

ABSTRACT

IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES: IMPROVING
THE GLOBAL SUPPLY CHAIN THROUGH TIGHTENING INFORMATION
TECHNOLOGY SECURITY

By

Kamal Kakish

MS ICS, Georgia Institute of Technology, 1988

BS ICS, Georgia Institute of Technology, 1982

Dissertation Submitted to the

Graduate Faculty of the College of Management

in Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF MANAGEMENT IN INFORMATION TECHNOLOGY

DISSERTATION COMMITTEE CHAIR: A.L. Steenkamp

Lawrence Technological University

December 7, 2007

IT HOSTED GLOBAL SUPPLY CHAIN SECURITY

SERVICES

IMPROVING THE GLOBAL SUPPLY CHAIN THROUGH TIGHTENING

INFORMATION TECHNOLOGY SECURITY

(FINAL DRAFT)

By:

Kamal M. Kakish

Dissertation Committee

Dr. Annette L. Steenkamp, LTU, Supervisor and Chair

Dr. S. Alan McCord, LTU, Academic Advisor

Mrs. Pat Snack, AIAG-GM, Industry Advisor

Graduate College of Management

Lawrence Technological University

December 7, 2007

ABSTRACT

Automotive Global Supply Chain (GSC) trade and transport is very complex. It involves multiple players and a gigantic number of complex transactions. Consequently, there is a constant need to obtain, analyze, and exchange data securely and compliantly.

The rapid changes in Information Technologies coupled with political and socio-economic factors are continuously transforming international trade and transport operations. However, much of the exchange of transactional data among international businesses remains electronically fragmented – parts of the data exchange are paper based and other parts are electronic. In recent years, world organizations have increasingly emphasized the importance of GSC security and compliance (e.g. World Customs Organization WCO SAFE Framework™ and Data Model, UN Recommendation 33, etc). Such phenomenon further complicates the ability to comply and exchange electronic data securely - and efficiently - within the GSC, since there is lack of congruence among standards to which an organization must comply.

In many security informatics applications, it is important to monitor traffic over various communication channels and efficiently identify those communications that are unusual for further investigation. Therefore, this research intends to analyze the GSC data exchange and trade compliance dynamics, and propose a conceptual solution (design model) along with a systematic approach to implement such a solution in a manner that could improve IT security and compliance levels in the USA and across the globe, especially in developing countries.

The hypothesis for this research is:

“The security of the global supply chain may be improved if all participating trading partners adopt a systematic approach to information exchange.”

The literature review shows that a significant portion of processing GSC documents in the automotive industry is still paper based. Although there are several research initiatives and an abundance of trade and data exchange standards, little is done to improve the situation, especially in underdeveloped countries. Therefore, one continues to see significant transport delays and increases in the potential for errors and exposures.

The conceptual model proposed by this research, and detailed in Chapter 4, involves establishing a GSC Hosted IT Security Infrastructure Framework coupled with a GSC IT Security Policy that aligns and interoperates with UN Recommendation 33 and is recommended to be imbedded within the WCO Data Model.

The research sought to explain strategic issues related to IT management and industry participants behavior. The study used a mixed-methods descriptive research design using a questionnaire and a set of 11 interviews, with representatives from the automotive industry, as the primary means for data collection.

The analysis of the research findings confirmed the hypothesis. The results of the questionnaire demonstrated a statistical correlation between IT Security and trade compliance. These results are beneficial to GSC IT Security administrators, technical, and operational specialists.

Keywords:

Global Supply Chain (GSC), IT Security, Hosted IT Services, Secure Electronic Transport

IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES: IMPROVING
THE GLOBAL SUPPLY CHAIN THROUGH TIGHTENING INFORMATION
TECHNOLOGY SECURITY

By:

Kamal M. Kakish

MS ICS, Georgia Institute of Technology, 1988

BS ICS, Georgia Institute of Technology, 1982

Dissertation Submitted to the
Graduate Faculty of the College of Management
in Partial Fulfillment of the Requirements for the Degree of

DOCTOR OF MANAGEMENT IN INFORMATION TECHNOLOGY

DISSERTATION COMMITTEE CHAIR: A.L. Steenkamp

Lawrence Technological University

December 7, 2007

UMI Number: 3423949

All rights reserved

INFORMATION TO ALL USERS

The quality of this reproduction is dependent upon the quality of the copy submitted.

In the unlikely event that the author did not send a complete manuscript and there are missing pages, these will be noted. Also, if material had to be removed, a note will indicate the deletion.



UMI 3423949

Copyright 2010 by ProQuest LLC.

All rights reserved. This edition of the work is protected against unauthorized copying under Title 17, United States Code.



ProQuest LLC
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106-1346

LAWRENCE TECHNOLOGICAL UNIVERSITY

COLLEGE OF MANAGEMENT

**IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES:
IMPROVING THE GLOBAL SUPPLY CHAIN THROUGH TIGHTENING
INFORMATION TECHNOLOGY SECURITY**

This Dissertation Was Presented And Defended By:

KAMAL M. KAKISH

And Was Approved On:

December 7, 2007

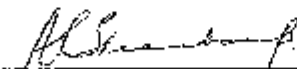
Approved By:

Dr. Annette L. Strunkamp, LTU, Supervisor and Chair

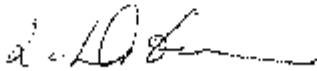
Dr. S. Alan McCurd, LTU, Academic Advisor

Mrs. Pat Snack, ALAG-CM, Industry Advisor

ACCEPTED AND SIGNED:



ANNETTE L. STRUNKAMP, Ph.D.
DMIT Program Director



LOUIS DEGENNARO, J.D.
Dean, College of Management

LAWRENCE TECHNOLOGICAL UNIVERSITY

COLLEGE OF MANAGEMENT

**IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES:
IMPROVING THE GLOBAL SUPPLY CHAIN THROUGH TIGHTENING
INFORMATION TECHNOLOGY SECURITY**

This Dissertation Was Presented And Defended By:

KAMAL M. KAKISH

And Was Approved On:

December 7, 2007

Approved By:

Dr. Annette L. Steenkamp, LTU, Supervisor and Chair

Dr. S. Alan McCord, LTU, Academic Advisor

Mrs. Pat Snack, AIAG-GM, Industry Advisor

ACCEPTED AND SIGNED:

ANNETTE L. STEENKAMP, Ph.D.

LOUIS DEGENNARO, J.D.
Dean, College of Management

DEDICATION

I dedicate this effort to my mother, who was educated to the third elementary grade only, yet had the wisdom that surpasses common understanding. The one who insisted that knowledge and the fear of God is what we can arm ourselves with at all times.

I also dedicate this work to my children Lydia, Lauren, and Daniel so they would continue the journey of life-time learning. So they could see that life is a never-ending learning process, and that at age 48 it is still possible to earn a doctorate degree in an advanced field.

ACKNOWLEDGMENTS

First and foremost, I want to thank my Lord and Savior Jesus Christ for giving me the courage, will, tenacity, and ability to perform this research. Yes indeed, “I can do ALL things through Christ who gives me strength” *Philippians 4:12*.

I am privileged to have some very special friends who lived through the entire DMIT experience with me. In particular, I thank Theresa Kraft and her husband John (and Lynn) for their sacrificial love and generous hearts. You are like family to me. I am forever indebted to your kindness.

I thank Dr. Steenkamp, who for many years has been a friend, a colleague, a co-author, and mentor. She exemplifies the meaning of scholarship in everything she does. I am honored to have Dr. Steenkamp as my DISCOM chair advisor. I thank Mrs. Pat Snack, my industry adviser, who showed me the true meaning of character. Her knowledge and expertise in the automotive industry is unmatched. Thank you for the tons of sacrifices you made for me and for taking care of arranging and attending the interviews, despite caring for your ill husband. Many thanks go to Dr. Al McCord, my friend and mentor, for his support, especially during the earlier part of my research. He is the best professor one could hope to have.

Last but not least, I’m indebted to several friends and loved ones for their endless support during my DMIT experience. I want to thank my sister Kaucab for her unconditional love and constant support. I also thank my brothers Dr. Jeries Qaqish and Mr. Jamal Qaqish for their frequent follow-ups and encouragements.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION.....	1
1.1 Background Theory and Application	3
1.1.1 The What	4
1.1.2 Current Situation.....	9
1.1.3 The Why	12
1.1.4 The Scope	13
1.1.5 The Focus.....	16
1.2 Focal Theory and Application.....	19
1.2.1 Components of the Global Supply Chain.....	21
1.3 The Research Problem	23
1.3.1 Current Problems.....	24
1.3.2 WCO Security Concerns	25
1.4 Brief Overview of Literature Review	26
1.5 Purpose of the Study	26
1.5.1 Research Objectives	27
1.6 Justification for the Study	28
1.7 Benefits of the Study	30
1.8 Research Questions and Hypothesis.....	31

1.9 Overview of the Research Strategy	34
1.10 Interviews and Questionnaire.....	38
1.11 Principles and Objectives of the Conceptual Solution.....	40
1.12 Contribution of the Dissertation.....	42
1.13 Chapter Summary.....	44
1.14 Outline of the Dissertation.....	44
CHAPTER 2 LITERATURE REVIEW	48
2.1 The Importance of GSC IT Security.....	54
2.1.1 The Significance of Compliance with GSC IT Security	57
2.1.2 Challenges of IT Security and Compliance in the GSC	61
2.1.3 Compliance Challenges.....	64
2.2 Literature Specific to the Hypothesis	65
2.2.1 State Of Information Exchange	67
2.2.2 Importance of Risk Planning and Effective Compliance	68
2.3 Technologies	72
2.3.1 RFID Potential for Operations.....	73
2.3.2 Legacy Systems and RFID	78
2.3.3 Current and Emerging GSC IT Security Technologies.....	79
2.3.3.1 Neutron-based Detectors	80
2.3.3.2 PFNA™ Technology.....	82

2.3.4 Recommended GSC IT Security Technologies	83
2.4 GSC Electronic Security Management	89
2.4.1 Globalization as a Change Agent	92
2.4.2 Interdependencies as Change Agents	93
2.4.3 Discontinuous Events as Change Agents	94
2.4.4 Principals of Security Management.....	95
2.5 The Strategic Pillars of GSC IT Security	96
2.6 GSC Security Management.....	96
2.6.1 The Security Management Value Creation Model.....	97
2.6.2 The Security Management Approach	98
2.7 Chapter Summary and Conclusions	100
CHAPTER 3 RESEARCH DESIGN AND PROCEDURES.....	102
3.1 Research Approach and Design.....	103
3.1.1 Data Collection Method	105
3.1.1.1 Interview Details	108
3.1.2 Data Analyses Method	113
3.1.3 Least Square Method (LSM)	114
3.1.4 Correlation and Regression Analysis.....	115
3.1.5 Putting the Analyses Together.....	117
3.2 Limitations of the Research Design.....	118
3.2.1 Complexity of Implementation.....	118

3.2.2 The GSC IT Security Policy.....	119
3.2.3 Access to Accurate Data.....	120
3.3 Chapter Summary.....	121
CHAPTER 4 RESEARCH ANALYSIS AND THE CONCEPTUAL SOLUTION	122
4.1 Introduction	122
4.2 Draft Conceptual Model	125
4.2.1 Conceptual Solution: Key Issues.....	132
4.2.2 Conceptual Solution: Skills Requirements	133
4.2.3 GSC IT Security Policy	134
4.3 Conceptual Model: Acceptance Criteria.....	134
4.4 Moving Into Analysis	135
4.4.1 Action Plan that contributed to refining the conceptual Model	135
4.5 Analyses of Research Findings	136
4.5.1 Information Analyses	137
4.5.1.1 Layering of Security Services	139
4.5.2 Gap Analysis.....	140
4.5.3 Analysis of Interview Data that Refined the Conceptual Solution.....	142
4.5.4 Analyses of Questionnaire Data.	144
4.6 Rummler-Brache Performance Matrix & Mappings.....	149
4.7 Refinement of Conceptual Solution: Key Issues and Requirements	150
4.7.1 Refined Conceptual Solution: Data Transportation.....	153

4.7.2 Conceptual Solution: Security Infrastructure Model.....	154
4.8 Systematic Approach for the Conceptual Solution.....	156
4.8.1 Systematic Approach: Process Model.....	157
4.8.2 Systematic Approach: Methodology.....	160
4.8.2.1 Initial Concept Stage.....	161
4.8.2.2 Initial Decision Stage.....	162
4.8.2.3 Feasibility Study Stage.....	162
4.8.2.4 Outsourcing Decision Stage.....	163
4.8.2.5 Feasibility Study Reporting Stage.....	163
4.8.2.6 Implementation Stage.....	164
4.8.2.7 Maintenance Stage.....	164
4.9 Summary and Conclusion.....	165
CHAPTER 5 DEMONSTRATION OF CONCEPT.....	167
5.1 Introduction.....	167
5.2 Overview.....	169
5.3 Demonstration of Concept Validation Criteria.....	169
5.4 Technology Selection Criteria.....	170
5.5 Global Motors Corp USA Business Case.....	173
5.5.1 Implementation Model.....	174
5.5.1.1 USA Model.....	175
5.5.1.2 European Models.....	176

5.6 Implementing GMC USA using the Systematic Approach	177
5.6.1 Initial Concept Stage.....	177
5.6.2 Initial Decision Stage	178
5.6.3 Feasibility Study Stage	178
5.6.4 Outsourcing Decision Stage	179
5.6.5 Feasibility Study Reporting Stage	179
5.6.6 Implementation Stage.....	180
5.6.7 Maintenance Stage	181
5.6.8 Key Factors In Establishing a Successful GSCITSS	182
5.6.8.1 Political Will.....	182
5.6.8.2 Establishment of Clear Project Boundaries and Objectives	183
5.6.8.3 Partnership between Government and Trade	183
5.6.8.4 Communications Strategy	184
5.6.8.5 Strong Advocacy	185
5.6.8.6 User Friendliness and Accessibility	185
5.6.8.7 Legal Environment	186
5.6.8.8 International Standards and Recommendations.....	186
5.6.8.9 Identification of Possible Obstacles.....	187
5.6.8.10 Financial Model.....	188
5.6.8.11 Payment Possibility	188
5.6.8.12 Promotion and Marketing	189
5.7 Chapter Summary and Conclusion.....	190

CHAPTER 6 FINDINGS, CONCLUSIONS, AND CONTRIBUTIONS	191
6.1 Findings Relative to Hypothesis.....	192
6.1.1 Findings Relative to Electronic Data Exchange	193
6.1.2 Findings Relative to Trade Compliance	195
6.1.3 Findings Relative to Best Practices	197
6.1.4 Findings Relative to Situational Awareness	200
6.1.5 Findings Relative to Training.....	201
6.2 Additional Findings.....	203
6.3 Answers to Research Questions.....	204
6.4 Conclusions Related to Hypothesis.....	219
6.5 Evaluation of Demonstration of Concept in Terms of Hypothesis	222
6.6 Other Conclusions	223
6.7 Summary of Contribution.....	225
6.8 Limitations	227
6.9 Recommendations.....	229
6.10 Opportunities for Future Research.....	230
6.11 Summary and Conclusion	232
APPENDIX A TWO-PART INTERVIEWEE QUESTIONNAIRE	1
Appendix A Section 1.....	2
Appendix A Section 2.....	5

Appendix A Section 3 – Performance Matrix	9
APPENDIX B RESEARCH MODELS AND DIAGRAMS	13
Section 1 Meta Model	13
Section 2 – Systematic Approach Process Model Details	14
Section 3 – GMC USA Implementation Model ProVision Details	15
APPENDIX C QUESTIONNAIRE RAW DATA	30
APPENDIX D GSC STANDARDS & RECOMMENDATIONS	31
EXHIBIT ONE WCO SAFE FRAMEWORK PILLAR 1 STANDARDS	38
EXHIBIT TWO WCO SAFE FRAMEWORK PILLAR 2 STANDARDS.....	39
EXHIBIT THREE RECOMMENDED BEST PRACTICES	40
GLOSSARY	41
REFERENCES.....	47
TERMINOLOGY AND ACRONYMS.....	59

LIST OF TABLES

Table 1-1: Comparison between EbXML and Web Services Specifications	2
Table 1-2: List of Research Interviewees & Organizations.....	39
Table 2-1: The Core Principles of Security Management	95
Table 3-1: Data Compiled from Answers to Questionnaire	107
Table 3-2: Interviewee Organizations (continued).....	111
Table 4-1: Global Supply Chain IT Security Gap Analysis Model.....	142
Table 4-2: Questionnaire Data for Security & Compliance	145
Table 4-3: Mapping of ISO 12207 to Rummler-Brache Performance Matrix.....	150
Table 5-1: Technology Assessment Selection Criteria	173
Table 6-1: Correspondence between Findings and Research Questions	222

LIST OF FIGURES

Figure 1-1: Sequence Diagram for Object Information Exchange.....	4
Figure 1-2: Components of SC Collaboration Interoperability Process	22
Figure 1-3: The Inductive-Hypothetic Research Strategy	35
Figure 2-1: A typical representation of a supply chain network.....	49
Figure 2-2: Basic Network Design	51
Figure 2-3: Risk and Compliance Landscape	70
Figure 2-4: Smart Containers.....	76
Figure 2-5: Cargo Inspection Technologies	85
Figure 2-6: SAFESITE™ Multi-Threat Detection System	88
Figure 2-7: GSC Security Management Approach	99
Figure 3-1: Research Process Model	104
Figure 4-1: Draft Conceptual Model.....	127
Figure 4-2: GSC IT Security Conceptual Framework	128
Figure 4-3: Class Model for GSC IT Security Policy	131
Figure 4-4: The Information Hierarchy.....	138
Figure 4-5: GSC IT Basic Security Services/Facilities.....	139
Figure 4-6: Conceptual Layering of Security Services	140
Figure 4-7: Generic Gap Analysis Model.....	141

Figure 4-8: Using Least Square Method to Correlate Security & Compliance....	146
Figure 4-9: Relationship between IT Security and Quality	147
Figure 4-10: Relationship between IT Security and Procurement	147
Figure 4-11: Relationship between IT Security and Governance	148
Figure 4-12: Relationship between IT Security and Business Strategy	148
Figure 4-13: Refined Conceptual Solution.....	152
Figure 4-14: Data Transaction Collaboration Process.....	154
Figure 4-15: Conceptual Solution: Security Infrastructure Model.....	156
Figure 4-16: Systematic Approach Process Model Organizational Form	157
Figure 4-17: Systematic Approach Process Model Top Level	158
Figure 4-18: GSCITSS Systematic Approach Process Model	159
Figure 4-19: Process Model: Initial Concept Stage	160
Figure 6-1: Information Security Operational Model	197

COPYRIGHT

Copyright © 2007 by KAMAL M. KAKISH. All rights reserved

A wise king once said...

"I thought in my heart, "Come now, I will test you with pleasure to find out what is good." But that also proved to be meaningless. I tried cheering myself with wine, and embracing folly—my mind still guiding me with wisdom. I wanted to see what was worthwhile for men to do under heaven during the few days of their lives.

I undertook great projects: I built houses for myself and planted vineyards. I made gardens and parks and planted all kinds of fruit trees in them. I made reservoirs to water groves of flourishing trees. I also owned more herds and flocks than anyone in Jerusalem before me. I amassed silver and gold for myself, and the treasure of kings and provinces. I acquired men and women singers and a harem as well—the delights of the heart of man. I became greater by far than anyone in Jerusalem before me. In all this my wisdom stayed with me.

I denied myself nothing my eyes desired; I refused my heart no pleasure. My heart took delight in all my work, and this was the reward for all my labor.

Yet when I surveyed all that my hands had done and what I had toiled to achieve, everything was meaningless, a chasing after the wind; nothing was gained under the sun.

