1), 1-15.

Chinander, K. R., Kleindorfer, P. R., & Kunreuther, H. C. (1998). Compliance Strategies and Regulatory Effectiveness of Performance-Based Regulation of Chemical Accident Risks. Risk Analysis, 18(2), 135-143.

Christmann, P., & Taylor, G. (2005). Firm Self-Regulation Through International Certifiable Standards: Determinants of Symbolic versus Sustainable Implementations. Paper presented at the First Annual Conference on Institutional Mechanisms for Industry Self-Regulation. from http://mba.tuck.dartmouth.edu/mechanisms/pages/Papers/ChristmannTaylorDartmouth.pdf

Closs, D. (2005). Dimensioning a Secure Supply Chain. Paper presented at the Institute of food technologists' First Annual Food Protection & Defense Research Conference. November 3-4., Atlanta, Georgia, USA.

Closs, D., & McGarrel, E. (2004). Enhancing Security Throughout the Supply Chain [Electronic Version]. Special Report Series, IBM Center for Business of Government. Retrieved 20 February 2005, from www.businessofgovernment.org

COAC/CBP. (2008). Minutes of the Departmental Advisory Committee on Commercial Operations of Customs and Border Protection and Related Homeland Security Functions. Washington, DC: Customs Border Protection

Cohen, W. M., & Levinthal, D. A. (1990). Absorptive Capacity-A New Perspective on Learning and Innovation. Administrative Science Quarterly, 35(1), 128-152.

Cook, R. L. (1998). International trends in the fresh fruit and vegetable sector [Electronic Version]. Acta Hort. (ISHS) 495:143-156. WCHR-World Conference on Horticultural Research 495, 143-156. From http://www.actahort.org/books/495/495_6.htm

Cordesman, A. (2001). Biological warfare and the "Buffy Paradigm". Washington, DC.: Center for Strategic International Studies

Cordesman, A., & Burke, A. A. (2001). Defending America: Asymmetric and terrorist attacks with biological weapons. Washington, DC: Center for Strategic and International Studies

Cortina, J. M. (1993). Interaction, Nonlinearity, and Multicollinearity: Implications for Multiple Regression. Journal of Management, 19(4), 915-922.

Cousins, P. D. (2002). A conceptual model for managing long-term inter-organisational relationships. European Journal of Purchasing & Supply Management, 8(2), 71-82.

Cousins, P. D., Lamming, R. C., & Bowen, F. (2004). The role of risk in environment-related supplier initiatives. International Journal of Operations & Production Management, 24(5-6), 554-565.

Cronqvist, L. (2005). Introduction to multi-value qualitative comparative analysis (MVQCA). COMPASSS Didactical Papers, 4.

Cronqvist, L. (2007). Konfigurationelle Analyse mit Multi-Value QCA als Methode der Vergleichenden Politikwissenschaft mit einem Fallbeispiel aus der Vergleichenden Parteienforschung (Erfolg Grüner Parteien in den achtziger Jahren). PhD diss., University of Marburg, Germany.

Cronqvist, L. (2009). Tosmana - Tool for Small-N Analysis (Version 1.3.1). http://www.tosmana.net.

Crotty, J. (2006). Greening the supply chain? The impact of take-back regulation on the UK automotive sector. Journal of Environmental Policy & Planning, 8(3), 219 - 234.

CTPAT/CBP. (2006). Supply chain security best practices catalog. Retrieved 5/18/2006. From http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_members/ctpat_best_practices.ctt/ctpat_best_practices.pdf.

CTPAT/CBP. (2007). C-TPAT Cost/Benefit Survey: Center for Survey Research, University of Virginia. Weldon Cooper, Center for Public Service, University of Virginia.

Dahlstrom, R., McNeilly, K. M., & Speh, T. W. (1996). Buyer-Seller Relationships in the Procurement of Logistical. Academy of Marketing Science. Journal, 24(2), 110.

Dalziel, G. R. (2009). FOOD DEFENCE INCIDENTS 1950–2008. A chronology and analysis of incidents involving the malicious contamination of the food supply chain [Electronic Version]. CENS Conference Reports, from http://www.rsis.edu.sg/cens/publications/reports/RSIS_Food%20Defence_170209.pdf

Dao, M., & Ofori, G. (2010). Determinants of firm compliance to environmental laws: a case study of Vietnam. Asia Europe Journal, 8(1), 91-112.

Del Sorbo, M. (2010). Competencies and capabilities: minding the Science and Technology gap in the Campania region. The role of universities and firms' associations. Unpublished Dissertation, Università degli Studi di Salerno, Fisciano, Italy.

Delmas, M. (1999). Exposing strategic assets to create new competencies: the case of technological acquisition in the waste management industry in Europe and North America. Ind Corp Change, 8(4), 635-671.

Delmas, M., & Toffel, M. W. (2008). Organizational responses to environmental demands: Opening the black box. Strategic Management Journal, 29(10), 1027-1055.

Department of Homeland Security. (2003). Modification of Free and Secure Trade Prototype. Federal Register/Vol. 68, No. 186, from http://edocket.access.gpo.gov/2003/pdf/03-24260.pdf

Dewick, P., & Miozzo, M. (2002). Sustainable technologies and the innovation - regulation paradox. Futures, 34(9-10), 823-840.

Dimitri, C., & Oberholtzer, L. (2009). Meeting market demand in the organic sector: Handler-supplier relationships in the face of tight supply. Renewable Agriculture and Food Systems, 24(02), 137-145.

Dolan, C., & Humphrey, J. (2000). Governance and Trade in Fresh Vegetables: The Impact of UK Supermarkets on the African Horticulture Industry. Journal of Development Studies, 37(2), 147-176.

Dosi, G., Faillo, M., & Marengo, L. (2008). Organizational capabilities, patterns of knowledge accumulation and governance structures in business firms: An introduction. Organization Studies, 29(8-9), 1165-1185.

Dosi, G., & Nelson, R. R. (1994). An introduction to evolutionary theories in economics. Journal of Evolutionary Economics, 4(3), 153.

Dosi, G., Nelson, R. R., & Winter, S. G. (2000). The nature and dynamics of organizational capabilities. USA: Oxford University Press.

Drew, M. (2007). Information risk management and compliance—expect the unexpected. BT technology journal, 25(1), 19-29.

Eisenhardt, K. M. (1989). Building Theories from Case Study Research. Academy of Management Review, 14(4), 532.

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? Strategic Management Journal, 21(10-11), 1105-1121.

EPA. (2000). Principal Findings: The U. S. Specialty-Batch Chemical Industry, Sustainable Industry: U.S. Environmental Protection Agency.

Erera, A. (2005). Providing Security to Food Transportation Systems without Compromising Productivity. Paper presented at the Institute of food technologists' First Annual Food Protection & Defense Research Conference. November 3-4., Atlanta, Georgia, USA.