... ..

Now all has been heard; here is the conclusion of the matter: Fear God and keep his commandments, for this is the whole duty of man."

Excerpts from the Book of Ecclesiastes, Chapters 1 and 12

CHAPTER 1 INTRODUCTION

The Global Supply Chain (GSC) serves as the backbone for international trade, which is an essential driver for economic prosperity and socio-economic development throughout the world. Research has revealed that today's global trading system is electronically fragmented (part paper based and part electronic data exchange) and vulnerable to security exploitations that could severely damage the entire global economy (Apurva & Moinzadeh, 2005). While world government organizations strive to control and administer standards to regulate the global movement of goods, evidence dictates that there exists ominous need to provide increased security and trade compliance in the global supply chain.

Processing and tracking shipment containers across long distances suffers significant problems throughout the world. Such inefficiencies include substantial delays in moving freight, missing critical information, limited end-to-end shipment visibility, split shipments and disruption, but chief of all is the wide exposure to disasters, natural and otherwise, due to the lack of robust information security mechanisms (Caballero, 2005; Katz, 2004). Clearly, these issues are manifested in significant increases in cost and poor delivery

performance. The lack of shipment visibility causes much manual follow-up and exposes the goods to delays that cannot be quickly resolved. Ultimately, it all boils down to business loss that could be avoided. While the causes and the sources of these problems vary widely, one apparent root cause that seems to be commonly agreed upon is electronic information security.

Functional Area	Relevant ebXML Specs	Comparable Web Services Specs
App-to-app Messaging	ebXML Messaging Services (ebMS)	<ul style="list-style-type: none"> ➤ SOAP ➤ WS-Security ➤ XML Signature ➤ XML Encryption ➤ WS-Reliable Messaging
Process Flows	ebXML Business Process Specification Schema (ebBP)	WS-Choreography
Registry	<ul style="list-style-type: none"> ➤ ebXML Registry Services ➤ ebXML Registry Information Model 	UDDI
B2B Collaboration Agreements	ebXML Collaboration-Protocol Profile and Agreement (ebCPP/A)	No comparable spec
Overall architecture specification for B2B collaboration	ebXML Technical Architecture Specification	No comparable spec

Table 1-1: Comparison between EbXML and Web Services Specifications

Over the past 45 years, GSC transactional data sets evolved from the traditional Electronic Data Interchange (EDI), which is based on ANSI X12 and

UN/EDIFACT, to a variety of XML based data types, protocols, and languages. These include but are not limited to ebXML, Web Services, SOAP, WSDL, UDDI, and others. Table 1-1 shows a functional comparison between OASIS ebXML® and WS-I® standards.

1.1 Background Theory and Application

The concept of Web services as a means of dynamically discovering, negotiating, composing, executing and managing services to materialize enterprise-scale workflow is an active research topic. However its realization has thus far been elusive. Existing approaches involve many disparate concepts, frameworks and technologies. What is needed is a comprehensive and overarching framework that handles the processing and workflow requirements of Virtual Enterprises. Such a framework maps GSC processing to a collection of service-oriented tasks, dynamically configures these tasks from available services, and manages the choreography and execution of these services. Hence, an IT hosted global supply chain security services solution is appropriate and necessary. The goal is to **add** semantics and **functionality** to Web services to endow them with **capabilities** currently lacking in the literature, but necessary for their successful deployment in future GSC systems.

1.1.1 *The What*

Typically, there are two main actors within a shipment port community (the forwarding sender and the industry participants' agents). These actors must communicate and coordinate various information flows securely and efficiently. These information flows are exchanged, in most cases, in terms of objects. Figure 1-1 illustrates a sequence diagram for object information exchange within a GSC community.

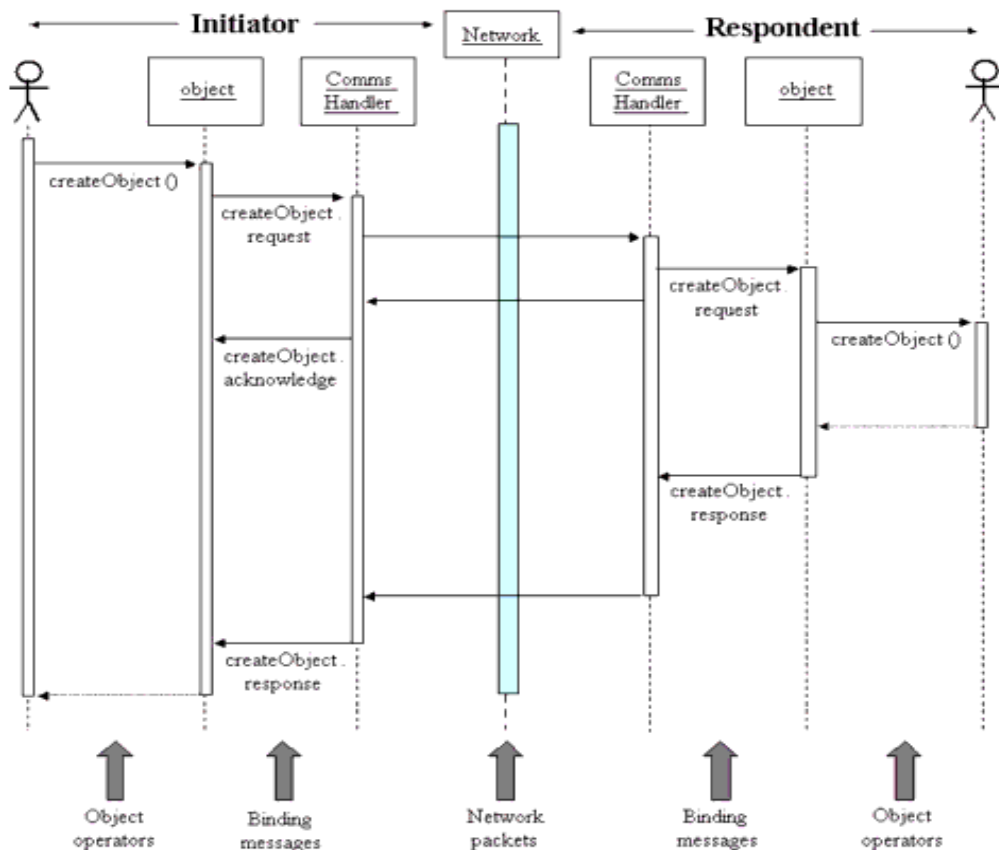


Figure 1-1: Sequence Diagram for Object Information Exchange

Studies have shown that the cost of securing and managing the exchange of information often accounts to about 10% or more of the commercial value of the traded goods (Stamp et al., 2006)ⁱ. Sources of information that could be involved include the port authority, shippers, banks, insurers, carriers, customs, and several others.

The rapid changes in Information Technologies (IT) coupled with political and socio-economic factors are continuously transforming international trade and transport operations. In recent years, governments and business organizations have increasingly emphasized the importance of supply chain security and compliance. This is evidenced by the recent adoption of the World Customs Organization (WCO) Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework – Refer Exhibit ONE), and the significant IT content of trade facilitation measures that are currently negotiated by the World Trade Organization (WTO). Such dynamics further complicate the ability of automotive industry participants to comply and operate efficiently and securely within the GSC. Information technology must support the required physical goods security through accurate and efficient data exchange to provide track and trace capability.

To gain a better appreciation of the magnitude of these issues, one needs to understand the underlying **processes, governances, technologies, tools, and techniques** associated with global supply chain inventory and freight management. However, the scope of this dissertation is focused on the elements of information technology security and trade compliance, with the inclusion of a model that enables third world country SMEs (Small and Medium Enterprises) to participate in GSC Information Security.

A variety of strategies, initiatives, and Internet-based materials and inventory tracking technology types are continually being integrated into supply chain management systems (Camarinha-Matos, 2004). International governments and businesses, as well as world trade and customs organizations have recently taken significant strides in establishing and implementing global standards and technologies in the quest of addressing various security exposures of the global supply chain (Gansler and Luby, 2004). These organizations include the World Customs Organization (WCO) with its Framework of Standards to Secure and Facilitate Global Trade (SAFE) and WCO Data Model (WCO, 2007). Other organizations include the U.S. Customs and Boarder Protection with its Customs Trade Partnership Against Terrorism (C-TPAT) (US CBP, 2003) and C-TPAT

Security Link Internet Web Portal initiatives (US CBP, 2004), the European Union Customs related security initiatives and EC Regulation 648/2005 (European Commission, 2005), along with several other countries that have committed to developing global trade implementation guidelines.

The WCO Data Model establishes an international standard set of harmonized data that will meet governments' requirements for international cross-border trade and is geared exclusively to the requirements of an automated environment. This makes it an **ideal framework in which to embed the GSC IT Security Policy**, discussed in Section 4.2.3.

Consistent information and documentation are key elements in the control of international cross-border trade. In today's interconnected electronic environment these controls will increasingly include information exchange prior to the arrival of the goods in order to provide the necessary level of security as well as acceptable release times.

Standardized and harmonized information requirements and procedures are essential to establish the common understanding which allows for an effective

and efficient exchange of information between all parties involved in the international cross-border movement. The WCO Customs Data Model provides this common understanding on Customs information requirements. The WCO Data Model also provides Contracting Parties of the revised Kyoto Convention a *global customs standard* to implement provisions dealing with reduced data requirements and electronic submission of declarations and supporting documents.

The research hypothesis is formulated, namely that the security of the global supply chain may be improved if all participating trading partners adopt a “systematic approach” to information exchange. This systematic approach is discussed in details in Chapter 4, Section 4.8 and Chapter 5, Section 5.6.

The **goal of this study** is to provide an innovative approach for addressing IT related GSC security issues (electronic data exchange and trade compliance) by examining the practices and technologies within the automotive industry. As such, this study aims to produce a **clearer understanding of the role of IT in improving global supply chain security** and to find out what could be obtained or improved by adopting the “systemic approach” to information exchange by

industry participants. Although the title of this research highlights IT security (systems and infrastructure/networks) within the GSC as the main topic, the conceptual solution on which this research is founded on, inherently addresses physical goods security and transactional (data exchange) security. The security of data in transit and exchanged throughout the GSC networks accounts for a significant portion of the conceptual solution.

1.1.2 *Current Situation*

Automotive GSC trade and transport is very complex. It involves multiple players (AKA Industry Participants – Industry participants) and a very large number of multifaceted transactions. For example, a typical automotive trade transaction may easily involve 30 parties, 40 documents, 200 data elements, and require re-encoding of 60 to 70 per cent of all data at least once. Consequently, there's a constant need to obtain, analyze, and exchange data.

The various industry participants exchange data over the GSC networks by issuing, transferring, and interchanging a huge number of documents containing extensive information. This information contains contractual arrangements, such as contracts of sale, contracts of carriage, letters of credit, and a multitude of

other agreements in order to satisfy international and domestic governmental and intergovernmental requirements in relation to Customs and other regulations (Melvin, 2005).

The current state of securing & managing exchange of information is costly. In addition, the state of the transactional dataset evolution and vulnerabilities has made addressing the current situation more important. Consider the long-term evolution of EDI, for example. The evolution from EDI (ANSI X12 and UN/EDIFACT) to XML based (ebXML, WS, SOAP, WSDL, etc.), as well as other formats and frameworks has caused delays and complications in the processing and exchange of electronic GSC data. Equally, Web Services, ebXML, and other transport protocols can present security exposures that are yet to be addressed (XML Europe, 2001).

To complicate matters further, today within the GSC there are a plethora of specifications, standards, control frameworks, harmonization concepts (ex: Single Window), approaches, techniques, tools, and much more. There is a global wealth of trade specs, standards, methods, tools, projects, and initiatives. For example, the United Nations alone offers 33 GSC Trade Recommendations, and

they are currently working on the 34th. The WCO offers the Framework of Standards to Secure and Facilitate Global Trade (SAFE) and the WCO Data Model. There are plenty of intergovernmental agencies, international organizations, and industry groups, **each promoting their own standards without cross-referencing them with others**. In fact, significant efforts were exerted by the US National Institute of Standards and Technology (NIST) to bring basic mapping capabilities to *some* of these standards. Such mappings are available at the NIST MOSS Project Worksite¹ (NIST, 2007). This abundance of standards and specifications is evidenced by the wealth of trade publications from the United Nations, WCO, WTO, IMO, ICC, ICC/UNCTAD, COBIT, NIST, ISO, FFIEC, DHS (C-TPAT), industry associations (AIAG, APQC), and several others. While such abundance of standards and recommendations may be helpful in some cases, they present significant challenges to the industry participants in terms of compatibility issues and implementation requirements, due to lack of enforcement and data transformation issues between participants. The impact of trade compliance on GSC IT Security merits serious considerations as well. As governments extend security mandates deeper into global supply

¹ <http://syseng.nist.gov/moss/moss-views>

chains, companies must meet multi-dimensional security needs to keep their goods in motion. This raises the issue of *Quality of Service*. Security is an aspect of quality and should be addressed throughout the system development life cycle (SDLC). In addition, there are problems associated with government security programs and compliance and targeting (WCO, 2006). Details of these concerns are discussed in Section 1.3.2.

1.1.3 *The Why*

In addition to the GSC IT security issues outlined in Section 1.1.2, another area of complexity is the lack of trade compliance, especially practiced by SMEs in third-world countries. Compliance process issues coupled with GSC IT security constraints, present unique challenges in today's GSC business environments.

These challenges include:

- 1) Lack of unified or common GSC IT Security Policy.
- 2) Lack of defined processes for maintaining and keeping IT security (privacy, availability, integrity) and other related business controls current and updated without a defined process for maintaining and keeping controls up to date. GSC industry participants will find that many of their controls will soon be “non-compliant” due to normal changes in their business and IT environments.
- 3) Continuous expansion and change in:
 - a) IT Security Technologies such as RFID which makes this very obvious.
 - b) Business boundaries, audit requirements (just consider Sarbanes-Oxley), and other factors.

- c) Local and international IT Security Policies.
- 4) New technology brings new risks, new processes and thus new compliance issues.
- 5) Lack of flexibility - GSC enterprises need flexibility to remain competitive:
 - a) Rigid control processes can hinder flexibility, thus hurt GSC IP business' ability to operate effectively.

Given these situations and challenges, this research aimed to analyze the dynamics of electronic data exchange within the automotive GSC, and propose a conceptual solution and an infrastructure framework that would contribute toward improving the IT security of data exchange and compliance for all industry participants. The conceptual solution is discussed briefly in Section 1.11 and in detail in Chapter 4 Sections 4.1 and 4.7.

1.1.4 *The Scope*

This research project addresses the issues associated with improving the GSC electronic security via IT governance (i.e., proposing the implementation of the GSC IT Security Policy within the WCO Data Model), technologies, processes, and industry best practices. In order to provide an innovative solution which strengthens the robustness of GSC electronic security and data exchange, the scope of this research project must focus on the investigation of two control areas:

1. GSC Information Technology Security: is discussed throughout this dissertation document. It consists mainly of the literature review (Chapter 2), the conceptual model (Chapter 4), the demonstration of concept (Chapter 5) and conclusions and recommendations (Chapter 6).
2. Trade Compliance: is discussed in Chapter 2.

To effectively secure the dynamics of GSC operations, industry participants must take the necessary steps recommended by this (and other) research to assess, evolve, and communicate practices that ensure tighter security of cargo and enhanced security throughout the entire supply chain (Pickett et al., 2003). As such, effective GSC improvement steps require involvement and focus, by the industry participants, within areas such as trade compliance, physical facility security, container security, physical access controls, security training, IT security, and conveyance security (Walker, 2005).

In order to apply appropriate GSC security measures, a well-designed risk analysis approach must be devised as part of the scope of this research endeavor. Such an approach must allow for flexible customization of security plans based on a variety of risk analysis business models (Brebbia et al., 2004). This risk analysis approach is discussed in details in sections 2.2.2 of Chapter 2. Regardless of the diversity of these business models, the risk analysis approach must accommodate for and incorporate areas such as:

- Business partner requirements, security procedures, and conformance to supply chain programs.
- Security criteria for selection and points of origin.
- Container security and inspection.
- Employees, visitors, deliveries, unauthorized persons, personnel security, and pre-employment verifications and checks.
- Procedural security:
 - Documentation Processing.
 - Manifesting Procedures.
 - Shipping and Receiving.
 - Cargo Discrepancies.
- Security training and threat awareness.
- Physical security (fencing, gates, parking, locking devices and key controls, lighting, alarm systems and video surveillance cameras).
- IT security such as password protection and IT security policies and procedures (Jordan & Silcock, 2005).

An integral part of the scope for this research required devising an effective approach to conducting this research work. A conceptual demonstration of the solution was developed using ProVision™ models (refer **Appendix B** for a complete listing of these models). A significant portion of this research initiative involved ongoing collaboration with AIAG and other industry professionals and experts in order to obtain analytical portrayals of these industry problems, and recommendations for enhanced communication tools to be used by all trading partners. These included OEMs, Tier-1 and sub-tier suppliers, transport providers and logistics, and related service providers. These recommendations also ensured ease of use and access availability to the SME's.

1.1.5 *The Focus*

The focus of this doctoral research is on approaches and best practices to *improve the overall security* of global and international supply chains for transactional data security, and trade compliance through IT security strategies, processes, techniques, and tools. It focuses on the automotive industry as a subset representing many issues of the GSC for investigative purposes. However, this research does not consider the auto industry to serve as a proxy for all GSC issues. The ultimate benefits of this focus would be to optimize the value of the GSC efficiency to the customer at the end of the chain. Effective implementation of IT security in the GSC is considered to be a critical element in the effort to reduce the threat of terrorism (Lensing, et al., 2003). Subsequently, if the information is timely and accurate to support the processing of physical goods, then conveyances and goods **could receive expedited processing at border crossings and ports of entry** into their targeted destinations. In order to realize such improvements, trading partners must participate in various programs offered, and in some cases mandated, by the US Customs and commercial enterprises.

Recent studies and surveys of over 200 automotive participants have shown that supply chain IT security ranks high among the major contributors of supply

chain inefficiencies (O'Brien et al., 2005). Further findings indicate that compliance-related spending was expected to reach nearly \$15.5 billion this year. The cost for a typical company is estimated at approximately \$500,000 (D'Antoni, 2005).

A 2005 AMR Research study concluded that 91% of automotive industry participants still use manual procedures to correct shipments, and to communicate status and visibility; 15% of shipments experience delays due to inaccurate or incomplete data; 79% believe standardizing “exchange of information” will reduce disruptions in supply chain; and 87% believe improvement in long distance supply chains is needed (AMR Research, 2005). This survey was done in collaboration with the AIAG MOSS project and by request. Recurring problems involving the **extensive use of paper documents, emails** and **faxes** to effect these complex material movements causes compliance problems, data quality deficiencies, and visibility deficiencies. These problems all result in avoidable delays and the expenditure of additional resources for problem resolution. Hence, they become an essential part of the focus of this research.

Researching improvements in the GSC is a never-ending endeavor which has been attempted by many researchers over the years (Connaughton, 2006). Some of the current and recent research efforts in this area include:

- Applying global security standards and frameworks to optimize the performance.
- Managing the volume and transparency of supply chain data.
- Anticipating appropriate services in the GSC which can create new business opportunities.
- Understanding which practices are more effective and in which industries.
- Protecting profits by managing uncertainty and risk.
- Benchmarking against the best performers across industries.
- Innovating and collaborating with partners and third parties.

Even a slight improvement in the defense against terrorism within the supply chain security mechanisms will not only reduce the opportunities for terrorist attacks and potential disasters but will also be manifested in significant financial savings and enhancements to the world's socio-economic developments and prosperity. Making resources available to assess, analyze, and improve the GSC security issues justifies the effort.

With such potential negative impact, the focus of this research must improve the security of the GSC data exchange and enhance the readiness across the globe. Benefits of conducting this study are discussed in Chapter 1 Section 1.7. A

focused interest by government and industry executive management promotes widening the topic's knowledge to maximize such benefits.

1.2 Focal Theory and Application

Tracking shipment of containers offers significant opportunities not only into inventory visibility but also about the carriers and drivers of such shipments and their whereabouts, the content being transported, its origin and destination, and a multitude of other relevant information (Han et al., 2005). Unlike goods management, which is exception based, the ability to know where a container is at any point in the sequence of ship events is a common requirement. This is known as "shipment visibility". When a hand-off is missed, then follow-up must occur. Radio Frequency Identification Devices (RFID) is one of several technologies that can facilitate this capability. The timely availability of information contained in RFID tags and devices could yield effective inventory management, visibility, and interoperability. Tampering with such information can significantly disrupt the entire supply chain operation (Pararas-Carayannis et al., 2002).

As outlined earlier, the automotive GSC trade and transport is very complex. Therefore, there is a constant need to obtain, analyze, and exchange data securely

and compliantly. The rapid changes in IT coupled with political and socio-economic factors are continuously transforming international trade and transport operations. In the last few years, governments and business organizations have increasingly emphasized the importance of supply chain security and import/export compliance (Neef et al., 2004). This is evidenced by the recent wide adoption of the WCO SAFE Framework, and the significant IT content of trade facilitation measures that are currently presented in the WCO SAFE Data Model (WCO, 2007) and negotiated by the World Trade Organization (WTO, 2007). Such dynamics further complicate the ability of automotive Industry participants to comply and operate efficiently and securely within the GSC.

One of the major **applications** of GSC IT Security improvements is Radio Frequency Identification Devices. RFID technology products are being used across a host of everyday applications including the insertion of RFID chips in US Passports all the way to cargo containers. The adoption of RFID applications in logistics is increasing. Logistics providers have evolved plans to analyze the long-term applicability of offering cost effective RFID services. Several logistics providers see strategic benefits in implementing RFID technologies. Section 2.3 in

Chapter 2 discusses these applications in detail. RFID technology applications are important because they offer benefits that include the following:

1. Reduce warehouse and distribution labor costs
2. Reduce point-of-sale labor costs
3. Reduce inventory
4. Improve forecasting and planning
5. Reduce theft
6. Reduce out-of stock conditions
7. Improve customer experience

1.2.1 *Components of the Global Supply Chain*

To gain understanding of the focal theory for this research, one needs to delve into the inner workings of the GSC. This could be accomplished by studying the infrastructure of the layers and components of the GSC, at least theoretically. Therefore, this section will focus on the roles these components play within the global economy.

The GSC is composed of several elements (AKA layers). When they work together according to a sound plan, these components should deliver effectiveness and efficiencies to that chain of supply. Figure 1-2 illustrates these layers in concept. The reality of how this structure is composed differs from one chain to another and from one industry to another. The flow of information starts within any layer and interoperates with any other layer or more.

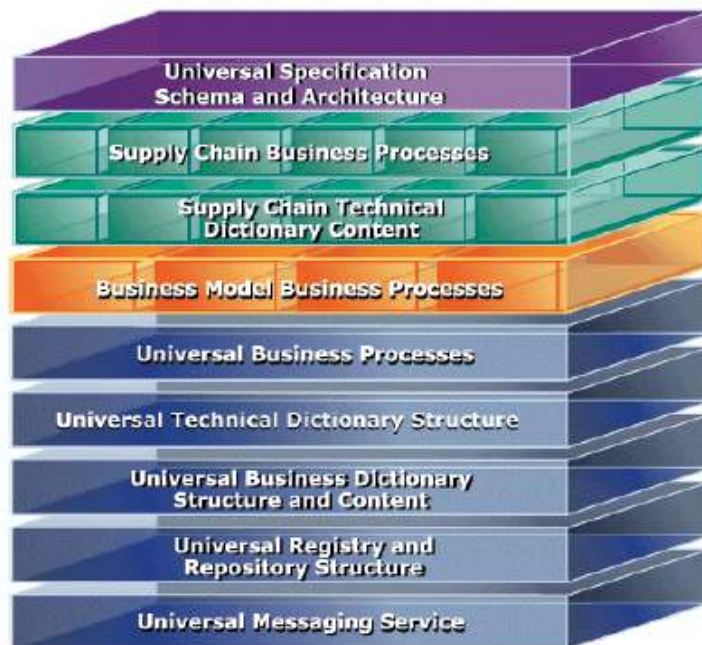


Figure 1-2: Components of SC Collaboration Interoperability Process²

At the top of this architectural model, the layer of **Universal Specification Schema and Architecture** includes the definitions for EDI, WSI, ebXML, SOAP, and other specifications and formats as outlined in the Introduction, Table 1-1, and Section 1.1.2. All **Supply Chain Business Processes** must comply with the Universal Specification Schema and Architecture. However, they don't necessarily comply to IT requirements, rather data and messaging must accurately and consistently support the business process. The **SC Technical Dictionary Content** acts as a repository (RDBMS and Object RDBMS) to house

² Adopted from: <http://xml.coverpages.org/rosettanetStandardsForIntegration.pdf>

the essential explanation (dictionary) of the content. **Business Model** and **Business Processes** define the operational flow of activities within the supply chain. Much research is being done in this area. The **Universal Business Processes** are those coming from global sources beyond the local chain of supply processes. The **Universal Technical Dictionary Structure** describes the architectural structure of the Technical Dictionary Content. The **Universal Business Dictionary, Universal Registry and Repository,** and **Universal Messaging Service** are all lower level support layers.

In summary, the idea behind this approach is to provide a *layered security architecture* which employs **several security methods** to accomplish a compromise that consumes more time and effort than it is worth to a potential attacker. It is important to implement *different layers* so that if intruders succeed at one layer, they could be stopped at the next. The redundancy of different layers assures that **there is no one single point of failure** pertaining to security.

1.3 The Research Problem

This dissertation aims to research innovative alternatives that could potentially yield a robust solution to the various IT security and compliance challenges facing the automotive industry GSC participants. Two key criteria of a

solution are strict **compliance** to US and WCO export/import laws and regulations, and the ability for offshore Small to Midsize Enterprises (SME's) to **compete** for U.S. business. At a minimum, the solution should offer innovative methods for providing Tier-1 US companies and their 3rd world SME suppliers the ability to compete and comply at a global level. To validate these criteria a conceptual solution needs to be illustrated with a demonstration of concept. For now however, one needs to define the core issues associated with the current problems that this research is intending to address.

1.3.1 *Current Problems*

In Sections 1.1.2 and 1.1.3, a variety of current problems were discussed; however, in this section the focus is more on the big picture of the GSC dynamics including characteristics of physical shipments. Additionally, the researcher presents some of the GSC IT security concerns from the WCO point of view in Section 1.3.2. The following is a common list of issues within the automotive GSC that need to be addressed with this research:

- IT Security Issues abound. These mostly revolve around current technology exploits and potential future threats.
- Trade Compliance Issues. These issues are discussed in details in Chapter 2 Section 2.1.3.

- End to end shipment visibility is limited. There are numerous proprietary systems, and many are not real time and do not cover all events end-to-end.
- Split shipments, changing modes, and other disruptions are very difficult to manage.
- Many trading partners use EDI internally and then revert to paper when conducting transportation and government business.
- Trade Barriers
 - Globalization and stricter security regimes made trans-border movements more complex
 - Integrity of end-to-end supply chains is at much greater risk

1.3.2 *WCO Security Concerns*

The WCO is considered by many to be the authority on global security. In fact, their WCO SAFE Standard with its pillars and the WCO Data Model are evidence of support for the WCO as such an authority. Subsequently, the WCO itself has documented some serious concerns about a variety of GSC security issues. The WCO stated that “Security of international trade supply chain as a basis for global trading system is vulnerable to terrorist threats” (Tweddle, 2003)ⁱⁱ. Furthermore, there is a need for global cooperative arrangements to avoid differences in national approaches, and provide coordinated approach with other international & regional organizations (UN, IMO, ICAO, and APEC). However, one of the major concerns for the WCO is to ensure avoidance of marginalizing developing countries. This concern aligns perfectly with the

objective of this research, i.e., to allow 3rd world SME supplier to compete for US business opportunities. To do so, the WCO states that we need to facilitate legitimate trade by providing new arrangements based on the revised Kyoto Convention and other WCO instruments.

1.4 Brief Overview of Literature Review

The literature review yielded several useful discoveries throughout the duration of this research. Chapter 1 reviews literature containing the background information about the current GSC data security situation. The review of literature discussed in Chapter 2 provides significant details on the focal theory and application of improvements to the GSC electronic data exchange security and trade compliance. It discusses technologies such as RFID and GPS at great lengths and details, showing how technology could be effectively applied to improve the overall efficiency of the GSC.

1.5 Purpose of the Study

The goals of this study included examining issues related to automotive GSC security technologies and practices. Areas of improvement were explored that will reduce security exploitation and address other IT security and trade

compliance related issues. Therefore, the chief objective of this research is to provide a practical and deployable solution to the GSC IT security issues outlined in Section 1.3.1 and throughout this document.

The main goal of this research was to provide an innovative approach involving the effective use of information technology to address the security improvements that need to be realized in the GSC. As such, this research has examined the current strategies, practices, procedures, some governance, and a variety of technologies, and has identified avenues for improvement.

1.5.1 *Research Objectives*

Attaining an enhanced level of security in the global supply chain will be sought by means of the following objectives:

- Improved global supply chain security in a manner that meets U.S. and World Customs Organization's requirements to secure and facilitate global trade. Please reference **Exhibit One** for a complete listing of the WCO Safe Framework requirements and standards.
- Improved supply chain trade compliance and exposure predictability.
- Enhanced real time visibility and consistency based upon real time business events while managing the volume, transparency, and accuracy of supply chain data.
- A significant reduction (potentially elimination) of the use of paper documents resulting in an enhanced level of the electronic flow of information.

- Creation of enhanced capabilities that will facilitate easy monitoring and resolution of shipping disruptions, avoidance of split shipments, creation of automatic alternate routings, dynamic changing of carriers, and decreased uncertainties.
- Increased corporate profitability, saving time and money by developing economies in the overall compression of the supply chain while managing uncertainty and risk and creating new business opportunities.
- Improved information messaging security of the Global Automotive Supply Chain.
- Improved GSC Data Transaction Security regardless of data types and messaging methods.
- Increased efficiency of GSC end-to-end Data Exchange.
- Simplified global Compliance to regulation (C-TPAT, WCO Standards for Secure Trade, etc)
- Enabled/empowered trading partners located in developing countries to compete globally and trade securely.

1.6 Justification for the Study

This research effort is one that is somewhat overdue. As discussed thus far, and given the challenging findings outlined in Section 1.3 and throughout Chapter 1, it is clear that this research is absolutely necessary and timely. Even a slight improvement in the defense against electronic terrorism within the global supply chain security mechanisms will reduce the opportunities for terrorist attacks and potential disasters. Furthermore, also it will be manifested in significant financial savings and enhancements to the world's socio-economic developments and prosperity. This alone could translate into hundreds of millions of dollars. However, there is a price associated with any achievement. While the need for a

secure GSC can be generally recognized, little is known about potential terrorist strategies and techniques (AbuKhalil, 2002). Making resources available to assess, analyze, and improve the global supply chain security and trade compliance issues **justifies the effort**. A negative impact by terrorists or criminal elements on the GSC would have significant impact on the world's economy. Thus, **there is urgency to this research** study to improve and enhance **GSC security readiness** across the globe.

To support the need of conducting this study further, a couple of excerpts from significant people in this field are cited:

“...Therefore, the sole means by which the safety of the global supply chain can be secured without imposing a crippling impact on the necessary free flow of legitimate trade is through the consistent and effective application of well reasoned risk management regimes along with the *effective use of technology and customs best practices in security and facilitation...*”

Michael Schmitz,
WCO Director of Compliance and Facilitation
New York, 23 February 2007

“...Among the main factors that further highlight the need for ICT (Information and communication technologies) at ports and border crossings are: the globalization of trade and production processes, ..., *the increasing importance of supply chain security*, as evidenced by the recent adoption of the WCO Framework of Standards to Secure and Facilitate Global Trade (SAFE

Framework), and the *significant ICT content of trade facilitation measures* that may be adopted at the conclusion of current WTO negotiations on trade facilitation. *Customs automation is a crucial component of any trade facilitation program...*"

Note by the UNCTAD Secretariat
United Nations Conference on Trade and Development
Geneva, 16–18 October 2006

1.7 Benefits of the Study

Benefits of conducting this study could significantly contribute to the following areas:

- Reducing the threats of cyber-terrorism on GSC data in transit.
- Solving end-to-end data visibility.
- Improving GSC goods security.
- Protecting electronic transactional data security.

The study results are be beneficial to GSC IT Security administrators, technical, and operational specialists when making decisions about technologies that affect the GSC electronic transport process as well as to assist in automotive industry decision making regarding where to commit resources. These results, whether inferred, calculated, observed, or directly obtained for the participants could prove to be of great benefit to a variety of partners within the industry including CIO's, IT Security administrators, technical and operational specialists, and government agents and employees at all levels throughout the globe. The direct benefactor is manufacturing operations. The rest are service support whose

purpose is to support the business. Whenever measurable benefits can be gained from addressing the research questions, a focused interest by government and industry executive management promotes widening the topic's knowledge to maximize such benefits.

1.8 Research Questions and Hypothesis

Based on the review of literature, it seems that the common perception among the majority of world governments and industry executives is one of major concern regarding the security of the global supply chain, especially when goods are in transit (WCO, 2006; European Commission, 2005; DHS, 2006; US Pentagon, 2003; FBI, 2005). Clearly, there have been copious observations and assumptions linking the impact that security technologies and processes have on the stability of world trade and the global economy, but research following a mixed methods approach may serve as evidence to the validity of such assumptions.

The question at hand deals with *the extent to which IT security improves the safety and stability of world trade and the global economy*, which can be translated directly to the bottom line objectives of world governments and businesses alike.

Two common complaints among business and government leaders revolve around the uncertainties surrounding the security of the supply chain, and the lack of concrete evidence for potential risks (Kehal et al., 2005). The assumption commonly made by those leaders is that IT can play a significant role in securing the global supply chain, but the specific implementation of the IT security role remains questionable. Such conjectures can be misleading, and they may potentially cloud these issues.

Careful consideration of the literature pertaining to the problem statement, and examining the exposures facing organizations regarding their security effectiveness represent a contradiction: what is reported (by Kehal et al) and the actual status of supply chain security measures and effects are not in harmony. In order to effectively deter potential electronic terrorist attacks on the supply chain at global and domestic levels, the researcher found it necessary to ask the following research questions of the various representatives of the industry participants:

1. *Based on your experience, what weaknesses in the global supply chain are impacting the security of your transactions?*
2. *What technologies have you deployed to secure of your GSC transactions?*
 - a. *How did these technologies help you to secure the global supply chain and enhance your operational effectiveness?*

3. *What security measures do you use to monitor the security of your transactions in the global supply chain?*
 - a. *Why did you select these measures?*
 - b. *How often do you collect these measures?*
 - c. *What do you use these measures for and how do you report them?*
 - d. *What are the effects of these measures?*
 - e. *How effective do you consider these measures? Why?*
4. *What security standards do you adopt/follow for your GSC transactions, if any? Why?*
 - a. *How might compliance to such standards improve inventory visibility and interoperability?*
 - b. *How has compliance impacted your security improvement efforts and IT budget?*
5. *What new ways or methods would you like to see implemented at a global level for the sake of improving your GSC security procedures?*
6. *How can the powers of technology be leveraged to secure the global supply chain and enhance its effectiveness?*
7. *What technologies are implemented to secure the global supply chain?*
8. *What knowledge can be discovered that may yield creative new ways of applying security procedures to the global trading process?*

This research project addressed these questions by investigating the dynamics of existing domestic and global supply chain security measures, standards, practices, and effects. There answers to these research questions are discussed in Chapter 6, Section 6.1.

The research hypothesis for this research project is:

“The security of the global supply chain may be improved if all participating trading partners adopt a systematic approach to information exchange.”

1.9 Overview of the Research Strategy

Researching improvements in the GSC is a never-ending endeavor. Over the years many researchers have tackled the various areas of inefficiencies within the GSC and attempted to find pragmatic ways in order to create improved efficiencies. However, with the recent heightened awareness of terrorism and the potential threats to the electronic security of the GSC, this research was timely justified. Therefore, creating a strategy for this research was necessary. The focus of this research is to provide a solution that addresses the security issues associated with the exchange of data in the GSC.

In order to formulate a research strategy, one needs to understand the problems and their sources, and then determine how to investigate and solve these problems. According to Sol (1988), the research problem represents an ill-structured problem. The researcher creates an image of reality and this raises questions and imposes requirements on the research approach.

The research strategy concerns the steps that are carried out to execute the inquiry into the phenomenon studied, and it consists of an outline of the sequence of data acquisition and analysis required to do the research at hand

(Vreede, 1995). In this research, the researcher followed the *inductive-hypothetic research strategy*, depicted in Figure 1-3, as it is applicable to this type of research. This strategy consists of five steps (Churchman, 1971; Sol, 1982; Vreede, 1995; Laere, 2003):

1. **Initiation:** using a number of undeveloped theories, some empirical situations are described.
2. **Abstraction:** the essential aspects are abstracted into a conceptual model.
3. **Theory formulation:** using the descriptive model, a prescriptive conceptual model is derived in the form of a theory.
4. **Implementation:** test the theory by implementing the model in one or more prescriptive empirical situations.
5. **Evaluation:** the results of the prescriptive empirical situations are evaluated.

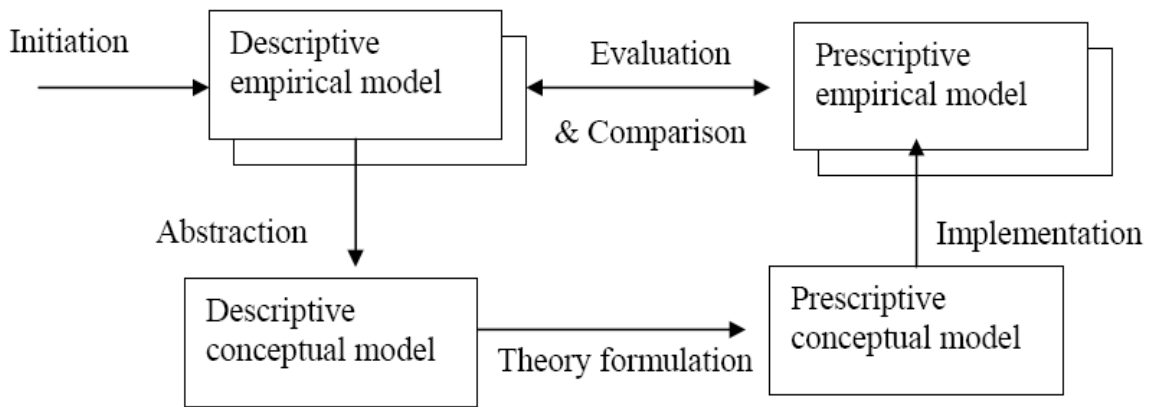


Figure 1-3: The Inductive-Hypothetic Research Strategy

The concept of “theory formulation” in the research strategy is used in a broad sense. It indicates an explicit and elaborated set of solutions for the original problem statement (Meel, 1994).

The Inductive-Hypothetic Research Strategy in the investigation of this research is organized around the execution of five steps (listed above) and four model types.