Ernst, D., & Kim, L. (2002). Global production networks, knowledge diffusion, and local capability formation. Research Policy, 31(8-9), 1417-1429.

European Commission. (2005). The Authorised Economic Operators. Retrieved 21/07/2008. From http://ec.europa.eu/taxation_customs/resources/documents/customs/policy_issues/customs_security/AEO_strategic_paper_en.pdf.

FDA/HHS. (2009). What You Need to Know About Prior Notice of Imported Food Shipments. Retrieved 17 August 2009. From http://www.fda.gov/Food/GuidanceComplianceRegulatoryInformation/default.htm

FHWA/USDOT (1984) TRUCK SIZE AND WEIGHT, ROUTE DESIGNATIONS, LENGTH, WIDTH AND WEIGHT LIMITATIONS, 658 C.F.R.

Field, A. P. (2009). Discovering statistics using SPSS. London: SAGE publications Ltd.

Fintor, L. (2002). Counterfeit Cases Set Stage for Today's Laws, Safety Mechanisms. J Natl Cancer Inst, 94(19), 1425.

Fiss, P. C. (2007). A set-theoretic approach to organizational configurations. Academy of Management Review, 32(4), 1180-1198.

Fleischman, E. H. (2001). Remarks on the Regulation of Securities and Security Exchanges in the Age of the Internet. NYUJ Legis. & Pub. Pol'y, 5, 1.

Flynn, S. (2004). America the Vulnerable: How our government is falling to protect us from terrorism. US: HarperCollins Publisher.
Foss, N. J. (1998). The resource-based perspective: an assessment and diagnosis of problems. Scandinavian Journal of Management, 14(3), 133-149.
Frank, S. D., & Henderson, D. R. (1992). Transactions costs as determinants of vertical coordination in the U.S. food industries. American Journal of Agricultural Economics, 74(4), 941.
Fremeth, A. R. (2009). The Dynamic Relationship between Firm Capabilities, Regulatory Policy, and Environmental Performance: Renewable Energy Policy and Investment in the US Electric Utility Sector. Unpublished Dissertation in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy, University of Minnesota, Minneapolis, US.
French, M., T., Neighbors, D., M., Carswell, L., K., Williams, R., A., & Bush, L., M. (1992). A model for estimating industry compliance costs of food labelling regulations. Agribusiness, 8(2), 165-186.
Froud, J., & Ogus, A. (1996). 'Rational' social regulation and compliance cost assessment. Public Administration, 74(2), 221-237.
Garcia-Martinez, M., Fearne, A., Caswell, J. A., & Henson, S. (2007). Co-regulation as a possible model for food safety governance: Opportunities for public-private partnerships. Food Policy, 32(3), 299-314.
Gereffi, G., Humphrey, J., & Sturgeon, T. (2005). The governance of global value chains. Review of International Political Economy, 12(1), 78-104.
Gerring, J., & McDermott, R. (2007). An experimental template for case study research. American Journal of Political Science, 51(3), 688-701.
Ghoshal, S., Hahn, M., & Moran, P. (1999). Management competence, firm growth and economic progress. Contributions to Political Economy, 18(1), 121-150.
Gilliland, D. I., & Manning, K. C. (2002). When do firms conform to regulatory control? The effect of control processes on compliance and opportunism. Journal of Public Policy & Marketing, 21(2), 319-331.
Gimenez, C. (2006). Case studies and surveys in supply chain management research-Two complementary methodologies. In H. Kotzab, S. Seuring, M. Muller & G. Reiner (Eds.), Research methodolodies in supply chain management (pp. 632): Springer.
Goddard, L. (2005). Cargo and Supply chain Security Trends 2005. Paper presented at the eyefortransport's 4th North American Cargo Security Forum, Willard InterContinental Hotel, Washington DC. December 5-6.
Goldberg, L. S. (2007). Financial sector FDI and host countries: New and old lessons. Economic Policy Review, 13(1).
Good, P. I. (2006). Resampling methods: a practical guide to data analysis: Birkhauser.
Gorga, E., & Halberstam, M. (2007). Knowledge Inputs, Legal Institutions and Firm Structure: Towards a Knowledge-Based Theory of the Firm. Northwestern University Law Review, 101(3).
Gorman, D. (1996). Loss Prevention Racks up Success. Security Management, 40(3), 55.
Grabosky, P. N. (1995). Using Non-Governmental Resources to Foster Regulatory Compliance. Governance, 8(4), 527-550.
Grabowski, H., Viscusi, W. K., & Evans, W. N. (1989). Price and Availability Tradeoffs of Automobile Insurance Regulation. Journal of Risk & Insurance, 56(2), 275-299.
Greer, C. R., & Downey, H. K. (1982). Industrial Compliance with Social Legislation: Investigations of Decision Rationales. The Academy of Management Review, 7(3), 488-498.

Griffith, D. A., & Myers, M. B. (2005). The performance implications of strategic fit of relational norm governance strategies in global supply chain relationships. Journal of International Business Studies, 36(3), 254-269.

Guston, D. H., & Sarewitz, D. (2002). Real-time technology assessment. Technology in Society, 24(1-2), 93-109.

Gyau, A., & Spiller, A. (2008). The impact of supply chain governance structures on the inter-firm relationship performance in agribusiness. Agricultural Economics-Zemedelska Ekonomika, 54(4), 176-185.

Haftendorn, H. (1991). The security puzzle: Theory-Building and Discipline-Building in international security. International Studies Quarterly, 35(1), 3-17.

Halldorsson, A., Kotzab, H., Mikkola, J., H., & Skjøtt-Larsen, T. (2007). Complementary theories to supply chain management. Supply Chain Management, 12(4), 284.

Harris, L., Farber, J., Beuchat, L., Parish, M., Suslow, T., Garrett, E., et al. (2003). Outbreaks Associated with Fresh Produce: Incidence, Growth, and Survival of Pathogens in Fresh and Fresh-Cut Produce. Comprehensive Reviews in Food Science and Food Safety, 2, 78-141.

Harris, R., & Li, Q. C. (2009). Exporting, RD, and absorptive capacity in UK establishments. Oxford Economic Papers-New Series, 61(1), 74-103.

Hart, S. L. (1995). A Natural-Resource-Based View of the Firm. Academy of Management Review, 20(4), 986-1014.

HeinOnline. (2011). U.S. Federal Legislative History Library (Publication. Retrieved 11 January 2011, from HeinOnline: http://heinonline.org/HOL/CSV.csv?index=leghis/leghistitle&collection=leghis

Helfat, C. E., & Peteraf, M. A. (2003). The dynamic resource-based view: Capability lifecycles. Strategic Management Journal, 24(10), 997-1010.

Henderson, R. (1994). The evolution of integrative capability: innovation in cardiovascular drug discovery. Industrial and Corporate Change, 3(3), 607.

Henson, S., & Heasman, M. (1998). Food safety regulation and the firm: understanding the compliance process. Food Policy, 23(1), 9-23.

Henson, S., & Humphrey, J. (2009). The Impacts of Private Food Safety Standards on the Food Chain and on Public Standard-Setting Processes, JOINT FAO/WHO FOOD STANDARDS PROGRAMME. Rome: Codex Alimentarius Commission: FAO/WHO.

Herrmann, A. M., & Cronqvist, L. (2009). When dichotomisation becomes a problem for the analysis of middle-sized datasets. International Journal of Social Research Methodology, 12(1), 33-50.

Herzog, P. (2008). Open and Closed Innovation: Different Cultures for Different Strategies. Germany: Gabler.

Hewitt-Dundas, N., Andreosso-O'Callaghan, B., Crone, M., & Roper, S. (2005). Knowledge Transfers from Multinational Plants in Ireland: A Cross-Border Comparison of Supply-Chain Linkages. European Urban and Regional Studies, 12(1), 23-43.

Hino, A. (2009). Time-Series QCA Studying Temporal Change through Boolean Analysis. Sociological Theory and Methods, 24(2), 247-265.

Homeland Security. (2006). Budget in brief: Fiscal year 2006. Retrieved 12/5/2006, from https://www.dhs.gov/xlibrary/assets/Budget_BIB-FY2006.pdf

Homeland Security Act of 2002, United States Congress, 107th Sess.(2002).

Hoopes, D. G., & Madsen, T. L. (2008). A capability-based view of competitive heterogeneity. Industrial and Corporate Change, 17(3), 393-426.

Huang, S., & Huang, K. (2007). Increased US Imports of Fresh Fruit and Vegetables. US Department of Agriculture, Economic Research Service, FTS-328-01.

Hutter, B. M. (1993). SETTING SAFETY STANDARDS - REGULATION IN THE PUBLIC AND PRIVATE SECTORS - CHEIT,RE. Law & Society Review, 27(1), 233-248.

Iizuka, M., & Borbon-Galvez, Y. (2009). Compliance with the private standards and capacity building of national institutions under globalization: new agendas for developing countries? [Electronic Version]. UNU-MERIT Working Papers, #2009-025. From http://EconPapers.repec.org/RePEc:dgr:unumer:2009025

InSYNC. (2007). Singapore tops customs authorities worldwide [Electronic Version]. Updates. Retrieved 21/07/2008. From http://www.customs.gov.sg/insync/issue01/updates/updates.html

James, P., Johnstone, R., Quinlan, M., & Walters, D. (2007). Regulating Supply Chains to Improve Health and Safety. Ind Law J, 36(2), 163-187.

Jaspers, F., & van den Ende, J. (2006). The organizational form of vertical relationships: Dimensions of integration. Industrial Marketing Management, 35(7), 819-828.

Johannessen, J. A. (2008). Organisational innovation as part of knowledge management. International Journal of Information Management, 28(5), 403-412.

Jones, P., Clarke-Hill, C., Comfort, D., Hillier, D., & Shears, P. (2005). Radio frequency identification and food retailing in the UK. British Food Journal, 107(6), 356-360.

Kalwani, M. U., & Narayandas, N. (1995). Long-term manufacturer-supplier relationships: Do they pay off for supplier firms? Journal of Marketing, 59(1), 1.

Kaplinsky, R., & Morris, M. (2001). A handbook for Value Chain Research. Retrieved June 3 2007. From http://www.inti.gob.ar/cadenasdevalor/manualparainvestigacion.pdf

Kaufman, D. (2007). Does Security Trump Trade? Law and Business Review of the Americas, 13(3), 619.

Kavilanz, P. (2010). Tylenol recall: FDA slams company. CNNMoney.com. Retrieved 2 January 2011. From http://money.cnn.com/2010/01/15/news/companies/over_the_counter_medicine_recall/

Kemp, R. (2000). Technology and environmental policy: innovation effects of past policies and suggestions for improvement. In OECD (Ed.), Innovation and the Environment: Sustainable Development (pp. 35–61). Paris: OECD Publishing.

Kim, L. (2004). The Multifaceted Evolution of Korean Technological Capabilities and its Implications for Contemporary Policy. Oxford Development Studies, 32(3), 341-363.

Kingsbury, B. (1997). Concept of Compliance as a Function of Competing Conceptions of International Law, The. Michigan Journal of International Law, 19, 345.

Kinser, J., Seltzer, J., & Friddle, C. (2005). Food Security Practices among Food Retailers, Foodservice Companies, and Wholesalers: Indicators of Excellence. Paper presented at the Institute of food technologists' First Annual Food Protection & Defense Research Conference. November 3-4., Atlanta, Georgia, USA.

Kitching, J. (2006). A burden on business? Reviewing the evidence base on regulation and small-business performance. Environment and Planning C-Government and Policy, 24(6), 799-814.

Kogut, B., MacDuffie, J. P., & Ragin, C. (2004). Prototypes and strategy: Assigning causal credit using fuzzy sets. European Management Review, 1(2), 114-131.

Kogut, B., & Ragin, C. (2004). Nations as institutional arenas: testing theories of complex causality. Paper presented at the workshop on "Do Facts Matter in Elaborating Theories? CRG-Ecole Polytechnique, Paris, France.

Kogut, B., & Ragin, C. (2006). Exploring complexity when diversity is limited: institutional complementarity in theories of rule of law and national systems revisited. European Management Review, 3(1), 44-59.

Kogut, B., & Zander, U. (1992). KNOWLEDGE OF THE FIRM, COMBINATIVE CAPABILITIES, AND THE REPLICATION OF TECHNOLOGY. Organization Science, 3(3), 383-397.

Kogut, B., & Zander, U. (1996). What firms do? Coordination, identity, and learning. Organization Science, 7(5), 502-518.

Koulikofff-Souviron, M., & Harrison, A. (2006). Using Case study methods in researching supply chains. In H. Kotzab, S. Seuring, M. Muller & G. Reiner (Eds.), Research Methodologies in Supply Chain Management (pp. 632). NY: Physica-Verlag.

Kuperan, K., & Sutinen, J. G. (1998). Blue Water Crime: Deterrence, Legitimacy, and Compliance in Fisheries. Law & Society Review, 32(2), 309-338.

Laden, M. D. (2007). The Genesis of the US C-TPAT program: Lessons learned and earned by the government and trade. World Customs Journal, 1(2), 75-80.

Lai, L. W. C., Yung, P., Li, R. Y. M., & Ho, D. C. W. (2007). The private supply of and public demand for planning: Compliance with planning conditions in the absence of direct statutory enforcement measures. Planning Practice & Research, 22(4), 535-557.

Lamm, F. (1997). Small businesses and OH&S advisors. Safety Science, 25(1-3), 153-161.

Lamming, R. C. (1992). Supplier Strategies in the Automotive Components Industry: Development towards Lean Production. Unpublished Doctoral Thesis. Science and Policy Research Unit, University of Sussex. Brighton, UK.