- Step 1. Construct one or more descriptive empirical models and describe a perceived situation in a specific field of interest for each. Next, we analyze these perceived situations in order to gain a better understanding of the area of the research. Elements from practice and from theory could be contained in the descriptive empirical models.
- Step 2. Create an abstraction from the empirical models. Such an abstraction could result in a single descriptive conceptual model. Such a model could provide a description of the problems found in the perceived situation at a generic level, which could lead to indications of possible solutions.
- Step 3. Combine the solutions into a grounded theory for solving the found problems. As indicated in Section 1.9, the term “theory” is used in a broad sense within the context of the inductive-hypothetic strategy. According to Vreede (1995), a theory constitutes a proposed solution for a problem situation in terms of a combination of a set of problem handling guidelines and modeling concepts, modeling support, or an inquiry system, for example.
- Step 4. Elaborate the prescriptive conceptual model into one or more prescriptive empirical models. This implies that the approach developed is applied in practice. We can then evaluate the effectiveness of the proposed theory by comparing the prescriptive empirical models and prescriptive conceptual model. As a result, we could obtain additional requirements for improving the prescriptive conceptual model. We repeat the cycle until no further requirements could be obtained.

The following benefits could be obtained by following this research strategy (Sol, 1982; Meel, 1994):

1. Emphasis on the specification and testing of premises in an inductive way.

2. Opening up possibilities for a problem specification using an interdisciplinary approach.
3. Enabling the generation of various alternatives for the solution of the problem.
4. Permitting learning by regarding the analysis and synthesis as interdependent activities.

These benefits make the inductive-hypothetic research strategy very useful for new and emerging research fields such as GSC IT Security improvement. The selection of a set of research instruments depends on the research philosophy used, current level of knowledge, nature of the research problem, availability of resources, and even the tradition of institute (Benbasat et al., 1987; Yin, 1989; Vreede, 1995). The main research instruments employed in this research are literature review, conceptual modeling of solution to research problem, testing the concept and validation of the conceptual solution, and refinement of the conceptual model.

A questionnaire was used to interview key subject matter experts within the automotive industry, and their responses were used for testing and refinement of the concept. The questionnaire was sent to the interviewees in advance in order to allow ample opportunity to understand the objectives of the research. The interviews and the questionnaire are discussed in greater details in Section 1.10

and in Chapter 3, Sections 3.1.1 and 3.1.2. Finally, complete versions of the interviews and the questionnaire can be found in Appendix “A”.

1.10 Interviews and Questionnaire

This research study sought to explain automotive GSC strategic issues related to the behavior of IT management and industry participants. The study used a mixed methods descriptive research design using a questionnaire and a set of interviews as the primary means of data collection.

The interviews covered a wide representation of Industry participants from the US government *Department of Homeland Security*, International standards and regulatory bodies such as the *United Nations*, *World Customs Organization*, the *National Institute of Standards and Technology* and *Automotive Industry Action Group*, technology providers such as *i-Connect Corp* and *Global Commerce Systems*, OEMs such as *General Motors* and *Ford*, and Tier-1 suppliers such as *American Axle and Manufacturing* and *Lear Corp*. Table 1-2 provides a list of the various industry representatives that were given the questionnaire and interviewed by the researcher for the purpose of conducting this research by answering the

research questions, addressing the research problem, and conceptualizing the solution, and refining the conceptual solution.

#	Interviewee Title ⁱⁱⁱ	Organization
1	VP IT, Procurement and CIO.	American Axle and Manufacturing. www.aam.com
2	GM Director, IT Supply Chain	General Motors. www.gm.com
3	NIST Director, Global Supply Chain	The US National Institute of Standards and Technology (NIST). http://www.nist.gov/
4	Manager Manufacturing & Process Support Systems	Federal-Mogul Corporation. http://www.federal-mogul.com/en
5	DHS Director, Global Supply Chain Facilitation and Standards.	US Department of Homeland Security (DHS). www.dhs.gov
6	IT Network Manager, Global Supply Chain. Retired	Ford Motor Company www.ford.com
7	Chief Information Officer and Deputy CIO.	The United Nations. www.un.org
8	WCO Director, WCO Data Model	World Customs Organization – WCO. http://www.wcoomd.org/
9	Lear VP of IT and AIAG Board Chairman, and Lear GSC IT Director.	Lear Corp. http://www.lear.com/
10	CEO and President, i-Connect	iConnect Inc. (Technology Provider) http://www.iconnect-corp.com
11	USGCS Customs Expert, and AIAG-GM MOSS Project Manager	Global Commerce Systems, Inc. http://www.usgcs.com/

Table 1-2: List of Research Interviewees & Organizations

In addition to the research questions listed in Section 1.8, the **questionnaire**, which is a customized representation of the Rummler-Brache Management Checklist (Perks & Beveridge, 2003) used over 50 yes/no/unsure questions covering 5 strategic IT related categories, including governance, integration, procurement, quality, and security. An additional category for “trade compliance” was later added to this questionnaire. This addition resulted from the feedback of the interviews. A response with more than 10 “yes’s” raises a red flag for action to be taken.

The results implied that compliance is almost non-existing among most developing countries SME’s and that the establishment of a Global Supply Chain IT Security Policy is necessary to improve compliance. The complete details of the Interviews and Questionnaire are described in Chapter 3, Section 3.

1.11 Principles and Objectives of the Conceptual Solution

In order to gain an appreciation of the design effort of the conceptual solution, one needs to review the drivers behind creating such design, and the leading design principles.

Therefore, to be able to demonstrate that the hypothesis of this research could be validated (or negated), a model in concept, along with a conceptual solution was necessary. The conceptual solution is explored in complete details in Chapter 4. However, at this stage of the dissertation documentation, it is appropriate to list the following principles that guided the design of the conceptual solution:

1. Application of IT security principles to GSC trading processes end-to-end.
2. Process of ensuring data transactions cannot easily be misused for malicious purposes.
3. Process of enabling industry participants to collaborate and exchange data securely.
4. Process of supporting 3rd world SME's to attain acceptable trade compliance status or certification.

The objectives of the conceptual solution were to:

1. Improve Overall GSC IT Security.
2. Simplify global Compliance (C-TPAT, WCO Standards for Secure Trade, etc).
3. Improve information messaging security of the Global Automotive Supply Chain.
4. Improve GSC Data Transaction Security regardless of data types and messaging methods.
5. Increase the efficiency of GSC end-to-end Data Exchange.
6. Enable/empower developing countries Small-to-Midsize-Enterprises and Joint Ventures to compete globally and trade securely.

Having defined, understood, verified, and presented the situations and challenges in the previous sections of Chapter 1, the researcher found it necessary to conduct the research effort. As such, a DMIT Research Proposal was

submitted and approved in June, 2006 in order to analyze the dynamics of IT Security and trade compliance within the automotive GSC (Kakish DMIT Proposal, 2006). Consequently, such analysis yielded an effort to design a conceptual solution for the purpose of addressing these issues. The objective of the conceptual solution was two-fold:

1. Contribute toward improving the IT security of GSC data exchange.
2. Improve the compliance levels of 3rd world countries SME's and their suppliers (Kakish, 2007).

The complete details of the Conceptual Solution are described in Chapter 4.

1.12 Contribution of the Dissertation

This research and documentation of its findings contribute to the GSC efficiency in general and to the security of electronic information in particular. The dissertation addresses a number of issues and complexities, but focuses on the improvement of electronic information security and trade compliance specifically. An integral part of this research involved the design and modeling of a conceptual solution. The conceptual solution promoted the idea of establishing a GSC Hosted IT Security Infrastructure Framework along with establishing a GSC IT Security Policy which aligns and interoperates with

international standards, including the UN Recommendation 33 (AKA Single Window Facilitation), the WCO Data Model and Framework (SAFE), as well as other international standards.

One of the significant contributions of this dissertation is the analysis of strategic issues related to the behavior of IT management and industry participants. The operational research for studying such behaviors involved the commonly known mixed-methods approach through the design and deployment of questionnaires and interviews with key industry leaders and representatives.

The results of this study revealed several significant findings about the state of electronic information security and compliance within the automotive industry domestically and globally. In addition, it showed a correlation between IT Security and compliance. Most importantly, the results of the study confirmed the validity of the research hypothesis and the conceptual model.

1.13 Chapter Summary

Chapter 1 provides a high level introduction to the research, and an overview of the major research activities and components. In this chapter, the researcher defined the problem at hand, and justified the need for conducting the research.

Chapter one topics include background theory and application (the current situation, what, why, purpose, scope, and focus). Next, the focal theory and application is discussed. The research problem follows. This includes current problems and WCO security concerns. A brief overview of literature review is discussed next followed by the purpose of the study, research objectives, need for the study, and hypotheses and research questions. An overview of the research strategy is discussed next. A special section was dedicated to discussing the interviews and questionnaire in the chapter. The principles and objectives of the conceptual solution are highlighted next. Finally, discussions regarding the contribution of the dissertation, and the research timeline are provided.

1.14 Outline of the Dissertation

This dissertation follows the Lawrence Technological University DMIT Dissertation Template. Table 1-3 provides an explanation for each chapter

including a link to the inductive-hypothetic research strategy elements, descriptive empirical model, descriptive conceptual model, prescriptive conceptual model and prescriptive empirical model.

Chapter	Description
1	Provides a high level introduction to the research, and an overview of the major research activities and components. In this chapter, the researcher defines the problem at hand, and justifies the need for conducting the research..
2	Describes what the researcher learned about this area of research from the review of literature. In this chapter, the researcher discusses the focus, purpose, and scope of the research. The researcher presents the literature findings that are specific to the hypothesis. This includes a discussion of current and emerging technologies, the state of information exchange within the GSC, and the importance of risk planning and effective compliance. The next section of the literature review considers legacy systems and the impact they have as they pertain to GSC IT security. Chapter 2 then delves into a deep discussion of the current and emerging GSC IT security technologies, including neutron-based detectors and PFNA™ technology. Next, this chapter addresses issues pertaining to global trade and electronic security management, and a number of change agents including globalization, infrastructure and economic interdependencies, and discontinuous events. The chapter then discusses the strategic pillars of GSC IT security, followed by suggested approaches to the GSC IT security management and the GSC IT security problem solving process. Next, the researcher discussed the GSC IT security risk management process, and risk factors. The chapter concludes with a chapter summary and conclusion.
3	Deals with research design and procedures. The chapter starts with a section describing the research approach and design. Next, the data collection methodology is discussed. The primary method for data collection in this research relied on interviews and questionnaires. The methodology for analyzing the collected data is discussed next. Section 3.3 is devoted to discussing the limitations of the research

Chapter	Description
	<p>design. This includes assumptions made with the collection of data for this research and the limitations of the analysis of such collected data. The discussion of research design limitations includes a section on transportation analysis data requirements.</p>
4	<p>Is dedicated to presenting the research discoveries and findings. In essence, this chapter portrays the heart of this research. This chapter begins with an introduction of the research findings, followed by a section on the analysis of these findings.</p> <p>The section of main significance in Chapter 4 is the conceptual solution, presented in section 4.4. Within this section, the researcher discusses the elements of the conceptual solution. These elements include the conceptual solution data transportation schemas, the conceptual solution meta model as created in the ProVision™ modeling tool, the conceptual solution security infrastructure model, and the conceptual solution technical infrastructure.</p> <p>The next logical step of the conceptual solution discussion deals with developing the initial concept for the combined Web-based GSC IT Security System on top of a Single Window™ platform. Once a discussion of the conceptual solution is finalized, the researcher turns the attention of the research to describing the interviews and questionnaires in detail.</p> <p>The final sections of chapter 4 are dedicated to discussing the findings as they pertain to the hypothesis, as well as other findings.</p>
5	<p>This chapter is about the demonstration of concept. It starts by describing the prototype, which is represented in a number of models and diagrams created in ProVision™. Next, the researcher presents a description of the proof of concept process model, followed by an evaluation of demonstration in terms of the hypothesis.</p> <p>A discussion regarding the findings relative to the hypothesis is followed. This includes findings relative to best practices, situational awareness, training and exercises, and outreach as well as additional findings.</p>

Chapter	Description
	The chapter concludes with findings relative to the four value chain V's: visibility, variability, velocity, and vulnerability; findings relative to the four solution set C's: coordination, cooperation, consultation, and collaboration, and findings relative to the four security D's: deter, detect, delay, and dispatch.
6	Provides a validation of the research questions and the research hypothesis as well as reflections on the research. The chapter begins with answers to research questions, followed by conclusions related to the hypothesis. The chapter then discusses a summary of the research contributions, limitations, and recommendations for further future research.

Table 1-3: Outline of the Dissertation

CHAPTER 2 LITERATURE REVIEW

Supply Chain Management (SCM) is defined by many experts in the field as the planning and management of all activities involved in sourcing, procurement, data conversion, and logistics management activities. In addition, it includes coordination and collaboration with channel partners (industry participants), which can be suppliers, intermediaries, third-party service providers, and customers. In essence, Supply Chain Management integrates supply and demand management within and across companies (Wikipedia, 2007). The sections of this chapter are outlined as follows:

- 2.1 General Review of the Field
- 2.2 The Importance of GSC IT Security
- 2.3 Literature Specific to the Hypothesis
- 2.4 Technologies
- 2.5 GSC Electronic Security Management
- 2.6 The Strategic Pillars of GSC IT Security
- 2.7 GSC IT Security Management
- 2.8 Chapter Summary
- 2.9 Chapter Conclusion

Creating a secure and efficient GSC - the dynamic network of interconnected organizations specifically for the purpose of conducting trade, from suppliers' suppliers to customers' customers, which work collaboratively to bring value to

the marketplace – is driven by globalization and technological innovation (Christopher, 2005). These customer-centric supply chains have accelerated the convergence of information flows, product flows, and payment flows, and are transforming the ways that companies produce goods and provide services (Chan & Lee, 2005).

To illustrate the complexities associated with global supply chains, a typical representation of today's supply network is depicted in Figure 2-1. Due to the fragmentation of the network, a company needs to deal with a variety of different entities in order to pull products together. Consequently, security exposures grow exponentially (Walker, 2005).

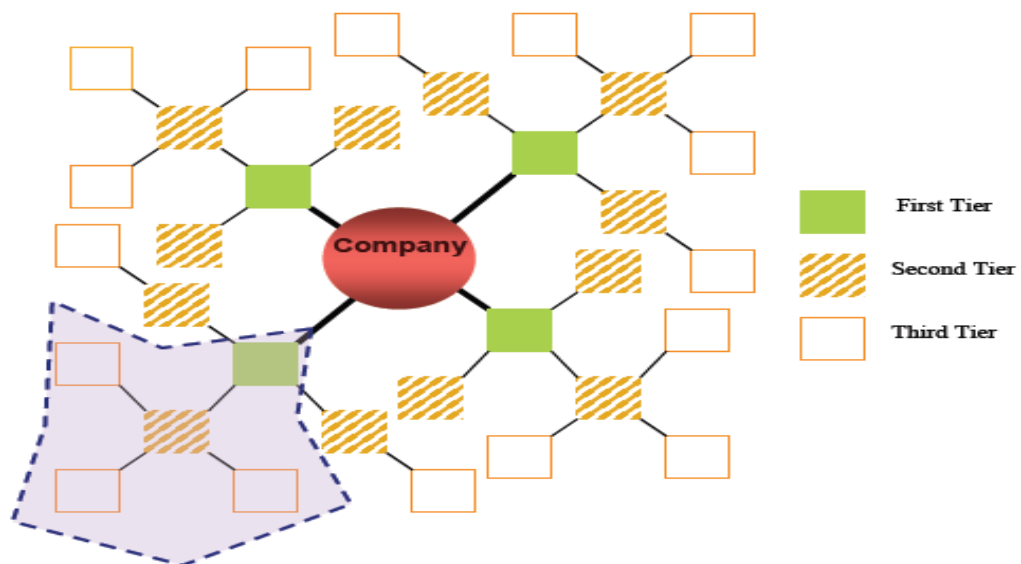


Figure 2-1: A typical representation of a supply chain network

Recent research indicates that with the increasing product proliferation, retail driven competition, and the inter-twining of several supply chains observed in many industries, the complexity and costs of coordination have become challenging. Companies must have control and influence on their supply chains to manage these costs and complexities (Lan and Unhelkar, 2006). In addition, managing internal business functions and relationships with external entities call for a different approach. Such an approach would involve a neutral third party who coordinates the network and aligns the incentives (Walker, 2005). This conceptually sound role is idealistic and maybe perceived by many to be hard to implement in reality. However, this *is* (almost exactly) what the conceptual model and conceptual solution of this research is attempting to solve.

Managing the GSC provides insight into new ways of doing business in a secure and effective manner. It moves beyond the linear thinking of incremental, short-term improvements in productivity and efficiency to address the longer-term, exponential changes that Industry participants must make in order to manage the complexity of today's fluid network of suppliers and customers (Thiele, et al., 2004). Figure 2-2 (adopted from Walker, 2005) depicts basic network architecture within any given Industry participants area of representation in the supply chain

network. In essence, the basic network depicted in Figure 2-2 could fit anywhere within any box inside the dotted area of Figure 2-1. It is worth noting that most third world SME's have a primitive version of the network depicted in. A more sophisticated figure would show the various modes of transportation, customs, freight forwarders, etc. Figure 2-2 simply shows the tier structure.

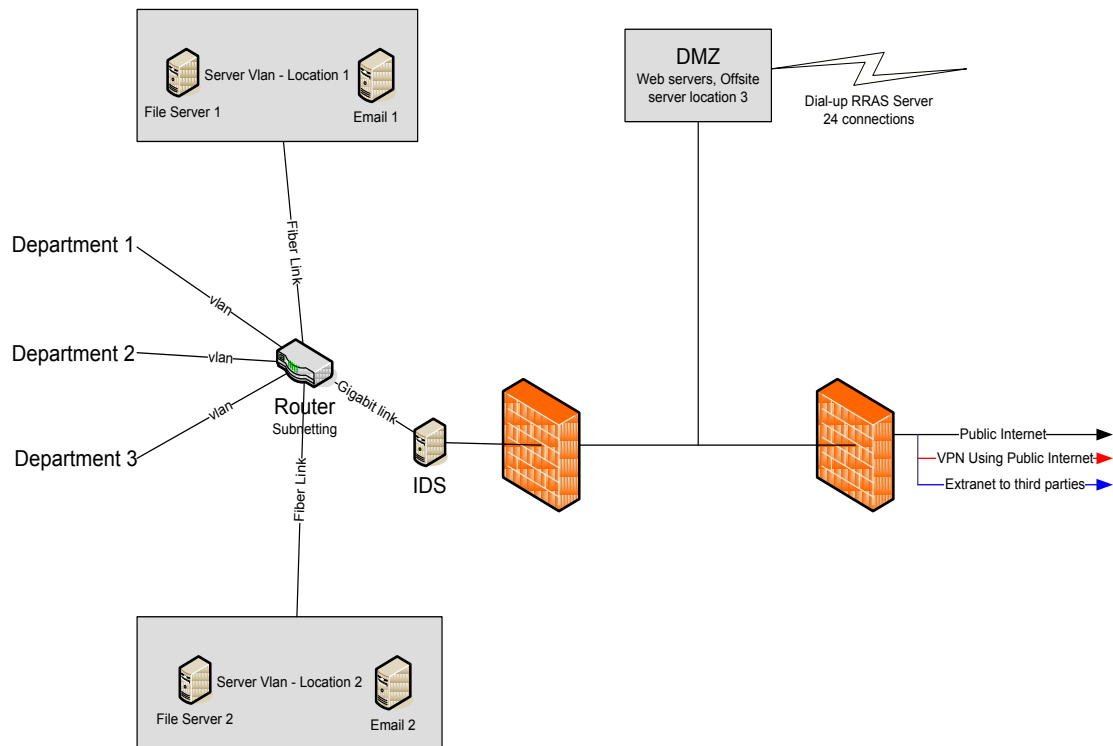


Figure 2-2: Basic Network Design

Recent research at MIT and other industry support groups discovered that a network capable of orchestrating collaborations, services, and linkages is necessary in order to optimize value to the customer (IMD International, 2007).