Lamming, R. C. (2000). Japanese Supply Chain Relationships in Recession. Long Range Planning, 33(6), 757-778.

Lamming, R. C., Caldwell, N. D., Harrison, D. A., & Phillips, W. (2001). Transparency in supply relationships: Concept and practice. Journal of Supply Chain Management, 37(4), 4.

Langlois, R., & Robertson, P. (1993). Business Organization as a Coordination Problem: Toward a Dynamic Theory of the Boundaries of the Firm. Business and Economic History On-Line, 22(1).

Lawson, B., Petersen, K. J., Cousins, P. D., & Handfield, R. B. (2009). Knowledge Sharing in Interorganizational Product Development Teams: The Effect of Formal and Informal Socialization Mechanisms. Journal of Product Innovation Management, 26(2), 156-172.

Lawson, B., Tyler, B. B., & Cousins, P. D. (2008). Antecedents and consequences of social capital on buyer performance improvement. Journal of Operations Management, 26(3), 446-460.

Lechner, C., & Gudmundsson, S. V. (2008). Which Types of Resources are Necessary to Achieve Competitive Advantage? SSRN eLibrary.

Lee, H. L. (2004). Supply Chain Security-Are You Ready? Paper presented at the Standford Global Supply Chain Management Forum: 3rd September, Standford, Ca. USA.

Lee, H. L., Padmanabhan, V., & Whang, S. J. (1997). Information distortion in a supply chain: The bullwhip effect. Management Science, 43(4), 546.

Lee, J., & Slater, J. (2007). Dynamic capabilities, entrepreneurial rent-seeking and the investment development path: The case of Samsung. Journal of International Management, 13(3), 241-257.

Lee, M., T. (1998). The Ford Pinto case and the development of auto safety regulations, 1893-1978. Business and Economic History, 27(2), 390.

Levi-Faur, D. (2002). Comparative Research Designs in the Study of Regulation: How to Increase the Number of Cases without Compromising the Strengths of Case-Oriented Analysis. Paper presented at the International Workshop of the Centre on Regulation and Competition, 4-6 September 2002, University of Manchester, Manchester, UK.

Lichtenthaler, U. (2007, Apr 27-29). Absorptive Capacity, Environmental Turbulence, and the Complementarity of Organizational Learning Processes. Paper presented at the 22nd Annual Meeting of the Society-for-Industrial-and -Organizational-Psychology, New York.

Lichtenthaler, U. (2009). ABSORPTIVE CAPACITY, ENVIRONMENTAL TURBULENCE, AND THE COMPLEMENTARITY OF ORGANIZATIONAL LEARNING PROCESSES. Academy of Management Journal, 52(4), 822-846.

Lichtenthaler, U., & Ernst, H. (2007). Developing reputation to overcome the imperfections in the markets for knowledge. Research Policy, 36(1), 37-55.

Lichtenthaler, U., & Lichtenthaler, E. (2009). A Capability-Based Framework for Open Innovation: Complementing Absorptive Capacity. Journal of Management Studies, 46(8), 1315-1338.

Lieberson, S. (2004). Comments on the Use and Utility of QCA. Qualitative Methods. Newsletter of the American Political Science Association Organized Section on Qualitative Methods, 2(2), 13-14.

LLTRM. (2004). Canadian Supply Chain Efficiency Smart Border Study. Lean Logistics Technology Roadmap (LLTRM). Retrieved 4/3/2006, 2006, from www.strategis.ic.gc.ca/logistics

Longest, K. C., & Vaisey, S. (2008). fuzzy: A program for performing qualitative comparative analyses (QCA) in Stata. Stata Journal, 8(1), 79-104.

Lorenzoni, G., & Lipparini, A. (1999). The Leveraging of Interfirm Relationships as a Distinctive Organizational Capability: A Longitudinal Study. Strategic Management Journal, 20(4), 317-338.

Lupton, D., Donaldson, C., & Lloyd, P. (1991). Caveat emptor or blissful ignorance? Patients and the consumerist ethos. Social Science & Medicine, 33(5), 559-568.

Lynch-Wood, G., & Williamson, D. (2010). Regulatory compliance: organizational capacities and regulatory strategies for environmental protection. In H. Quirk, T. Seddon & G. Smith (Eds.), Regulation and Criminal Justice: Innovations in Policy and Research (pp. 134). United Kingdom: Cambridge University Press.

Macdonald, K. (2007). Globalising justice within Coffee supply chains? Fair Trade, Starbucks and the transformation of supply chain governance. Third World Quarterly, 28(4), 793-812.

Maertens, M., & Swinnen, J. F. M. (2009). Trade, Standards, and Poverty: Evidence from Senegal. World Development, 37(1), 161-178.

Maijoor, S., & Van Witteloostuijn, A. (1996). An empirical test of the resource-based theory: Strategic regulation in the Dutch audit industry. Strategic Management Journal, 17(7), 549-569.

Majone, G. (2002). What price safety? The precautionary principle and its policy implications. Journal of Common Market Studies, 40(1), 89-109.
Malhotra, A., Gosain, S., & El Sawy, O. A. (2005). Absorptive capacity configurations in supply chains: Gearing for partner-enabled market knowledge creation. Mis Quarterly, 29(1), 145-187.
Manning, L., Baines, R. N., & Chadd, S. A. (2005). Deliberate contamination of the food supply chain. British Food Journal, 107(4/5), 225.
Maranon, B. (1997). La agroexportación no tradicional de México y Perú. Comercio Exterior, 47(12), 997-1006.
Matopoulos, A., Vlachopoulou, M., Manthou, V., & Manos, B. (2007). A conceptual framework for supply chain collaboration: empirical evidence from the agri-food industry. Supply Chain Management: An International Journal, 12(3), 177-186.
McCarthy, T., M., & Golicic, S., L. (2002). Implementing collaborative forecasting to improve supply chain performance. International Journal of Physical Distribution & Logistics Management, 32(6), 431.
McGee, J. (1998). Commentary on 'corporate strategies and environmental regulations: An organizing framework' by A. M. Rugman and A. Verbeke. Strategic Management Journal, 19(4), 377-387.
McInerney, T. F. (2004). Implications of High Performance Production and Work Practices for Theory of the Firm and Corporate Governance. Colum. Bus. L. Rev., 135.
McInerney, T. F. (2007). Putting Regulation Before Responsibility: Towards Binding Norms of Corporate Social Responsibility. Cornell International Law Journal, 40, 171.
McLeish, C., & Nightingale, P. (2007). Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and security policy. Research Policy, 36(10), 1635-1654.
Meidinger, E. E. (2006). The Administrative Law of Global Private-Public Regulation: the Case of Forestry. Eur J Int Law, 17(1), 47-87.
Meidinger, E. E. (2009). Private Import Safety Regulation and Transnational New Governance. In Cary Coglianese, Adam Finkel & David Zaring (Eds.), Import Safety: Regulatory Governance in the Global Economy (pp. 233). Philadelphia: University of Pennsylvania Press.
Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. London: Sage Publications.
Mill, J. S. (1867). A system of logic, ratiocinative and inductive. Toronto: Toronto University Press.
Millstone, E. (1994). Regulation, Innovation and Public Welfare: The Example of the Food Industry. Technology Analysis & Strategic Management, 6(3), 329.
Montealegre, R. (2002). A Process Model of Capability Development: Lessons from the Electronic Commerce Strategy at Bolsa de Valores de Guayaquil. Organization Science, 13(5), 514.
Monteverde, K., & Teece, D. J. (1982). APPROPRIABLE RENTS AND QUASI-VERTICAL INTEGRATION. Journal of Law & Economics, 25(2), 321-328.
Moreno-Luzon, M. D., & Lloria, M. B. (2008). The role of non-structural and informal mechanisms of integration and coordination as forces in knowledge creation. British Journal of Management, 19(3), 250-276.

Mowery, D. C., Oxley, J. E., & Silverman, B. S. (1996). Strategic Alliances and Interfirm Knowledge Transfer. Strategic Management Journal, 17(Winter Special Issue), 74-77.

Muradian, R., & Pelupessy, W. (2005). Governing the coffee chain: The role of voluntary regulatory Systems. World Development, 33(12), 2029-2044.

Nadvi, K. (2008). Global standards, global governance and the organization of global value chains. Journal of Economic Geography, 8(3), 323-343.

Nefussi, J., & Priolon, J. (1997, Jun 12-13). Coordination without vertical integration: The case of the French food system. Paper presented at the Conference on Vertical Relationships and Coordination in the Food System, Piacenzo, Italy.

Nelson, R. R. (1994). The Co-evolution of Technology, Industrial Structure, and Supporting Institutions. Ind Corp Change, 3(1), 47-63.

Nelson, R. R., & Winter, S. G. (1975). Growth theory from an evolutionary perspective: The differential productivity puzzle. The American Economic Review, 65(2), 338-344.

Nganje, W., Bier, V., Han, H., & Zack, L. (2008). Models of Interdependent Security along the Milk Supply Chain. American Journal of Agricultural Economics, 90(5), 1265.

Nganje, W., Richards, T., Bravo, J., Hu, N., Kagan, A., Acharya, R., et al. (2009). Food Safety and Defense Risks in U.S.-Mexico Produce Trade. Choices, 24, 16-20.

Nganje, W., Wilson, W. W., & Nolan, J. (2004). Agro-terrorism and the Grain Handling Systems in Canada and the United States. A Journal of the Canadian Agricul tural Economics Society, 5 (Current Agriculture, Food & Resource Issues), 148-159.

Nicholas Hughes, A. (2006). The container security initiative costs, implications and relevance to developing countries. Public Administration and Development, 26(5), 439-447.

Nielsen, V., & Parker, C. (2008). To What Extent Do Third Parties Influence Business Compliance? Journal of Law and Society, 35(3), 309-340.

Nightingale, P. (2004). Technological capabilities, invisible infrastructure and the un-social construction of predictability: the overlooked fixed costs of useful research. Research Policy, 33(9), 1259-1284.

Nightingale, P. (2008). Meta-paradigm change and the theory of the firm. Ind Corp Change, 17(3), 533-583.

Nooteboom, B. (2009). A cognitive theory of the firm: learning, governance and dynamic capabilities. UK and US: Edward Elgar Publishing.

Nunez-Noriega, L., & Salazar-Solano, V. (2007). Criterios para la Definicion del Modelo de Centro de Investigacion en Alimentacion y Desarrollo del Estado de Nayarit. Tepic, Nayarit: Consejo Nacional de Ciencia y Tecnología, Universidad Autónoma de Nayarit. Centro de Investigación en Alimentación y desarrollo A.C.

Nunez, J. (2007). Can self regulation work? : a story of corruption, impunity and cover-up. Journal of Regulatory Economics, 31(2), 209-233.

O'Toole, T., & Donaldson, B. (2000). Relationship Governance Structures and Performance. Journal of Marketing Management, 16(4), 327-341.

OECD. (2000). Reducing the risk of policy failure: Challenges for Regulatory Compliance. Retrieved from www.oecd.org.

Office of Management and Budget. (2006a). Budget of the United States Government Fiscal Year 2007. Retrieved 510/5/2006. From http://www.gpoaccess.gov/usbudget/fy07/index.html

Office of Management and Budget. (2006b). Historical Tables, Budget of the United States Government, Fiscal Year 2007. Retrieved 12/5/2006. From http://www.gpoaccess.gov/usbudget/fy07/pdf/hist.pdf.

Ogus, A. (1995). Rethinking self-regulation. Oxford Journal of Legal Studies, 15(1), 97-108.

Palac-McMiken, E. (2004). Combating Terrorism in the Transport Sector. Economic Costs and Benefits. Retrieved from http://www.mipt.org/pdf/Combating-Terrorism-Transport-Sector-AU.pdf.

Parashes, P. T. (1978). Legal Overview of the OSHA Noise Standard, A. Akron L. Rev., 12, 55.

Paraskevopoulou, E. (2008). Evolutionary Dynamics of Hidden Innovation Policy: Regulation and Innovation in the Detergents Industry. Unpublished Thesis submitted to the University of Manchester for the degree of Doctor of Philosophy in the Faculty of Humanities, University of Manchester, Manchester, UK.

Parker, C. (2000). Reinventing regulation within the corporation - Compliance-oriented regulatory innovation. Administration & Society, 529-565.

Parker, C. (2006). The “compliance” trap: The moral message in responsive regulatory enforcement. Law & Society Review, 40(3), 591-622.

Patnayakuni, R., Rai, A., & Seth, N. (2006). Relational antecedents of information flow integration for supply chain coordination. Journal of Management Information Systems, 23(1), 13-49.

Pavitt, K. (1984). Sectoral patterns of technical change: Towards a taxonomy and a theory. Research Policy, 13(6), 343-373.

Pavitt, K. (1998). Technologies, products and organization in the innovating firm: What Adam Smith tells us and Joseph Schumpeter doesn't. Industrial and Corporate Change, 7(3), 433-452.

Peck, H., & Juttner, U. (2000). Strategy and relationships: Defining the interface in supply chain contexts. International Journal of Logistics Management, 11(2), 33-44.

Penrose, E. T. (1955). Limits to the Growth and Size of Firms. The American Economic Review, 45(2), 531-543.

Penrose, E. T. (1956). FOREIGN-INVESTMENT AND THE GROWTH OF THE FIRM. Economic Journal, 66(262), 220-235.

Penrose, E. T. (1960). THE GROWTH OF THE FIRM - A CASE-STUDY - THE HERCULES-POWDER-COMPANY. Business History Review, 34(1), 1-23.