These researches focused on companies achieving outstanding performance using innovative supply chain strategies. Exploring the optimization of value to the customer was one of the ultimate goals of the MIT research study. This entailed discovering the knowledge of *how to create new ways of securely doing business*, improve outsourcing processes, design smarter interfaces, develop mutually beneficial long-term relationships with customers and suppliers, and manage the internal changes necessary to make it all happen (Fandel, 2004).

Additional GSC IT security improvement research in the last few years has focused on the following areas:

- Applying the concepts of global security standards and frameworks to optimize the performance of the different parts of the supply chain (Ongchin et al., 2005).
- Managing the volume and transparency of supply chain data (Dolgui & Zaikin, 2005).
- Anticipating the appropriate services in the supply chain which can create new business opportunities (Gupta & Westney, 2003).
- Understanding which practices are more effective and in which industries (Vervest, 2005; Sheffi, 2005).
- Protecting profits by managing uncertainty and risk (Fike, 2005).
- Benchmarking against the best performers across industries (Kantor, 2005).
- Innovating and collaborating with partners and third parties (Chiles & Dau, 2005).

Several U.S. and international initiatives have surfaced in recent years for the purpose of securing the GSC. One of these initiatives is known as Customs Trade

Partnership against Terrorism: C-TPAT (US CBP, 2003-2007). It is a joint initiative between the U.S. government and businesses designed to protect the security of cargo entering the United States while improving the flow of trade. Other initiatives include the following:

- The Container Security Initiative, a program led by U.S. Customs and Border Protection in the Department of Homeland Security focused on screening containers at foreign ports (AIAG, 2006).
- Efforts for countries around the world to implement and enforce the International Ship and Port Facility Security Code (ISPS Code), an agreement of 148 countries who are members of the International Maritime Organization – IMO (Wikipedia SC Security, 2007).
- Pilot initiatives by companies in the private sector to track and monitor the integrity of cargo containers moving around the world using technologies such as RFID and GPS (Wikipedia SC Security, 2007).

One of the global strategic initiatives that contribute to securing the global supply chain and improving inventory visibility and interoperability is known as Materials Offshore Sourcing – MOSS (AIAG, 2005-2007). The MOSS project is designed to provide enhanced electronic communication between trading partners including OEMs, Tier-1 and sub-tier suppliers, transport providers, logistics and related service providers throughout the intercontinental supply chain. Support for this project has been demonstrated by participation at the Automotive Industry Action Group's (AIAG) MOSS Project Town hall on June 23, 2005 where 85 representatives from 48 different companies expressed interest

in working to improve the visibility of shipments through multiple carriers in the long distance offshore supply chain. Additional information showing the need and interest for this project was gathered from 210 participants as a result of a survey designed by AIAG and AMR Research. This project includes the analysis of the existing business and technical processes utilized to move goods from the foreign supplier to the domestic customer (AIAG, 2005).

2.1 The Importance of GSC IT Security

We've established thus far that the GSC serves as the backbone for international trade, which is an essential driver for economic prosperity and socio-economic development throughout the world. We've also argued, and confirmed based on the review of literature, as well as feedback from conducting the interviews that today's global trading system is vulnerable to a variety of IT security exploitations that would severely damage the entire global economy (Dresser, 2004). Therefore, we derive the understanding that while world governments and business organizations strive to control and administer the international movement of goods, real evidence dictates that there *is* dire need to provide increased electronic security to the GSC (Kakish & Steenkamp, 2005).

Furthermore, based on the efforts of this research, coupled with the review of literature (AMR Research, 2005), we derive the theory that processing and tracking shipment containers across long distance and global supply chains suffers significant problems throughout the world. Such inefficiencies include substantial delays in moving freight, missing critical information, limited end-to-end shipment visibility, split shipments and disruption, and most importantly the wide exposure to electronic data security risk due to the lack of robust IT security mechanisms (AIAG, 2007). Clearly, these issues are manifested in significant increase in cost and deficient interoperability. The lack of interoperability between trading partners is not totally due to IT security issues. Other issues such as data semantics, different syntax and data formats, and incongruent software applications impact interoperability as well. While the causes and the sources of these problems vary widely, the apparent root cause that is commonly agreed upon is that of electronic IT security (Kakish and McCord, 2005).

Therefore, in order to gain a more profound appreciation of the magnitude of these issues, one needs to understand the underlying processes, governances, technologies, tools, approaches, and techniques associated with global supply

chain inventory and freight management. However, since the scope of this effort is focused on the elements of IT security and trade compliance, particularly as relevant to GSC data exchange and security, researching the processes of inventory and freight management is left for future efforts and will not be part of this research study.

Thus far, it was established that there exists a variety of strategies, initiatives, and Internet-based materials and inventory tracking technologies that are continually being integrated into supply chain management systems (Christopher, 2005). It has also been shown that international governments and businesses, as well as the WCO and other organizations, such as the UN, EU, and WTO have taken significant strides in recent years, in establishing and implementing global standards, global trade guidelines, and technologies in the quest of addressing various security exposures of the GSC (Simchi-Levi, et al., 2004). Additionally, the researcher relied on a number of recent studies and surveys, such as the 2005 AMR Research study to show following findings:

- 91% of automotive industry participants still use manual procedures to correct shipments, and to communicate status and visibility.
- 15% of shipments experience delays due to inaccurate or incomplete data.
- 79% of the surveyed organizations believe that standardizing “exchange of information” will reduce disruptions in supply chain.

- 87% believe improvement in long distance supply chains is needed.

Additional discoveries demonstrated that recurring problems involving the extensive use of paper documents, emails and faxes have a negative effect on these complex material movements and cause compliance problems, data quality deficiencies, and visibility deficiencies. Needless to say, these effects result in avoidable delays and additional expenditures of resources.

2.1.1 The Significance of Compliance with GSC IT Security

Today's GSC environment is highly regulated. These stringent regulations contribute toward making compliance a daunting challenge to organizations because they face a mountain of regulatory obligations. The recent increase in terrorism and related activities played a major role in evolving the laws and regulations to unprecedented levels, never seen before in history (D'Antoni, 2005). Furthermore, the expansion of these laws and regulations caused or resulted in an opportunity to comply with significant changes to IT systems and electronic data. Ultimately, the net effect of the expanded and new laws caused havoc in the industry participants' ability to keep up with trade compliance. Experts commonly agree that compliance involves policy, people, process, and technology (Melvin, 2005). Not surprisingly, these are the same elements that

make up the integrated components of conceptual solution presented in this research. However, organizations have historically tackled compliance as islands of projects scattered throughout the organization, leading to inconsistent approaches and a duplication of efforts (U.S. Office of Compliance, 2004).

An extended review of the literature has revealed that there is a unique relationship between trade compliance and IT security in today's GSC. The common trend among many IT security technology providers has recently revealed a special interest and an increased focus on the effects of trade compliance on IT security of supply chain information exchange (Neef et al., 2004). For example, VeriSign® Corp., one of the prominent global IT security technology providers recently announced the acquisition of Retail Solutions Inc, and a partnership with the WorldWide Retail Exchange™ - WWRE (Connaughton, 2006). Organizations such as Retail Solutions Inc. and the WWRE are highly interested in developing trade compliance software products. This is a sign that demonstrates significant interest within the IT security industry to extend their products and services to include trade compliance products as they penetrate their marketing efforts deep into the global supply chain. They are doing this by taking on supply chain collaboration, which recognizes trade

compliance as an essential ingredient, and establishing themselves as low-cost alternatives for point-of-sale (POS) visibility.

Several IT vendors claim to have the answers for the compliance and IT security problems that most midsize organizations in the developing world face. However, most of these vendors provide capabilities to meet only a single requirement or a handful of requirements and are not really a security and compliance management vendor themselves. Real IT security and compliance vendors are those that provide a platform for documenting and overseeing security and compliance across a developing world organization (ex: SME's), US Tier-1 organizations, and the GSC as a whole (Kagami et. al, 2004).

Further review of the literature revealed that IT security spending has steadily risen over the past few years to become a significant percentage of the corporate budgets (U.S. Government Accountability Office, 2006). Up until now, senior executives had given free reign to security managers due to compliance initiatives. Nevertheless, most organizations are over the hump of initial spending on compliance, and senior executives want to know where the money is being spent, so as to judge whether benefits are worth the expense (Sheffi, 2005).

To achieve sustainable compliance, firms must develop a process and management function. In line with government guidance, sustainable compliance must encompass and sustain best compliance practices that include the following steps (TCC, 2006):

1. Document the policy and control environment.
2. Assign appropriate oversight of compliance management.
3. Require personnel screening and access control.
4. Ensure compliance through training and communication.
5. Implement regular control monitoring and auditing.
6. Consistently enforce the control environment.
7. Prevent and respond to incidents and gaps in controls.

Organizations that do not embrace compliance management as a defined business process will approach compliance as fragmented projects, trying to sneak past the regulators' gaze (Chiles, et al., 2005). This minimalist mindset may appear to work for a short time; however, it is a recipe for disaster because no specific oversight compliance is in place. In today's dynamic business environment, gaps quickly arise that can push an organization out of compliance. IT systems, employees, relationships, and compliance requirements have changed. Therefore, the business has ultimately changed. With such increasing change, it becomes extremely difficult for anyone to manage compliance effectively. Furthermore, when regulators ask questions and there is

no central person ready to answer them, the organization looks confused and unorganized and will receive more scrutiny. To avoid this situation, we must recognize and address the challenges of compliance when coupled with IT security in the GSC.

2.1.2 Challenges of IT Security and Compliance in the GSC

Over the past five years, the GSC has seen a dramatic increase in trade information requirements. The chief causes of such an increase are the convolution of the supply chains, the number of parties involved, and the speed at which goods are exchanged.

In Chapter 1 Section 1.1.2, the current situation of the international specifications, standards, control frameworks, and trade recommendations was presented. Furthermore, it was concluded that this abundance of specifications and standards, presents significant challenges to the industry participants in terms of compatibility, implementation, and lack of enforcement. It was also inferred that a typical SME in a 3rd world country doing business with a tier-1 business in the US faces significant confusion and difficulty when it comes to preparing and presenting their data for exchange purposes. As a result, one needs to consider

how these challenges impact the management of IT security, and examine the various alternatives to address them.

The challenge for IT security managers in addressing these confusions is to not only identify what is important but also to be able to tie this information from disparate tools into business-centric metrics so that the senior executives can understand them, take action, and be confident that the enterprise is secure. We've already established that the exchange of electronic data across the GSC is fragmented and disparate. We've also shown that the full round-trip of a given data transaction in electronic format is almost non-existing. This means that the reality of the exchange of data among the various origin and destination points of the GSC is part paper-based and part electronic. Therefore, in today's world, paper documents no longer guarantee efficiency, security or accuracy, which is one of the biggest issues.

Despite the positive efforts of governments and business organizations to simplify the processes of GSC data exchange, the new stringent security measures that governments introduced after the events of 9/11 attacks in the US, complicated these processes further, and added significant requirements for

changes in IT systems and processes, especially in the area of electronic security.

These new and additional complications can be clearly seen in regulations and mandates such as the following:

- Advance Cargo Information (ACI), where complete transaction information must be provided to the various Customs Agencies up front – long before the execution of the requested transaction starts.
- Container Security Initiative (CSI), where significant amounts of transactional data is required, again prior to the delivery of goods.
- Customs-Trade Partnership against Terrorism (C-TPAT) mandates and regulations (US CBP, 2003-2007), which were discussed in details in Chapter 1.

Each one of these initiatives, and several others that were not listed here, depends heavily on reliable, structured, and sophisticated information on the trade transaction. Using automated risk assessment procedures, they profoundly analyze the electronic information provided, however incomplete or inaccurate. As such, it is becoming increasingly obvious that by adopting more electronic-based (and less paper-based) trades, organizations and governments can comply more fully with trade procedures and conduct more accurate and faster risk analysis. The trends toward electronic based trading make the GSC more efficient and secure (Kakish & Steenkamp, 2005; Jordan, et al., 2005; Lensing, et al., 2003). One might argue that the creation of additional regulations compounds the cycle of data exchange and collaboration complexity. This added sophistication slows the process of global data transaction messaging and

impacts the funds and resources that were once available for IT security purposes (Hengst and Vreede, 2004).

Clearly, there is a need to build an effective strategy to deal with compliance issues. Participants in the automotive GSC should determine the requirements of all the various regulations covering corporate governance, privacy, risk management, information integrity, and identity theft among others. However, determining specific requirements could be difficult. Most automotive organizations face multiple regulations and will have to consider multiple control frameworks (Cranor & Wildman, 2003). Moreover, many of these frameworks and standards reference each other, adopt each other, and in some cases can be outdated.

2.1.3 *Compliance Challenges*

In addition to the GSC IT security challenges discussed in Section 2.1.2, today's GSC business environments present additional challenges and constraints to the combine IT Security-Compliance processes. These challenges include, but are not limited to the following:

1. Lack of Unified/Common GSC IT Security Policy.

2. Lack of defined processes for maintaining and keeping IT security, privacy, and other related business controls current and updated.
 - 2.1. Without a defined process for maintaining and keeping controls up to date, GSC industry participants will find that many of their controls will soon be “non-compliant” due to normal changes in their business and IT environments.
3. Continuous expansion and change in:
 - 3.1. IT Security Technologies (a quick look at RFID makes this very obvious).
 - 3.2. Business boundaries, audit requirements (just consider Sarbanes-Oxley), and other factors.
 - 3.3. Local and international IT Security Policies.
4. New technology brings new risks, new processes and thus new compliance issues.
5. Lack of flexibility - GSC enterprises need flexibility to remain competitive
 - 5.1. Rigid control processes can hinder flexibility, thus hurt GSC industry participant business's ability to operate effectively.
6. SOX compliance mandates for supply chain activities
7. Other related compliance issues in EU and elsewhere in the world.

2.2 Literature Specific to the Hypothesis

GSC IT security is a complex issue that covers and touches almost every aspect of an organization. As a result, security applications, services, and support spending are the fastest growing parts of most IT budgets (Kantor, 2005). Staying ahead of the virus/worm writers and identity theft rings is extremely important to any business and companies need to adopt a comprehensive threat management approach to securing their GSC IT systems. The research hypothesis for this research project states that “The security of the global supply

chain may be improved if all participating trading partners adopt a systematic approach to information exchange and collaboration.”

Equipped with this hypothesis, the researcher set out to explore and examine the literatures in order to discover documented facts that either support and confirm this hypothesis or proves it invalid. But first, one needs to ask: What is this “systematic approach to the exchange of information”?

After careful research of the literature within the space of GSC security of data exchange among the industry participants, the researcher discovered that the most effective way to define the “systematic approach” would be the following:

1. Take the most advanced efforts for data security exchange standards and models, as described in Section 1.3 – The Research Problem.
2. Identify the issues and concerns associated with the current state of GSC data exchange, and then
3. Address these concerns by devising the conceptual solution of this dissertation.

The review of literature specific to the hypothesis yielded significant discoveries that are documented in the remainder sections of Chapter 2. These discoveries can be summarized by saying that current developments in GSC IT security involve a number of technologies, approaches, issues, and concerns which are discussed next.

2.2.1 *State Of Information Exchange*

This section provides a quick update on the state of information exchange among the trading partners of the GSC with special focus on the effects of IT security risks and compliance. The common trend among many IT security technology providers has recently revealed a special interest and an increased focus on supply chain information exchange (Neef et al., 2004).

A number of GSC information/data exchange models were devised in recent years. The common approach to these models begins with analyzing information coming from any single point of the supply chain; say a manufacturer, and sharing this information about the supply with a retailer (Apurva & Moinzadeh, 2005). The manufacturer is modeled as a production queue with finished goods warehouse, the retailer as an inventory location, and other customers as an external demand stream. In this type of model, the manufacturer allows the retailer access to inventory status at the warehouse. To take advantage of this new information, the retailer changes from a single-level base-stock policy to a two-level, state-dependent base-stock policy. This type of model provides a method for computing performance and developing a procedure for evaluating optimal policy (Ongchin, 2005). Using such model, one is able to demonstrate the

impact of the new policy on the manufacturer and other customers to some extent. Additional numerical computations coming from all parties could lead to insights about the value of information to the retailer, and to guidelines for the manufacturer on sharing information.

Other developments in information exchange within the GSC include initiatives that attempt to blend IT security software applications with those of trade compliance as the case with VeriSign® and WWRE, which is discussed in Section 2.4.

2.2.2 Importance of Risk Planning and Effective Compliance

In section 2.4, it was indicated that organizations are inundated with IT vendors that claim to have the answer for their IT security risk and trade compliance problems. However, additional research quickly revealed that the majority of these vendors are not truly risk and compliance management providers. Furthermore, we concluded that real risk and compliance vendors are those that provide a platform for documenting and overseeing risk and trade compliance not only across one organization, but perhaps an entire chain. There are, however, a number of product categories in this market such as Enterprise Risk

Management (ERM) dashboards and Governance, Risk, and Compliance (GRC) platforms. Such applications specifically target financial risk management; as well as specific areas of operational risk and control oversight.

As demonstrated in Sections 2.1 and 2.2, for most organizations compliance is a daunting challenge, especially in the highly regulated environments such as the automotive GSC, because these organizations are faced with mountains of regulatory obligations. Organizations face a variety of risks: strategic, financial, litigation/legal, product/services, operational, environmental, health and safety, geopolitical, suppliers, business partners, technology, workforce, project, compliance, and reputation. The list of risks appears endless. The challenge is that many of these organizations do not have a holistic view of risk (Lan and Unhelkar, 2006). It is easy to become isolated in one corner of risk and fail to understand the interconnected network of risks that an organization faces.

To achieve sustainable compliance, firms should consider developing processes that are in line with government guidance (US Office of Compliance, 2006), and encompass and sustain best compliance practices. Figure 2-3 depicts the landscape for Risk and Compliance (Adopted from Forrester Research, 2007).

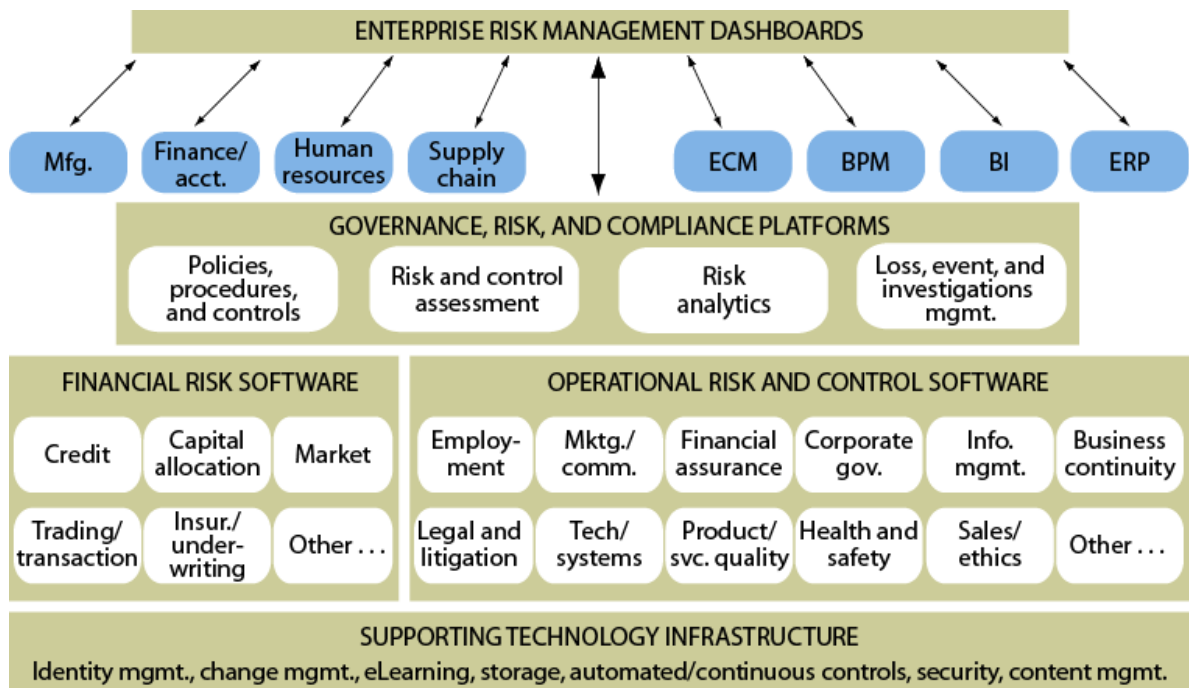


Figure 2-3: Risk and Compliance Landscape

The following seven steps represent a collection of compliance and risk best practices:

1. Document the policy and control environment. To demonstrate compliance, firms must start with how they document compliance and control architecture and explain this throughout the organization. Policies must establish corporate governance, including the governance of compliance obligations. Controls are the essential outcome of policies, procedures, and standards. Ultimately, controls are defined from policy statements and include the fine detail of the expectations and requirements established to meet compliance objectives.
2. Assign appropriate oversight of compliance management. A project approach for compliance could lead to disastrous situation. Continuous business environment changes would mean that a new project would have to be launched. Compliance oversight must achieve the mission and charter of the compliance program. Establishing the proper authority and governance of compliance is a critical requirement, followed by

establishing the appropriate lines of communication to the extended business operational areas.

3. Require personnel screening and access control. The next step in achieving effective compliance is the assurance that the organization is not giving access to information and business processes to an individual likely to exhibit unethical behavior. Organizations must ensure through reasonable controls that they are not giving improper access to sensitive organization roles and information. This is accomplished through initial background checks and screening and ongoing regular reviews.
4. Ensure compliance through training and communication. Effective compliance requires the establishment of effective compliance awareness through active training and communication to internal employees, contractors, and business partners. To effectively manage compliance, organizations need to validate that those in authority and with access to sensitive processes and information understand their compliance role and responsibility.
5. Implement regular control monitoring and auditing. This step focuses on the working operation of those controls documented in the first step. The implementation of effective controls is essential to the success of a compliance program. The proper controls to monitor and audit vary in type. These controls include policy, operational, and technical controls, detective and preventive controls, and compensating controls.
6. Consistently enforce the control environment. Consistent enforcement of the control environment ensures that controls are applied appropriately across the organization and its business processes and relationships, guaranteeing that a specific individual's or business group's violations of controls or conduct are not ignored or overlooked but are enforced according to policy.
7. Prevent and respond to incidents and gaps in controls. An effective compliance program prevents and responds to compliance violations and gaps in controls and includes a lessons-learned process to prevent further violations.

Organizations that exhibit all of these best practices make effective compliance a cost of being in business, not a one-time business event. For these firms,

spending money on a compliance program averts far greater expense as a result of losses and penalties. They also establish greater operational control oversight, enabling them to invest more funding into expanding the business into new areas with confidence. These well-run proactive companies will contrast sharply with those that remain imprudent and tackle compliance problems as isolated and reactionary initiatives. The end game is a culture of compliance and controls. An organizational culture that encourages a commitment to compliance with the law is one in which compliance with the law is expected behavior.

On the other hand, organizations that do not embrace compliance management as a defined business process will approach compliance as fragmented projects, trying to sneak past the regulators' gaze (Kagami, Tsuji et al. 2004). This minimalist mindset may appear to work for a short time; however, it is a recipe for disaster because no specific oversight compliance is in place.

2.3 Technologies

Of the myriad of technologies being experimented with and applied to the protection of cargo and the security of electronic information in transit, e.g. Neuron Based Detectors, PFNA, and others discussed in Section 2.3.3, RFID in

combination with Global Positions Systems (GPS) seem to be gaining the most attention. Significant advancements with RFID technology products are emerging and are being used across a host of everyday applications. The scope of RFID technology covers a wide gamut of applications. These include the insertion of RFID chips in US Passports and inspecting cargo containers (InfoWorld, 2006). It is interesting to note that the providers of these technologies are global, and not necessarily US based companies. For example, the vendor that is installing RFID chips in US passports is a German company (Infineon). Countries such as Germany, Norway, and Sweden are also using Infineon's RFID chips for their electronic passport systems. This goes to show that global IT security solutions are obscuring the physical boundaries among countries across the globe.

2.3.1 RFID Potential for Operations

Indicative of the increasing penetration of RFID adoption in logistics, a large number of providers presented strategic plans to leverage RFID in their supply chains. Logistics providers have evolved these plans to analyze the long-term applicability of this technology while still offering cost effective services to shippers that are looking to comply with retailers' mandates (InfoWorld

Magazine, 2006). In other words, not all logistics providers and retailers are on the same page regarding the applicability of RFID technology in today's GSC environments. For instance, FedEx® indicated that there is very limited potential in implementing RFID technologies in its already optimized, highly automated package-sorting centers. But other logistics providers see strategic benefits in implementing RFID technologies.

A number of studies have shown that RFID technologies could eliminate plant interruptions at just-in-time clients (O'Brien et al., 2005). Logistics providers struggle to meet service-level commitments in industries like electronics and automotive, in which just-in-time replenishment and lean manufacturing frameworks are practiced. It is not uncommon for a logistics provider like TNT Logistics to commit to parts delivery within an hour of a customer placing an order (TNT Logistics, 2007). But, with limited visibility of the location and availability of the parts ordered, logistics providers resort to expedited shipping to meet service-level agreements. This avoids production interruptions or worse, plant shutdown (Ayers, 2002). Using RFID to determine the location of the part and the progress of fulfilling a customer order, logistics providers can determine

the time of delivery for this part, and determine if expedited service is necessary.

However, the most important function is the track and trace capability.

RFID technologies also offer less costly transportation services, with guaranteed visibility, by locating missing goods in transit and tracking their movement.

Logistics providers are challenged by the inability to offer any visibility of the product flow, as soon as it departs their distribution centers (Geunes, 2002). This is a major problem for logistics providers looking to serve verticals with high product value or strict regulatory requirements. Shippers in these verticals avoid what a logistics provider referred to as the "black hole" of transportation, by opting for the more expensive, more secure air freight services. With RFID, a logistics provider like Horizon Lines can target importers in these verticals, as long as the logistics provider guarantees uninterrupted visibility, from the time the product leaves the distribution center to the time it arrives at its destination.

The optimization of internal operations with accurate asset management is enhanced by RFID technologies (Christopher, 2005). Logistics providers are continuously challenged by the lack of visibility of assets like trailers and pallets in their yards and distribution centers (AIAG, 2007). Using RFID to gauge the

location and the status of these assets, logistics providers can significantly reduce asset use (Taniguchi and Thompson, 2004). For example, Menlo Worldwide can use RFID-based technologies to assess whether a trailer is present in the yard, and if it is empty or already loaded. Additionally, using RFID-based triangulation techniques, the provider is kept up to date on the location of assets and space availability in its yard, minimizing the efforts of drivers and yard operators to place and locate trailers.

One of the common areas of inserting RFID tags in the shipping process is shipping containers. Because of the benefits of RFID and GPS, these containers are called “Smart Containers”. Figure 2-4 depicts an image of a smart container with specific characteristics such as:

Have Electronic Seal, Container Security Devices, RFID, or GPS Tags to Electronically Monitor and Provide Information.

Reduce Processing Time and Documentation Error Rates, Speeding Up Inspections and Intermodal Transfers of Containers

Carry Manifest Information to Provide Accurate and Real Time Data About Container ID, Contents, and Chain of Custody



Figure 2-4: Smart Containers

- Electronic seals or container security devices, RFID, or GPS tags for electronically monitoring and providing information such as time, date, and location of an intrusion into a container.
- Manifest information for providing accurate and real time data about the container ID, contents, and chain of custody.
- A reduction of the processing time and documentation error rates, expediting the inspection process and intermodal transport of containers.

The use of “smart containers” has been tested in real world situations. A combination of mobile and fixed reader technologies can query sensor data throughout a container’s end-to end movement. RFID tagging and electronic seals have the additional benefits of allowing officials to monitor the containers movement around the world and provide data used to make informed decisions about which containers might require inspection before entering any given facility (Ritter et al., 2007).

Although RFID offers several benefits, logistics providers are still concerned about issues regarding security and data encryption, "kill-switch" functionality³, and high tag costs. Additionally, the challenges of the industry specific business have shifted their attention away from RFID. Other challenges facing Industry

³ A kill switch (also called an e-stop) is a security measure used to shut off a device in an emergency situation in which it cannot be shut down in the usual manner. Unlike a normal shut down, which shuts down all systems naturally and turns the machine off without damaging it, a kill switch is designed to completely abort the operation at all costs.

participants who contemplate the application and ramifications of RFID include the role of legacy systems.

2.3.2 Legacy Systems and RFID

Logistics providers are apprehensive about the ramification of new RFID-generated streams of data because there are hundreds of millions of dollars invested in building legacy systems for warehouse management with track and trace functionality. Amassing these legacy systems, via acquisitions and internal growth, most logistics providers, like UPS for example, now have an optimized network that allows them to offer customers a high level of visibility. These legacy systems will now have to handle not just a growing volume of data, but also new data hierarchies, associations, and business logic that can capitalize on RFID investments.

For example, having RFID-based item-level visibility of highly valued products like a plasma widescreen TV, will require the logistics provider's legacy track-and-trace system to offer the association logic needed to map the item to a pallet, a shipping container, a ship or a tractor, and a driver. Can the system make this data available to a growing number of trading partners, while maintaining the

appropriate authorization and security needs? The answer to this question could have a significant impact on the use of RFID with legacy systems.

Logistics providers are questioning whether it's feasible to extend this functionality by enhancing the legacy system, or if it is cheaper and more effective to start investigating more advanced technologies. Such advanced technologies can provide the logistics shippers with the flexibility to cope with the constantly changing business logic needed to enable end-to-end supply chain visibility (Pickett et al., 2003).

2.3.3 Current and Emerging GSC IT Security Technologies

In the six years since the Sept. 11 attacks, governments around the world have been implementing a variety of anti-terror technologies. Some appear to be particularly useful and deserve to spread. Others raise privacy concerns and may not be all that effective. As we already established, some of the more effective technologies that are applicable to GSC IT security include RFID and GPS. Of course, not everyone agrees with the effectiveness of these technologies, as is the case with FedEx® which we discussed earlier. However, due to the wide acceptance of RFID applications within the GSC, especially by giant retailers like

Wal-Mart, we will continue with the assumption that these technologies are generally applicable.

In addition to RFID chips being inserted in U.S. passports, puffers, chemical scanners, and biometrics devices are increasingly appearing in airports. Despite these advancing new developments, several governmental entities are still struggling with computer systems that are significantly out of date. The Department of Homeland Security (DHS) is having problems with inspections of shipping containers (McCullagh, 2006). Ultimately, it is still not completely proven that RFID technologies are robust enough to secure the GSC despite their many applications. Therefore, further research is needed to support the impact of RFID on this research. Other leading edge GSC IT security technologies include cargo inspection technologies such as Neutron-based Detectors and PFNA™ Technology.

2.3.3.1 Neutron-based Detectors

The Rapiscan™ Pulsed Fast Neutron Analysis (PFNA™) Truck and Container Inspection System (TCIS) is based on PFNA™ technology that quickly,

automatically and non-intrusively inspects fully loaded cargo containers and trucks. Unlike X-ray radiography systems, PFNA™ does not rely on a human screener to detect objects by their distinguishable shapes. The Rapiscan PFNA™ TCIS identifies and locates the presence of concealed contraband, terrorist threats or illegitimate cargo in containers by their unique material specific signatures. Besides its primary role of security inspection, it can enhance shipping revenue by identifying mislabeled and dangerous shipments of hazardous material (Rapiscan Systems, 2006). The Rapiscan PFNA™ TCIS has configurations for inspection of land and sea cargo containers, trucks and cars. All inspection processes are automatic. The objects to be inspected are conveyed through a shielded inspection tunnel where they are scanned. The location and relative size of detected contraband or threats are displayed on an operator screen, and are useful for subsequent manual searches. New threats or material signatures can be added to update PFNA's database whenever required. The Rapiscan PFNA™ TCIS is the most advanced truck and cargo inspection system available as of the writing date of this dissertation.

2.3.3.2 PFNA™ Technology

The Rapiscan PFNA™ TCIS was developed as an innovative application of Pulsed Fast Neutron Analysis (PFNA) technology. The presence of specific materials are detected and measured through their constituent elements, by exposing them to short bursts of fast subatomic particles called neutrons. Interactions between a fast neutron and the elemental contents of cargo produce signals, called gamma rays, specific to that element. Sensors around the inspected object detect these signals. The energy and number of signals give the elemental signature and quantity. The time of arrival pinpoints the location of the elements in the cargo.

The PFNA™ signal processing reconstructs the material signatures into 3-D volume elements called “voxels”. Many elements can be directly detected, including carbon, nitrogen, oxygen, silicon, chlorine, aluminum and iron. The elemental signals are processed by the Rapiscan PFNA TCIS and combined into unique, material specific signatures in each voxel. These signatures are compared to a database of contraband, terrorist threats, hazardous materials or dutiable

goods signatures. If there is a match, the system automatically alerts the operator. The cost impacts of this technology require further research.

2.3.4 *Recommended GSC IT Security Technologies*

Researching the literature has revealed a number of effective GSC IT security technologies. Consequently, coming up with a list of recommended technologies for this research is not a straight forward task. Therefore, in order to reach and provide such recommendation, the researcher took into consideration a number of factors. These factors included the objectives of this research, the documented research problem, the automotive GSC objectives and needs, the WCO objectives, and the overall U.S. documented needs and objectives for GSC IT security scenarios. As a result, the five technologies in this section are suggested as a high-level recommendation. The researcher recommends that these technologies be adopted speedily to help in automotive industry as well as US homeland security efforts. These five technologies are listed as follows:

1. **Cargo and Vehicle Inspection Technologies.** Is it reasonable to think that terrorists could smuggle a nuclear, biological, or radiological explosive device into the U.S. by hiding it in a cargo container? Clearly, there are plenty of adequate reasons to think so. Last year, eleven million cargo containers arrived at U.S. seaports, and only a small percentage were physically inspected by Homeland Security agents (US Government Accountability Office, 2006). The U.S. Customs and Border Protection, part of DHS,

introduced on August 19, 2006 the *Sea Cargo Targeting Initiative*, an automated system that better identifies high-risk sea-going shipments into U.S. ports of entry and establishes new policies for dealing with these shipments. This is a computerized modeling system that's supposed to help identify which cargo containers should be inspected based on intelligence from sources including the CIA. It's called the Automated Targeting System- ATS (US Customs and Boarder Protection, 2002). Customs Commissioner Robert Bonner said:

"The aim of this new initiative is to improve the way we address high-risk cargo. The challenge we face is constantly changing and our policies will evolve accordingly. This initiative will better protect Americans and seaports, and it will introduce greater uniformity, predictability and efficiency to global commerce."

This initiative contains three major components:

- Adding new criteria to U.S. Customs automated systems that *reflect the latest information* about possible terrorist activities.
- Ensuring that all manifests are processed through the ATS and reviewed by trained personnel.
- Standardizing U.S. Customs procedure and practice when the system pinpoints a high-risk shipment.

The ATS has been deemed a failure by government auditors in a report this year (McCullagh, 2006). They concluded that the DHS "has not yet put key controls in place to provide reasonable assurance that ATS is effective at targeting oceangoing cargo containers with the highest risk of containing smuggled weapons of mass destruction."

Fixing the ATS would be a good first step. Equally important would be to make greater use of *noninvasive methods of scanning containers* and preventing unions from derailing security methods. The West Coast longshoremen's union prohibits its members from driving through gamma ray scanners, even though DHS officers do it routinely and the Nuclear Regulatory Commission (NRC) has approved the low exposure level. Union leaders won't allow members to drive through even more promising systems using *neutron-based detectors* either (Rapiscan Systems, 2006). Figure 2-5 illustrates these Cargo Inspection Technologies pictorially.



Figure 2-5: Cargo Inspection Technologies

Rapiscan™ Systems offers all three core inspection technologies: X-ray, Gamma-ray and Neutron analysis; placed in mobile, portal, gantry and facility configurations. The high energy X-ray systems with their linear accelerator sources penetrate the densest cargo and produce quality images for successful contraband detection. The Gamma-ray systems have an intrinsically lower radiation field, when compared to equivalent X-ray systems, which provides a smaller operational area and exclusion safety zone. This also results in less maintenance and lower cost of ownership. The Neutron analysis technology provides material-specific inspection capabilities and can be combined with our other technologies for unique, versatile inspection solutions. Figure 2-5 shows the various Cargo inspection technologies and techniques:

2. **Wireless Technologies.** The wide availability of wireless technology in recent years has had a significant impact on GSC security measures. Ever since cameras on cell phones became popular a few years ago, millions of

Americans have taken rough snapshots back and forth wirelessly. An FBI pilot program launched during August, 2006 in Washington, D.C., and New York City was designed to outfit field agents with wireless technology. They were able to take digital photos of a suspect, upload the images to a broadband wireless-enabled laptop, and e-mail it off to other on-the-go agents. They, in turn, could view the suspect's image (complete with that day's attire and haircut length) on a BlackBerry™ handheld device. Although this idea is not original, it is still a useful upgrade to the FBI's existing and legacy technologies.

3. **Better Search Engine Technology.** The private sector has had advancement over the FBI not just in wireless technology, but also in search engines. Internet search engines have been around since the early 1990s. They advanced significantly in the last 5 years. The FBI finally obtained a rudimentary Web-based search tool in 2004 in the form of its Investigative Data Warehouse (IDW). It simply enables its users to use a single Web-based front end to scrutinize about 650 million records, ranging from intelligence wires to terrorist watch lists to no-fly lists, across multiple government agencies, including the State Department and the DHS. Agents stated that it acts as a "one-stop shop" for a wide range of information that takes an average of three to five seconds to return results (CBS News, 2006).

Unfortunately, the IDW's records aren't updated in real time. Instead, the system relies on copies of documents that must be "affirmatively uploaded into the warehouse" by participating agencies, according to a 2005 auditor's report (FBI, 2005). Depending on who's in control of the data, which can happen anywhere from daily to weekly to monthly to quarterly, although in an emergency situation, updates can be speeded up to hourly intervals. The IDW doesn't yet have the capability to search directly into databases of different agencies. Therefore, a real-time US government portal would be ideal.

4. **Smarter Translation Software.** It is a well-known fact that intelligence agencies around the world continue to face a shortage of speakers of Arabic and other languages often associated with terrorist groups. Furthermore,

human-assisted (non-machine) translation has proven to be extremely time-consuming. To solve this problem, a new translation approach known as the “statistical approach” was developed in recent years. Although discussing this approach is outside the scope of this research, suffice it to say that this approach to automatic language translation and natural language processing, is highly controversial among linguists and translation experts. However, it is considered by many, especially in the US government, to be the best option available for now. Therefore, a company known Language Weaver, Inc. was incorporated in January 2002 to commercialize the translation statistical approach. As such, it developed machine translation tools that can dynamically translate Arabic, Russian, Chinese and 10 other languages into English. In its sales presentations, the company has its software produce an English transcript of an Al-Jazeera broadcast while the broadcast is airing. But more obscure languages like Pashtu and Somali are still unavailable for automated translations, which is why the federal government is working on its own internal projects. One of those projects is the Defense Department’s Language and Speech Exploitation Resources program, or LASER. It’s designed to provide intelligence analysts and the military with speech transcription and translation capabilities. Other similar government-funded efforts include Babylon™, a portable device, and the Effective, Affordable, Reusable Speech-to-Text project (U.S. Pentagon, 2003).