Perez Sanchez, D., Barton, J. R., & Bower, D. (2003). Implementing environmental management in SMEs. Corporate Social Responsibility and Environmental Management, 10(2), 67-77.

Perry, A. (2011). ARS Scientists Study the Ins and Outs of E. coli Contamination. Agricultural Research Magazine, April 2011, 7.

Petersen, K. J., Handfield, R. B., & Ragatz, G. L. (2003). A Model of Supplier Integration into New Product Development. Journal of Product Innovation Management, 20(4), 284-299.

Petroni, A. (1998). The analysis of dynamic capabilities in a competence-oriented organization. Technovation, 18(3), 179-189.

Pettus, M. L., Kor, Y. Y., & Mahoney, J. T. (2009). A theory of change in turbulent environments: the sequencing of dynamic capabilities following industry deregulation. International Journal of Strategic Change Management, 1(3), 186-211.

Pfarrer, M. D., Smith, K. G., Bartol, K. M., Khanin, D. M., & Zhang, X. M. (2008). Coming forward: The effects of social and regulatory forces on the voluntary

restatement of earnings subsequent to wrongdoing. Organization Science, 19(3), 386-403.
Philbrick, M. (2010). An Anticipatory Governance Approach to Carbon Nanotubes. Risk Analysis, 30(11), 1708-1722.
Phillips, W., Lamming, R. C., Bessant, J., & Noke, H. (2006). Discontinuous innovation and supply relationships: strategic dalliances. R&D Management, 36(4), 451-461.
Pietrobelli, C., & Saliola, F. (2008). Power relationships along the value chain: multinational firms, global buyers and performance of local suppliers. Cambridge Journal of Economics.
Pilkington, A. (1998). The fit and misfit of technological capability: Responses to vehicle emission regulation in the US. Technology Analysis & Strategic Management, 10(2), 211.
Pinch, T. J., & Bijker, W. E. (1984). The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other. Social Studies of Science, 14(3), 399-441.
Poland, B. D. (1995). Transcription Quality as an Aspect of Rigor in Qualitative Research. Qualitative Inquiry, 1(3), 290-310.
Porter, M. E. (1991). Towards a Dynamic Theory of Strategy. Strategic Management Journal, 12, 95-117.
Porter, M. E., & van der Linde, C. (1995). Toward a New Conception of the Environment-Competitiveness Relationship. The Journal of Economic Perspectives, 9(4), 97-118.
Premus, R., & Sanders, N. (2003). A Framework for Strategic Sourcing. Academy of Strategic Management Journal, 2, 49.
Prencipe, A. (2004). Corporate Strategy and Systems Integration Capabilities: Managing Networks in Complex Systems Industries. In A. Prencipe, A. Davies & M. Hobday (Eds.), The business of systems integration. USA: Oxford University Press.
Priem, R. L., & Butler, J. E. (2001). Tautology in the resource-based view and the implications of externally determined resource value: further comments. Academy of Management Review, 26(1), 57-66.
Prieto, I. M., & Easterby-Smith, M. (2006). Dynamic capabilities and the role of organizational knowledge: an exploration. European Journal of Information Systems, 15(5), 500-510.
PUBLIC HEALTH SECURITY AND BIOTERRORISM PREPAREDNESS AND RESPONSE ACT OF 2002, US Congress, 107 Sess., 116 Cong. Rec. 593-697 (2002).
Rabin, R. L. (1986). Federal regulation in historical perspective. Stanford Law Review, 38(5), 1189-1326.
Ragin, C. (1987). The comparative method: Moving beyond qualitative and quantitative strategies. US: University of California Press.
Ragin, C. (1989). The comparative method: Moving beyond qualitative and quantitative strategies. US: University of California Press.
Ragin, C. (2000). Fuzzy-set social science. US: University of Chicago Press.
Ragin, C., & Strand, S. I. (2008). Using qualitative comparative analysis to study causal order - Comment on Caren and Panofsky (2005). Sociological Methods & Research, 36(4), 431-441.
Rama, R., & Rello, F. (1979). La internacionalización de la agricultura. Estudios rurales latinoamericanos, 2(2), 199-223.

Raynaud, E., Sauvee, L., & Valceschini, E. (2005). Alignment between Quality Enforcement Devices and Governance Structures in the Agro-food Vertical Chains. Journal of Management and Governance, 9(1), 47-77.

Raynaud, E., Sauvee, L., & Valceschini, E. (2009). Aligning branding strategies and governance of vertical transactions in agri-food chains. Ind Corp Change, 18(5), 835-868.

Reardon, T. (2006). The rapid rise of supermarkets and the use of private standards in their food product procurement systems in developing countries. In R. Ruben, M. Slingerland & H. Nijhoff (Eds.), Agro-Food Chains and Networks for Development (Vol. 14, pp. 79-105). Dordrecht: Springer.

Reardon, T., Henson, S., & Berdegue, J. A. (2007). Proactive fast-tracking diffusion of supermarkets in developing countries: implications for market institutions and trade. Journal of Economic Geography, 7(4), 399-431.

Reeves, K. A. (2007). Supply chain governance: A case of cross dock management in the automotive industry. Ieee Transactions on Engineering Management, 54(3), 455-467.

Rice, J., & Spayd, P. (2005). Investing in Supply Chain Security. Special Report Series Retrieved 3/4/2006, 2006. From www.businessofgovernment.org

Richards, L. (2005). Handling qualitative data: A practical guide. London: Sage.

Richey, R. G. (2003). Technological readiness and strategic interactive fit: Dynamic capabilities impacting logistics service competency and performance. Unpublished Ph.D., The University of Oklahoma, United States -- Oklahoma.

Rihoux, B. (2003). Bridging the gap between the qualitative and quantitative worlds? A retrospective and prospective view on qualitative comparative analysis. Field Methods, 15(4), 351.

Rihoux, B. (2006). Qualitative comparative analysis (QCA) and related systematic comparative methods: Recent advances and remaining challenges for social science research. International Sociology, 21(5), 679.

Ritchie, J., & Lewis, J. (2003). Qualitative research practice: A guide for social science students and researchers. London: Sage Publications Ltd.

Rivera, J. (2002). Assessing a voluntary environmental initiative in the developing world: The Costa Rican Certification for Sustainable Tourism. Policy Sciences, 35(4), 333-360.

Robertson, P. L., & Langlois, R. N. (1995). Innovation, Networks, and Vertical Integration. Research Policy, 24(4), 543-562.

Rojas, M. (2005). C-TPAT Statistics. In Y. Borbon-Galvez (Ed.). Hermosillo, Mexico.

Romijn, H. (1997). Acquisition of technological capability in development: A quantitative case study of Pakistan's capital goods sector. World Development, 25(3), 359-377.

Romijn, H., & Albaladejo, M. (2002). Determinants of innovation capability in small electronics and software firms in southeast England. Research Policy, 31(7), 1053-1067.