5. **Faster Chemical Detection.** The possibility of chemical attacks by terrorists has federal officials running nervous, and justifiably so. The Aum Shinrikyo attack on the Tokyo subway system in 1995 using sarin gas, which killed 12 people and injured more than 5,000 people, showed that it's possible. The attack would have been deadlier if the group had been more skilled. In open-air environments like city streets, the threat of a chemical attack is not as severe. Winds are unpredictable and, coupled with rising air currents, can quickly disperse a chemical agent unless a larger quantity is used. But in subways, train stations and airports, the threat of a chemical attack is higher. In an article published in Time magazine in June, 2006, author Ron Suskind reported that a terrorist cell had planned a hydrogen cyanide attack on New York City subways but inexplicably called it off with just a few weeks to go (Time Magazine, 2006). Hazard materials teams at local police departments historically have used colorimetric tubes (DHS, 2006), which are designed to detect specific gases such as ammonia or chlorine. A pump is used to draw

air samples through the tubes (ECO Environmental, 2005). The problem is that many chemicals can be used as weapons, and standard-issue colorimetric tubes will detect relatively few. A panel organized under the National Research Council (NRC) concluded that many modern detection devices used by hazmat teams have not been thoroughly tested for their utility and reliability to detect chemical weapons (Science Magazine, 1994).

Detection technology, however, is advancing. The SafeSite™ Detector (Life Safety Systems, 2006), depicted in Figure 2-6, for instance, can electronically determine the difference between nerve agents, blister agents, and toxic gases such as chlorine, hydrogen cyanide, and hydrogen chloride. An article in the journal *Analytical Chemistry* last year described how to use photoionization mass spectrometry to detect chemical warfare agents (ACS Publications, 2006). The detection took about 45 seconds, which is much faster than the traditional way of performing mass spectrometry that can take an hour or more.



Figure 2-6: SAFESITE™ Multi-Threat Detection System

2.4 GSC Electronic Security Management

The totality of activities that add value to the business, including primary partners in the supply chain and entities that affect sales, marketing, infrastructure management and other support functions are known as the Value Chain. It has become common place to observe that as the world is changing the technology has altered the dynamics of the GSC. We are in the midst of a revolutionary redefinition of how each part of the global economy impacts and interacts with all other parts. One of the most significant results has to do with the realization that the complex and ever expanding international value chains have created a certain inherent fragility. Currently, business practices that are put in place that help reduce the risk of this fragility are typically neither recognized nor measured by the analysts who specialize in evaluating a firms relative value.

Having this understanding, this research aims to seek ways that could explain these measures in a practical manner. Hence, the researcher opted to describe a high-level approach to addressing these fragilities within the GSC. Such an approach is simply called The Security Management Approach.

This security management approach is about more than just electronic security – It is a unifying theory about the resiliency and survivability of the enterprise. As such, it redefines security as a key aspect of the firm’s lasting value proposition, taking security goals from the periphery of the firm’s processes to the very core of the imperative to remain competitive in the face of change.

According to Deloitte Research, “It typically takes twenty five different parties and thirty different documents to get goods from one end of the supply chain to another. With all these handoffs, the opportunities for tampering are plentiful”. As a result the potential benefits of implementing effective IT security practices have never been greater, but only because the threat of cascading costs due to a systematic interruption have never been greater. Such interruptions include earth quakes, hurricanes, labor strikes, civil wars, and terrorist attacks.

Governments around the world have proven time and time again that they can not protect against nor rapidly recover from distributive events everywhere and at all times. This means that the private sector must take more responsibility for preparing itself for the aftermath of future disruptive events (Ritter et al., 2007).

In a study conducted by Stanford University GSC Management Forum, titled: “Innovators in Supply Chain Security: Better Security Drives Business Value”, companies were able to quantify business benefits associated with security initiatives (Stanford University Global Supply Chain Management Forum 2006), on average, these companies:

- Reduce custom inspections by 48%.
- Saw 29% reduction in transit times.
- Improved asset visibility by 50%.
- Improved on-time shipping to customers by 30%.
- Reduced time taken to identify problems by 21%.
- Reduced theft and inventory management by 38%.
- Reduced excess inventory by 14%.
- Reduced customer attrition by 26%

The first step that the global business community can take to manage the newly recognized and emerging risks is to examine its root causes. The ongoing processes that are leading to the redefinition of business processes and the realignment of global economic power have created both the need for and insured the value of the security management approach. The three distinct and related change agents that embody the most significant aspects of the processes are 1) Globalization, 2) Infrastructure and Economic Interdependencies, 3) Discontinuous Events.

2.4.1 *Globalization as a Change Agent*

The very definition of globalization and the extent of its influence continue to change almost as fast as one can place a label on it. Now one denies that globalization is occurring. It appears that globalization is real and is here to stay, regardless of who defines it. Though wide spread availability and use of laptop computers, email, and wireless internet connection were barely imaginable just twenty five years ago, today such tools are essential to the conduct of business. Indeed, in today's global economy cellular phones and pocket PC's can be designed in Japan, to use parts manufactured in China, South Korea, and a dozen other countries, which are then shipped half way across the world, assembled in Mexico and sold in the United States (Ritter et al., 2007).

The telecommunications revolution has connected the world with high speed phone lines and digital connections that enable data process from any where in the world at minimal costs. The global telecomm infrastructure and the internet that it sustains have connected factory workers in China with end users in Europe, and increasingly the lower wage but highly skilled work force of developing nations like India with global firms that are outsourcing. According to a study by McKinsey and Company on the future of business process

outsourcing, the current world wide offshore market for such services exceed eleven billion dollars per year, but the potential market is between one hundred twenty to one hundred fifty billion dollars per year (Gibson, 2006).

2.4.2 Interdependencies as Change Agents

Infrastructure & Economic are interdependencies that play the role of change agents in today's GSC environments. The term critical infrastructure refers to the interrelated economic sectors that are essential to the "minimum operations of the economy and the government" (Clinton, 1998).

A less obvious but equally significant factor plays a major role in the functioning of our modern world. That factor is a direct product of the system itself, whereby a seemingly endless quest for maximum efficiency has created such lean systems that very little excess capacity remains. It is true that such efficiency confers important economic advantages in periods of normalcy by reducing waste and driving up profits. However, whenever there is a shock to the system, the lack of excess capacity and spare parts, cargo transportation, and even finished goods leave the modern, streamlined firm without the ability to conduct business. This shock can come in the form of any disruptive event, be it

severe weather, civil war, terrorism or even just a labor dispute at any critical signal node. And this shock, like waves crashing forth from a sudden tsunami, will spread inexorably across the global economic system in unforeseeable ways. As a result, we find ourselves collectively at much greater risks from what would once have been relatively minor disruptions with minimum impact on the overall system.

2.4.3 Discontinuous Events as Change Agents

The third change agent of discontinuous events refers to those disruptive occurrences that alter normal patterns and cause changes in the availability of services and the free flow of goods. In addition to the obvious category of severe weather and extreme political upheaval, severe discontinuity can be brought about by terrorists and other criminal elements. These activities are tied to globalization, because as an outgrowth of the market, forces that are driving the world to greater integration, certain significant segments of the world's population have voiced violent opposition. This opposition is embodied most notably in both the terrorists' threats of those seeking to role back modernity and the less severe but still important anti-globalization movement that continue to oppose these trends of globalization often through violence. This "rejectionism"

is a significant factor in the increased risk facing all manors of players in the international market place. Thus, it deserves to be examined along with traditional causes of discontinuity such as severe weather and civil war.

2.4.4 *Principals of Security Management*

Security Management is the business practice of developing and implementing comprehensive risk management and security practices for a firms' entire value chain. This includes an evaluation of the preparedness of suppliers, distribution channels, internal policies and procedures for discontinuous events such as terrorism, political upheaval, natural disasters, and significant accidents. Table 2-1 demonstrates these principles.

Process Improvements Present an Opportunity for New Success	Proper Security is a Benefit to Medium and Long Term Resiliency , Not a Drag on Efficiency
Knowledge of Risks Leads to Better Investments and Overall Cost Savings	Supply Chain Visibility is Crucial for Continuity of Operations.

Table 2-1: The Core Principles of Security Management

2.5 The Strategic Pillars of GSC IT Security

The five pillars of security management (Ritter et al., 2007) are composed of the following:

1. Security practices must be based on creating value that can be measured. It is a process of requiring self evaluation, careful planning and integration and thoughtful implementation as opposed to a standard solution set that can simply be added to the existing corporate mix.
2. Security involves everyone throughout the GSC. It requires a holistic approach because the integrated nature of today's GSC solutions means that a failure of the processes that enable a firm to conduct business could put the firm at risk of significant compromise.
3. Security implies continual improvement. As with many best practices in a dynamic business environment, security management is a process that builds upon previous changes and makes incremental improvements all along the way.
4. Security help firms avoid, minimize, or survive disruptive events. Value can be created and certain forms of risk can be mitigated merely by thoughtful reflection and a willingness to challenge status-quo processes.
5. Security requires resiliency and business continuity planning as essential business functions. It is possible to plan for and test against certain more likely types and classes of disruptions.

2.6 GSC Security Management

Having described the principles of GSC security management and the strategic pillars of GSC security, the researcher now presents the GSC security management approach as an alternative to show how securing the exchange of

data can **create value** within the GSC, not only for one organization but for the entire industry. This approach is strongly recommended in order to attain the objectives of this research. First we will identify the value creation model, and then we will describe the approach.

2.6.1 *The Security Management Value Creation Model*

The value creation model is the summation of the four value chain Vs, the four security Ds, and the four solution set Cs (Ritter et al., 2007).

The four value chain Vs are visibility, variability, velocity, and vulnerability. Visibility is the ability to identify movement in the value chain. Variability is the level of consistency in the quality of value chain processes. Velocity is the speed throughput in the value chain. Vulnerability is the level of exposure to value chain disruptions

The four security Ds are Deter, Detect, Delay, and Dispatch. Deter is the ability to discourage or prevent value chain disruption. Detect is the ability to discover the existence of a threat in the value chain. Delay is the ability to temporarily impede or hinder a threat to the value chain. Dispatch is the response to value chain threat.

The four solution set Cs are Coordination, Cooperation, Consultation, and Collaboration. Coordination is the harmonious functioning of business and security initiatives for effective value chain results. Cooperation is the support given and received from others for mutual security and business benefit. Consultation is seeking knowledge to improve business and security posture. Collaboration is deliberately combining forces with others to improve business and mitigate risks.

2.6.2 The Security Management Approach

The GSC security management practices begin with adherence to the bedrock principles, the five security strategic pillars. Using these principles as a guide for implementing processes and solutions makes it possible to create value for an organization, while also ensuring standardization across all Industry participants that adhere to the GSC security management approach. They are necessarily generalized because they serve as the overarching guide for implementing the GSC security approach, marking the limits of the security processes, procedures, and initiatives that need to be managed and the areas that need to be addressed for proper implementation.

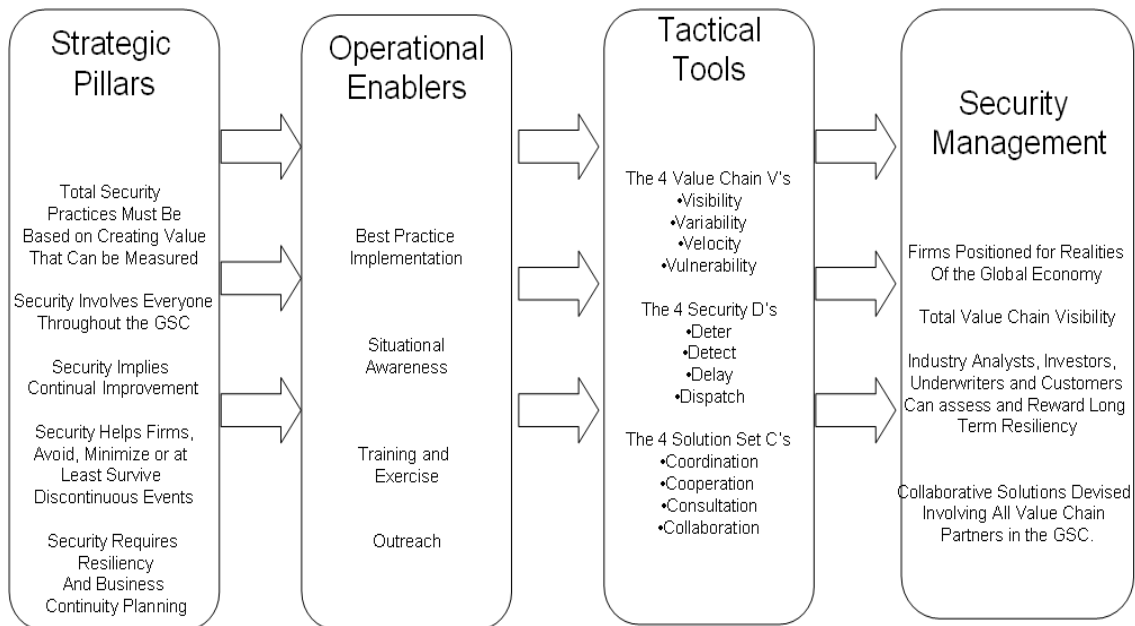


Figure 2-7: GSC Security Management Approach

Figure 2-7 underlies the GSC security management approach to show the creation of value rather than merely being a cost to the Industry participants who choose to implement it.

With the backdrop of the change agents discussed in Sections 2.4.1, 2.4.2, and 2.4.3, namely: globalization, infrastructure and economic interdependencies, and discontinuous events we have the necessary background to take a closer look at the business case that underlies the GSC security management approach. Furthermore, the addition of specifics of the five strategic pillars, the four

operational enablers, and the value creation model can help us examine how we can use the security approach to meet the GSC security objectives.

2.7 Chapter Summary and Conclusions

Securing Global Transportation Networks demonstrates how improved security processes can create value across all the business functions throughout an entire value chain. This chapter presented a review of the literature within this field. The discussions in this chapter included the importance of GSC IT Security, the significance of compliance with GSC IT security, and the challenges of IT Security and compliance in the GSC. Next, the literature findings that are specific to the hypothesis were presented. This includes a discussion of current and emerging technologies, the state of information exchange within the GSC, and the importance of risk planning and effective compliance. An extended discussion regarding RFID technology and its potential applications for GSC operations was reviewed in detail. A consideration of the ramifications of using RFID with legacy systems was discussed. The technology discussion touched on current and emerging GSC IT security technologies, including neutron-based detectors and PFNA™ technology. Technology recommendations based on the research objectives were provided.

Next, issues pertaining to global trade and electronic security management, and a number of change agents including globalization, infrastructure and economic interdependencies, and discontinuous events were addressed. In addition, the strategic pillars of GSC IT security were discussed, followed by suggested approaches to the GSC IT security management and the GSC IT security problem solving process. Finally, the importance of the GSC IT security risk management approach was examined.

Maintaining electronic security in the GSC is a daunting task. Although technologies abound, a solid approach to GSC security management is needed. Such an approach must reflect the core issues associated GSC electronic security problems, and then provide the necessary changes in GSC processes. Once the issues are understood and the processes are made effective, then the appropriate application of the right technologies could be effective by enabling the deployed technologies to create the needed security.

CHAPTER 3 RESEARCH DESIGN AND PROCEDURES

Research is the systematic process of collecting and analyzing information which helps to increase our understanding of the phenomenon under study. Chapter 1 Section 1.9 provided an overview of the research strategy and described the research methods which were used in conducting this research. Use of the Inductive-Hypothetic Research Strategy to conduct and report the investigation was described. Elaboration on the benefits that could be gained from implementing such method was provided.

This chapter discusses the research approach, research design, the methods used to collect and analyze data, and their assumptions. It concludes with some of the limitations of conducting the research in the described manner.

In the process of learning how to conceptualize the solution, the researcher has investigated and contemplated the use of a variety of modeling techniques, approaches, and tools. In addition, the researcher considered the creation of **criteria** for investigating the soundness of the conceptual solution and the demonstration of concept of the conceptual solution. Additional criteria for

adoption of the appropriate technologies were considered and established as well (refer to Section 5.4 - Technology Selection Criteria).

3.1 Research Approach and Design

As mentioned in Research Strategy - Section 1.9, in order to formulate an approach for the research strategy, one needs to understand the problems and their sources, and then determine how to investigate and solve these problems. The formulation of such an approach is based on the research process model (Steenkamp, 2005) given in Figure 3-1. The research problem required a mixed methods approach (qualitative and quantitative). These methods were applied objectively, free of bias, and adhering to standards of validity and reliability. Qualitative research methods leveraged a variety of techniques including a literature survey on GSC in the automotive industry, interviews with supply chain experts, knowledge claims (derived from observation, dialogue, and participation), and knowledge based on a grounded theory.

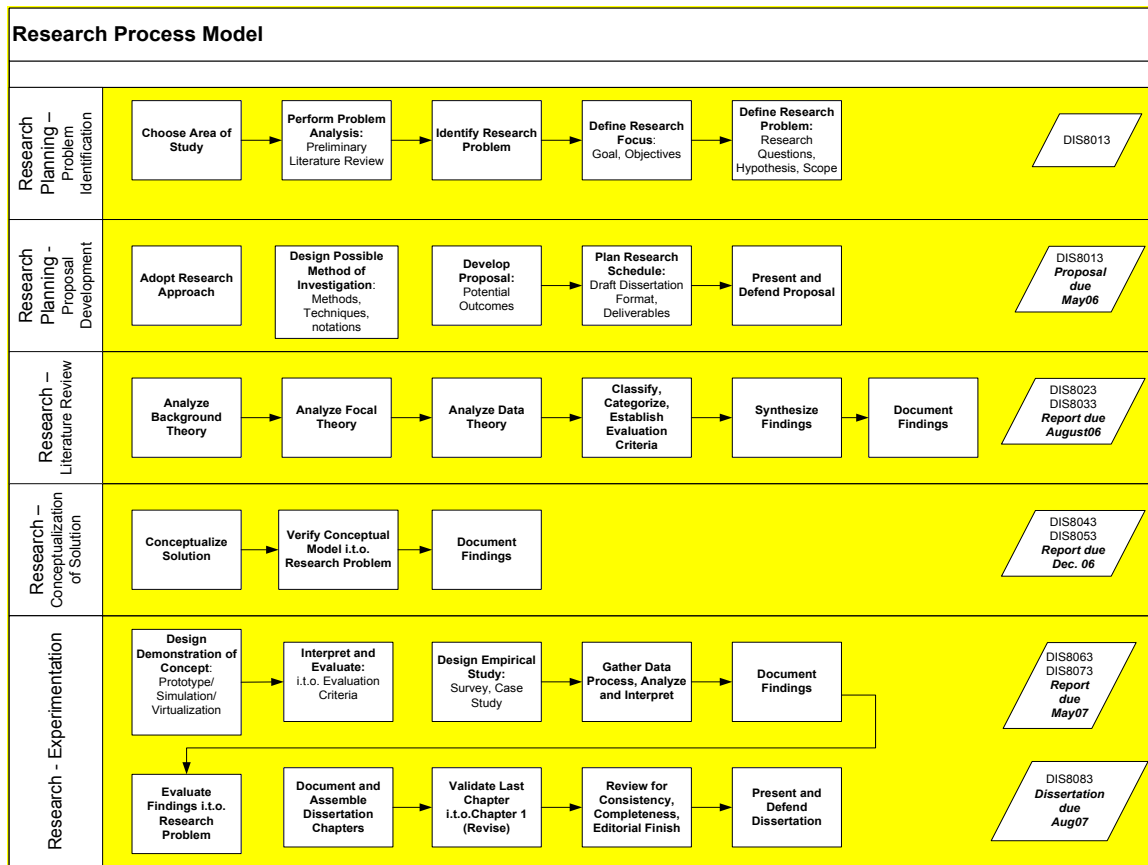


Figure 3-1: Research Process Model

The phases of the research process model are described as follows:

1. Research Planning and Problem Identification. During this phase, the researcher sets out to identify what the research is all about by describing the high level area of the research, analyzing the major problems within that area of research, identifying the specific research problem, defining the goals and objectives of the research, and formulating the research questions and hypotheses.
2. Developing the Research Proposal. During this phase, the researcher creates the research proposal which documents the research problem, the context of the research, the research strategy, and a plan conduct the proposed research. Next, the researcher presents the proposal to the dissertation committee for approval, prior to embarking on conducting the research.
3. Review of literature. During this phase the researcher analyzes the background, focal, and data theories and their application, and then

- establishes the evaluation criteria in order to synthesize the findings. This is discussed in Chapter 2 in detail.
4. Conceptualize the solution. During this phase the researcher designs a draft conceptual model of the solution to the research problem. Criteria are then developed for the evaluation of the conceptual solution and the demonstration of concept. The conceptual model is then evolved into a final conceptual solution using a modeling technique that demonstrates the relationships among the conceptual components, and how they work together to illustrate the dynamics of this conceptual model. For this research, the illustration of the conceptual solution was created by way of modeling the conceptual solution models in ProVision™ models (refer Appendix B).
 5. Validate the conceptual model and refine it into a conceptual solution. This was done by interviewing experts in the field and collecting answers to the questionnaire, as described in Chapter 1, Section 1.10.
 6. Demonstration of concept. This was done by applying the proposed “systematic approach”, discussed in Section 5.6 and developing models in each of the application phases using ProVision™.
 7. Validate the demonstration of concept in terms of the conceptual solution using previously created evaluation criteria. This is an iterative approach that continuously refines the conceptual solution.