Rubenzer, T. (2008). Ethnic Minority Interest Group Attributes and U.S. Foreign Policy Influence: A Qualitative Comparative Analysis. Foreign Policy Analysis, 4(2), 169-185.

Rugman, A. M. (1997). Canada. In J. H. Dunning (Ed.), Governments, globalization, and international business. USA: Oxford University Press.

Rugman, A. M., & Verbeke, A. (1998). Corporate strategies and environmental regulations: An organizing framework. Strategic Management Journal, 19(4), 363-375.

Sako, M. (2004). Supplier development at Honda, Nissan and Toyota: comparative case studies of organizational capability enhancement. Industrial and Corporate Change, 13(2), 281-308.

Salazar-Solano, V., Sandoval, S., & Wong-Gonzalez, P. (1999). Los Intermediarios Comerciales en la Agricultura Sonorense de Exportacion. Revista de Estudios Sociales de El Colegio de Sonora, 17(Jul-Dec).

Sarathy, R. (2006). Security and the Global Supply Chain. Transportation Journal, 45(4), 28-51.

SC1&5T. (2008). Interview 12/03/2008. In Y. Borbon-Galvez (Ed.). Culiacan, Sinaloa. Mexico.

SC1D. (2007). Interview 28/11/2007. In Y. Borbon-Galvez (Ed.). Nogales Arizona, United States.

SC1E. (2007). Interview 11/12/2007. In Y. Borbon-Galvez (Ed.). Culiacan Sinaloa, Mexico.

SC2E&T. (2008). Interview 09/01/2008. In Y. Borbon-Galvez (Ed.). Sinaloa, Mexico.

SC3D. (2007). Interview 21/11/2007. In Y. Borbon-Galvez (Ed.). Nogales Arizona, United States.

SC3T. (2008). Interview 15/03/2008. In Y. Borbon-Galvez (Ed.). Culiacan Sinaloa, Mexico.

Scharfeld, T. A. (2003). Compliance and Certification: Ensuring RFID Interoperability: The MIT Auto-ID Center.

Scheppele, K. L. (1988). Legal Secrets: Equality and Efficiency in the Common Law. Chicago; London: University of Chicago Press.

Schneider, C., & Wagemann, C. (2010). Standards of Good Practice in Qualitative Comparative Analysis (QCA) and Fuzzy-Sets. Comparative Sociology, 9, 397-418.

Schot, J., Hoogman, R., & Elzen, B. (1994). Strategies for shifting Technological Systems. The case of the automobile system. Futures, 26(10), 1060-1076.

Schot, J., & Rip, A. (1996). The past and future of constructive technology assessment. Technological Forecasting and Social Change, 54(2-3), 251-268.

Scott, W. R. (1987). The adolescence of Institutional Theory. Administrative Science Quarterly, 32(4), 493-511.

Seuring, S. (2006). Case study research in supply chains-An outline and three examples. In H. Kotzab, Seuring, S., Muller, M., Reiner, G. (Ed.), Research Methodologies in Supply Chain Management (pp. 235-250). NY: Physica-Verlag.

Shannon, D. L., Lee, G. Y. H., & Stephenson, C. A. (2006). United States Patent No. 7129837. U. S. P. A. T. Office.

Shavell, S. (1983). Liability for harm versus regulation of safety. Journal of Legal Studies, 13(2), 357-374.

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. International Journal of Logistics Management, 12(2), 1-12.

Sherman, J. D. (2004). Optimal modes and levels of integration, and the identification of cross-functional coordination deficiencies in concurrent engineering. Ieee Transactions on Engineering Management, 51(3), 268-278.

Sheu, C., Lee, L., & Niehoff, B. (2006). A voluntary logistics security program and international supply chain partnership. Supply Chain Management: An International Journal, 11, 363-374.

Silverman, D. (2005). Doing qualitative research: A practical handbook. London: Sage Publications Ltd.

Singapore Customs. (2007). Secure Trade Partnership Programme (STP). Retrieved 21/07/2008. From http://www.customs.gov.sg/topNav/new/Launch+of+STP.htm.

Sirmon, D. G., Hitt, M. A., & Ireland, R. D. (2007). Managing firm resources in dynamic environments to create value: Looking inside the black box. Academy of Management Review, 32(1), 273-292.

Smith, M., & Crotty, J. (2008). Environmental regulation and innovation driving ecological design in the UK automotive industry. Business Strategy and the Environment, 17(6), 341-349.

Song, M., Droge, C., Hanvanich, S., & Calantone, R. (2005). Marketing and technology resource complementarity: An analysis of their interaction effect in two environmental contexts. Strategic Management Journal, 26(3), 259-276.

Sporleder, T. L. (1994). Assessing Vertical Strategic Alliances by Agribusiness. Canadian Journal of Agricultural Economics, 42(4), 533-540.

Sproull, L. S. (1981). RESPONSE TO REGULATION - AN ORGANIZATIONAL PROCESS FRAMEWORK. Administration & Society, 12(4), 447-470.

Squire, B., Cousins, P. D., & Brown, J. R. (2009). Cooperation and Knowledge Transfer within Buyer–Supplier Relationships: The Moderating Properties of Trust, Relationship Duration and Supplier Performance. British Journal of Management, 20(4), 461-477.

Stenzel, P. L. (2000). Can the ISO 14000 Series Environmental Management Standards Provide a Viable Alternative to Government Regulation? American Business Law Journal, 37(2), 237-298.

Stewart, R. B. (1981). Regulation, Innovation, and Administrative Law: A Conceptual Framework. California Law Review, 69(5), 1256.

Strange, R. (2009). The outsourcing of primary activities: theoretical analysis and propositions. Journal of Management and Governance, 1-21.

Stuart, D. (2008). The illusion of control: industrialized agriculture, nature, and food safety. Agriculture and Human Values, 25(2), 177-181.

Stuart, I., McCutcheon, D., Handfield, R. B., McLachlin, R., & Samson, D. (2002). Effective case research in operations management: a process perspective. Journal of Operations Management, 20(5), 419-433.

Suarez-Bello, M. (2003). A case study approach to the supplier selection process. Unpublished Master Thesis, University of Puerto Rico, Anasco, Puerto Rico.

Sunstein, C. R. (1997). Free markets and social justice. New York, Oxford: Oxford University Press.

Sutinen, J. G., & Gauvin, J. R. (1989). An Econometrics Study of Regulatory Enforcement and Compliance in the Commercial Inshore Lobster Fishery of Massachusetts. In P. A. Neher, R. Arnason & N. Mollet (Eds.), Rights based fishing (pp. 414–428). Dordrecht, Boston, London: Kluwer Academic Publishers.

Tallontire, A. (2007). CSR and regulation: towards a framework for understanding private standards initiatives in the agri-food chain. Third World Quarterly, 28(4), 775 - 791.

Teece, D. J. (1986). Profiting from Technological Innovation - Implications for Integration, Collaboration, Licensing and Public-Policy. Research Policy, 15(6), 285-305.

Teece, D. J., & Pisano, G. (1994). The Dynamic Capabilities of Firms: an Introduction. Ind Corp Change, 3(3), 537-556.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. Strategic Management Journal, 18(7), 509-533.

Tran, T. A., & Daim, T. (2008). A taxonomic review of methods and tools applied in technology assessment. Technological Forecasting and Social Change, 75(9), 1396-1405.

Tyler, T. R. (2006). Why people obey the law. New Jersey, US, and Oxfordshire, UK: Princeton University Press.

United States Sentencing Commission, Guidelines Manual, §3E1.1, (nov. 2009).

van den Berg, H. (2008). Knowledge-based Vertical Integration: The Nature of Knowledge and Economic Firm Boundary Location. Unpublished Thesis, University of Toronto, Toronto, US.

van der Vorst, J. G. A. J., Beulens, A. J. M., de Wit, W., & van Beek, P. (1998). Supply chain management in food chains: improving performance by reducing uncertainty. Paper presented to the Seventh International Special Conference of IFORS: `Information Systems in Logistics and Transportation', Gothenburg, Sweden, 16-18 June 1997. International Transactions in Operational Research, 5(6), 487-499.

van Merkerk, R. O., & Smits, R. E. H. M. (2008). Tailoring CTA for emerging technologies. Technological Forecasting and Social Change, 75(3), 312-333.

Vink, M. P., & Van Vliet, O. (2009). Not Quite Crisp, Not Yet Fuzzy? Assessing the Potentials and Pitfalls of Multi-value QCA. Field Methods, 21(3), 265-289.

Viscusi, W. K. (1979). The Impact of Occupational Safety and Health Regulation. The Bell Journal of Economics, 10(1), 117-140.

Viscusi, W. K. (1988). Product Liability and Regulation: Establishing the Appropriate Institutional Division of Labor. American Economic Review, 78(2), 300.

Viscusi, W. K. (1995). Fatal tradeoffs: Public and private responsibilities for risk. USA: Oxford University Press.

Viscusi, W. K., Vernon, J. M., & Harrignton, J. E. J. (1995). Economics of Regulation and Antitrust (Second Edition ed.). US, UK: The MIT Press.

Vlachos, J. (2004). Do Regulatory Similarities Increase International Portfolio Holdings? SSRN eLibrary.

von Tunzelmann, N. (2003). Historical coevolution of governance and technology in the industrial revolutions. Structural Change and Economic Dynamics, 14(4), 365-384.

von Tunzelmann, N., & Wang, Q. (2003). An evolutionary view of dynamic capabilities. Economie Appliquee, LVI(3), 33-64.

von Tunzelmann, N., & Wang, Q. (2007). Capabilities and production theory. Structural Change and Economic Dynamics, 18, 192-211.

Wernau, J. (2010). Consumers pushed to Tylenol alternatives. Retailers use shortage to promote store brands as safe, effective substitutes. Tribune Newspapers. Retrieved 2 January 2011. From healthkey.com/health/drugs-medicines/tylenol-(drug)/sns-health-tylenol-alternatives,0,2774600.story

Wernerfelt, B. (1984). A Resource-Based View of the Firm. Strategic Management Journal, 5(2), 171-180.

Wigger, A., & Nolke, A. (2007). Enhanced roles of private actors in EU business regulation and the erosion of Rhenish capitalism: The case of antitrust enforcement. Jcms-Journal of Common Market Studies, 45(2), 487-513.

Williams, R., & Edge, D. (1996). The social shaping of technology. Research Policy, 25(6), 865-899.

Williamson, O. E. (1971). VERTICAL INTEGRATION OF PRODUCTION - MARKET FAILURE CONSIDERATIONS. American Economic Review, 61(2), 112-127.

Williamson, O. E. (1981). The Economics of Organization: The Transaction Cost Approach. The American Journal of Sociology, 87(3), 548-577.

Williamson, O. E. (1991). Comparative Economic Organization: The Analysis of Discrete Structural Alternatives. Administrative Science Quarterly, 36(2), 269-296.

Williamson, O. E. (2002). The Theory of the Firm as Governance Structure: From Choice to Contract. The Journal of Economic Perspectives, 16(3), 171-195.

Willis, H. H., & Ortiz, D. S. (2004). Evaluating the security of the global containerized supply chain: Rand Corp.

Wilson, P. N., & Thompson, G. D. (2003). Time Integration: Agribusiness Structure for Competitive Advantage. Review of Agricultural Economics, 30-43.

Wilson, P. N., Thompson, G. D., & Cook, R. L. (1997). Mother nature, business strategy, and fresh produce. Choices (Ames, Iowa)(USA), First Quarter.

Wilson, R. (1997). The conformance vs. compliance debate. Pollution Engineering, 29(7), 47.

Winter, S. G. (2000). The satisficing principle in capability learning. Strategic Management Journal, 21(10-11), 981-996.

Winter, S. G. (2003). Understanding dynamic capabilities. Strategic Management Journal, 24(10), 991.

Winter, S. G., & Szulanski, G. (2001). Replication as strategy. Organization Science, 12(6), 730-743.

Wong-Gonzalez, P. (2005). CiberPuerto: Infraestructura Fronteriza, Competitividad y Desarrollo en la Region Sonora-Arizona: Hermosillo, Mexico: SIUE-Gobierno del Estado de Sonora. CIAD. CEE.

Wood, M. (2011). ARS Scientists Study the Ins and Outs of E. coli Contamination. Agricultural Research Magazine, April 2011, 14-15.

World Customs Organizations. (2007). SAFE framework of standards. Retrieved 29/04/2011. From http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/SAFE%20Framework_EN_2007_for_publication.pdf.

Yamin, S., Mavondo, F., Gunasekaran, A., & Sarros, J. C. (1997). A study of competitive strategy, organisational innovation and organisational performance among Australian manufacturing companies. International Journal of Production Economics, 52(1-2), 161-172.

Yapp, C., & Fairman, R. (2006). Factors affecting food safety compliance within small and medium-sized enterprises: implications for regulatory and enforcement strategies. Food Control, 17(1), 42-51.

Yin, R. (2003). Case study research. Design and Methods. California: Sage Publications Ltd.

Zhou, Y., Zhang, Z., & Liu, K. (2005). Impact of Technological Innovation on Growth Trajectory of Enterprise's Technological Capability: A Theoretical Analysis. Singapore Management Review, 27(2), 81-101.

Zilinskas, R. (2003). Bioterrorism Threat Assessment and Risk Management Workshop: Final Report and Commentary (Final Report and Commentary). Washington, DC: Monterey Institute of International Studies.

Zollo, M., & Winter, S. G. (2002). Deliberate learning and the evolution of dynamic capabilities. Organization Science, 13(3), 339-351.