Project outcomes and deliverables are documented throughout the research in the form of progress reports, and draft chapters of the dissertation. The final deliverable is the dissertation.

3.1.1 *Data Collection Method*

Data collection begins with the knowledge available on hand, from literature review and other sources, and expands on it to create the additional necessary knowledge to conduct the research (Yin, 2003).

Since empirical experimentation was difficult to perform due to the cost and technical resource limitation issues; structured **interviews** and **questionnaires** were used to collect informed opinions about the appropriateness of the conceptual solution thereby support or oppose the hypothesis. The process used to generate the questions took into consideration the research problem and the objectives of conducting the research. The questions were formulated in a manner that ties them back to the hypothesis. One of the major objectives of these interviews was to obtain validation of the conceptual solution in order to refine it to a shape that truly addresses the research problem. Other methods of collecting data are discussed later in this section. The interviews were designed to be adaptive and flexible, and without bias on the part of the researcher or the interviewer (Narayanan and Armstrong, 2005).

This method of data collection (interviews and questionnaires) was selected as it seemed to match the needs of this research more than other alternatives. Since access to real data of GSC IT security issues is limited and data fragmented, the researcher concluded that conducting the interviews and the questionnaire were the best techniques for collecting the data necessary to address the research problem and support the conceptual solution.

The data collected during this research came from several sources of evidence. This data was housed in a “research study spreadsheet” which can be found in Appendix C. However, data that was collected from the questionnaire only was compiled into Table 3-1. It illustrates the data that was compiled from the questionnaire answers.

IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES
Improving the Global Supply Chain through Tightening Information Technology Security

Raw Data from 11 Questionnaires

Interview #	5			7			9			5			9			10			5		
	Security			Governance			Quality			Rankings Procurement			Strategy			Integration			Compliance		
	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U
1	1	4	0	5	1	1	2	5	2	0	5	0	2	6	1	4	4	2	5	0	0
2	1	4	0	6	1	0	2	4	3	1	4	0	3	4	2	5	3	2	4	1	0
3	0	3	2	7	0	0	1	6	2	0	5	0	2	6	1	6	3	1	2	0	0
4	2	2	1	2	1	0	1	8	0	1	3	1	1	8	0	6	2	2	1	1	0
5	0	4	1	4	3	0	2	6	1	1	4	0	2	7	0	7	2	1	4	1	0
6	0	5	0	6	0	1	2	5	2	0	5	0	3	5	1	5	4	1	4	1	0
7	1	4	0	6	1	0	2	6	1	1	4	1	2	6	1	7	1	2	5	0	0
8	0	5	0	5	2	0	1	6	2	0	4	1	1	7	1	6	3	1	5	0	0
9	0	4	1	3	2	2	0	6	3	2	3	0	2	6	1	5	2	3	4	1	0
10	1	3	1	5	2	0	1	7	1	2	2	1	3	4	2	5	5	0	3	2	0
11	1	4	0	3	3	1	2	6	1	1	4	0	2	7	0	4	4	2	4	1	0

Interview number corresponds to numbers in Table 1 of Dissertation (Interviewee Organizations)
 Security Ranking: Number of No's. 5 is highest, 0 is lowest
 Governance Ranking: Number of No's. 7 is highest, 0 is lowest
 Quality ranking has possibility of 9 as a high score. 9 is highest, 0 is lowest
 Procurement ranking has possibility of 5 as a high score. 5 is highest, 0 is lowest
 Strategy ranking has possibility of 9 as a high score. 9 is highest, 0 is lowest
 Integratio ranking has possibility of 10 as a high score. 10 is highest, 0 is lowest
 Compliance Ranking: 5 questions on compliance. Positive answer is 3 to 5, and negative is 1-2.

Table 3-1: Data Compiled from Answers to Questionnaire

The **implication for the interpretation** of the sets of data caused an iterative process of refining the conceptual model.

Data was collected using the following methods:

1. Interviews with AIAG, OEM, suppliers, technology providers, and US Customs executives, managers and personnel. The interviews were discussed in detail in Chapter 1, Section 1.10.
2. Interviews with suppliers, vendors, and end users of the global supply chain. This group of interviewees was more inclined to provide answers as they have a special interest in reducing the threats of the global supply chain without interrupting the mission critical services to the business operations. The hope with the end user interviews was to inject the action research model, thereby showing them the impact of global supply chain security issues on their business decisions.
3. Data generated as a result of current government and industry global supply chain security documents, standards, policies, and processes.
4. Other government and industry documentation and historical records available via the Internet, such as UN, WTO, and WCO archives.
5. Results from industry research and supply chain support organizations such as AIAG and others.
6. Public supply chain documents and publications from academic research institutions and professional associations.
7. Note-taking from direct and participant observations
8. Several other potential sources from reading materials (books and articles) and sample case study reports on the subject of investigation at hand (please see the bibliography or List of References at the end of this dissertation).

3.1.1.1 Interview Details

As stated in Chapter 1 and various other sections throughout this dissertation, the primary method of collecting data for this research relied heavily on conducting interviews (Kakish, 2007c) and questionnaires (Kakish, 2007e) with a comprehensive representation of the GSC IT Security and Compliance industry. The process of identifying the interviewees required prior approval by the

dissertation committee and the research advisor. Eleven (11) interviews were conducted over a period of 8 weeks, involving over 20 supply chain professionals and IT executives (Snack, 2007), using a variety of collaboration methods, and in various locations. Table 3-2 represents the organizations that were interviewed and answered the questionnaire^{iv}.

#	Organization Type & Name	Description of Business
1	Supplier AAM	American Axle and Manufacturing is a 4.5 billion dollar business that specializes in manufacturing Gears and Axles. www.aam.com
2	OEM GM	General Motors is the largest OEM in the world. www.gm.com
3	Standards Body NIST	The US National Institute of Standards and Technology mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. http://www.nist.gov/
4	Supplier Federal Mogul	Federal-Mogul Corporation is an innovative and diversified \$6.3 billion global supplier of quality products, trusted brands and creative solutions to the automotive, light commercial, heavy-duty truck, off-highway, agricultural, marine, rail and industrial markets. The 45,000 people of Federal-Mogul located in 35 countries and drive excellence in all they do. http://www.federal-mogul.com/en
5	US Government DHS	Homeland Security leverages resources within federal, state, and local governments, coordinating the

#	Organization Type & Name	Description of Business
		<p>transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the federal, state, and local level have homeland security responsibilities. The comprehensive national strategy seeks to develop a complementary system connecting all levels of government without duplicating effort. Homeland Security is truly a “national mission.”</p> <p>www.dhs.gov</p>
6	<p>OEM Ford Motor Company</p>	<p>Ford is the 2nd largest OEM. www.ford.com</p>
7	<p>Governing Body United Nations</p>	<p>The United Nations is the ultimate authority on standards throughout the world. www.un.org</p>
8	<p>Governing Body World Customs Organization</p>	<p>Established in 1952 as the Customs Co-operation Council, the WCO is an independent intergovernmental body whose mission is to enhance the effectiveness and efficiency of Customs administrations. With 169 Member Governments, it is the only intergovernmental worldwide organization competent in Customs matters.</p> <p>http://www.wcoomd.org/ie/index.html</p>
9	<p>Supplier LEAR</p>	<p>Lear Corporation is one of the world's largest suppliers of automotive interior systems and components. Lear provides complete seating systems, electronic products and electrical distribution systems. In 2006, Lear ranked #130 among the Fortune 500. Lear's world-class products are designed, engineered and manufactured by a diverse team of more than 90,000 employees at 242 facilities in 33 countries. http://www.lear.com/</p>
10	<p>Technology Providers i-Connect</p>	<p>iConnect Inc. has the worldwide presence and electronic commerce experience necessary to implement global trading communities quickly and</p>

#	Organization Type & Name	Description of Business
		cost effectively. http://www.iconnect-corp.com
11	Technology Providers USGCS	Global Commerce Systems, Inc. (GCS) is a consulting company that offers services designed to help commercial and government clients manage their Global Border Operations. Their solutions increase security and compliance and reduce business risks and costs helping to streamline the flow of international border traffic. http://www.usgcs.com/

Table 3-2: Interviewee Organizations (continued)

Prior to each interview, a Letter of Introduction was sent to each interviewee in order to orient them with the researcher’s efforts, the objectives of the research, and the purpose of the interview. In addition, four documents were made available to each interviewee^v:

- An Abstract of the research (Kakish, 2007b)
- An Overview of the Interview (Kakish, 2007c) - around 30 pages of research and interview details.
- The Questionnaire (Kakish, 2007e), and
- The PowerPoint presentation used during the interview (Kakish, 2007d).

The interviews lasted from 45 minutes to 3 hours. While one-half of the interviews were conducted in person, the other half was conducted using WebEx™ conferencing technology (WebEx, 2007). Some of the interviews were structured and others were unstructured, thereby collecting a diverse set of viewpoints (Yin, 2003).

The interviews started by presenting a PowerPoint presentation that identified the research objectives, reviewed the GSC IT Security and Compliance issues and challenges, then overviewed the conceptual solution. The role of the interviewer during this process was that of an observer who is interested in investigating how IT security practices and technologies are applied by practitioners, and how the experience and knowledge of practitioners could help to improve their proposed global supply chain security framework. The interviews have served as means to achieve the following:

1. Understand the perspectives of the interviewees on global supply chain security and the issues related to it, including the potential impact it may have on the global economy. This helped with refining the conceptual solution.
2. Assess, as participant observer, concerns and reasons for the factors that lead to global supply chain improvement decisions within the US and across the globe (behavioral study).

The questions were mostly open-ended and phrased in a manner allowing the interviewees to talk openly, while the interviewer listened actively. Some have vented some of their frustrations and dissatisfaction with current supply chain security issues, policies and processes. The interviews concluded with the researcher asking for validation of the conceptual solution and any suggestions and/or recommendations that could contribute to the refinement of the conceptual solution.

The collected data was analyzed according to predetermined questions for the interviews and criteria for interpreting the answers. The research design was refined once the literature review had been completed.

3.1.2 *Data Analyses Method*

The objective of conducting the interviews sought to validate the soundness and applicability of the conceptual solution and to refine it. Therefore, analysis results of the answers provided by the interviewees were processed for this purpose. Furthermore, using the questionnaire answers, additional data were collected and analyzed with respect to the relationships among several IT related strategic business areas. These strategic IT areas included: strategy, governance, integration, quality, procurement, IT security and trade compliance.

Given the questionnaire answers, the researcher analyzed the collected data from a number of perspectives, such as comparing the category of “*compliance*” to that of “*security*”, in order to determine the most effective method(s) of applying the outcome of the analyzed data in a meaningful way. For example, the analysis of the relationship between “*compliance*” and “*security*” showed that there is a statistical correlation between the two categories. That is: as organizations

complied more with US and international trade requirements, the electronic security of these organizations were enhanced. Upon such consideration, it was determined that the most pragmatic method to use in performing quantitative analysis on this data is the Least Square Method (LSM) with Correlation and Regression Analysis. With LSM the researcher has the ability determine statistical Linear Regression and make meaningful observations and inferences (Anderson et. al., 2003). Section 3.1.3 discusses the Least Square Method and Correlation and Regression Analysis briefly.

3.1.3 *Least Square Method (LSM)*

LSM is a statistical method that is widely used in a variety of applications both in the academic and business worlds. Most importantly, it is a mathematical optimization technique which, when given a series of measured data, attempts to find a function which closely approximates the data, a "**best fit**". It attempts to minimize the sum of the squares of the ordinate differences, called residuals, between points generated by the function and corresponding points in the data. Specifically, it is called LSM when the number of measured data is 1 and the gradient descent method is used to minimize the squared residual (Anderson et al., 2003). An implicit requirement for the LSM to work is that errors in each

measurement be randomly distributed. The Gauss-Markov theorem proves that least square estimators are unbiased and that the sample data do not have to comply with, for instance, a normal distribution. It is also important that the collected data be well chosen, so as to allow visibility into the variables to be solved for.

3.1.4 *Correlation and Regression Analysis*

Correlation and Regression Analysis is another statistical method often used in experimental situations. Correlation is a measure of association between two variables. It is a measure of strength of linear relationship between two variables. The variables are not designated as dependent or independent. The two most popular correlation coefficients are: Spearman's correlation coefficient and Pearson's product-moment correlation coefficient.

The value of a correlation coefficient can vary from minus one to plus one. A minus one indicates a perfect negative correlation, while a plus one indicates a perfect positive correlation. A correlation of zero means there is *no relationship* between the two variables. When there is a negative correlation between two variables, as the value of one variable increases, the value of the other variable

decreases, and vice versa. In other words, for a negative correlation, the variables work opposite each other. When there is a positive correlation between two variables, as the value of one variable increases, the value of the other variable also increases. The variables move together. The standard error of a correlation coefficient is used to determine the confidence intervals around a true correlation of zero. If a correlation coefficient falls outside of this range, then it is significantly different than zero.

R^2 is the coefficient of determination. It is a comparison of the estimated and actual y-values, and ranges in value from 0 to 1. If it is 1, there is a perfect correlation in the sample – there is no difference between the estimated y-value and the actual y-value. At the other extreme, if the coefficient of determination is 0, the regression equation is not helpful in predicting a y-value.

The Coefficient of Determination, or multiple correlation coefficient, is a statistic which is widely used to determine how well a regression fits. It represents the fraction of variability in y that can be explained by the variability in x. In other words, it explains how much of the variability in the y's can be explained by the fact that they are related to x, i.e., how close the points are to the line. The equation for R^2 is:

$$R^2 = \frac{SSTotal - SSRes}{SSTotal} = 1 - \frac{SSRes}{SSTotal},$$

where SSTotal is the total sums of squares of the data. In the simple linear regression case, it is simply the square of the correlation coefficient.

3.1.5 *Putting the Analyses Together*

With the brief understanding of these statistical methods, one now moves toward applying these analysis techniques to the collected data for this research. The analysis techniques described in this section proved appropriate to be adopted because they provide the capability of creating inferences and conclusions based on the results of their statistical significance, i.e., correlation and regression. The **detailed analysis and actual findings** of the questionnaire data are discussed comprehensively in **Chapter 4, Section 4.5**.

The analysis of the questionnaire data was performed as follows:

1. The Questionnaire Raw Data Tables, which is found in Appendix C, was divided into several sub-tables, each containing two categories – Security and one of the remainder categories. For example, Security and Compliance, Security and Governance, Security and Quality, and so on.
2. Each sub-table contained a portion of the raw data that was collected from the answers to the strategic IT related business areas of the questionnaire for the purpose of comparing the two categories.
3. Using the LSM statistical technique, the data from the two categories (each category is represented in a column) were plotted using a “fitted line” to show statistical *correlation* or *regression*.

4. A narrative conclusion was made based of the shape of the fitted line to interpret the direction of the fitted line in layman terms. For example, a fitted line showing correlation between two categories is interpreted as such: “there exists statistical correlation between category A and category B. As category A increases in value, category B increases (in the same direction) OR decreases (in the opposite direction).
5. Although the data population was small, the assumption is made that the persons that answered the questionnaire are high-level executives or senior industry experts who represent the opinions of hundreds, even thousands of people in the field.

3.2 Limitations of the Research Design

As with any research design, there are always limitations and exploits, intentional or otherwise. Therefore, it would be wise to be aware of these limitations, and in cases where the chance of risk happening is significant, mitigation techniques and back up plans are readily available.

3.2.1 *Complexity of Implementation*

The strongest limitation of this research is the sheer size of the effort to implement the conceptual solution. Implementing a prototype alone could easily rank among the largest IT global projects, and could involve millions of dollars in initial costs and nine months to one year to implement. Training and documentation of the system adds to the complexity of such implementation.

Due to these implementation complexities, this research recommends and encourages implementing the conceptual solution on top of an existing Single Window Facilitation install base (refer Chapter 4, Section 4.6 – Conceptual Solution Implementation).

3.2.2 *The GSC IT Security Policy*

Another major limitation to this research design is the recommendation of the Global Supply Chain IT Security Policy. Establishing the global infrastructure is relatively easy compared to getting consensus on the GSC IT Security Policy. The UN and the WCO have been earnestly trying to establish and enforce a similar policy for decades, and have poured hundreds of millions of dollars, and they are yet to make a dent in this complex international challenge.

In addition, a discussion regarding the complexities of the abundance of standards and specification was presented Section 1.3 - the Research Problem. Getting only two of these international standards bodies, for example, to agree on a set of common specifications is a nearly impossible mission. So, coming to agreement on a Global IT Security Policy could only become a possible reality when at a minimum, the WCO, the UN, and the US DHS could come to

agreement. These three major regulatory and standard bodies working together could have a positive influence on the establishment of such a policy. This research suggests that the easiest route to reach this agreement could be through making the GSC IT Security Policy part of the WCO Data Model. By doing so, all organizations that subscribe to the WCO Data Model will inherently subscribe to the GSC IT Security Policy.

3.2.3 Access to Accurate Data

A third limitation to this research design has to deal with the lack of access to detailed and accurate data (specifically relative to GSC IT Security and Trade Compliance questions) from most industry participants, despite their willingness to participate. This is often explained by many enterprises' inability to access its own data effectively and promptly. In fact, sometimes, these enterprises rely on contracted services to furnish them with information about their own business. In cases where data was not readily available, the researcher relied on quotes from industry experts and IT executives.

These limitations coupled with the shortness of time and the lack of availability of some of the original intended interviewees (there were substitutes in some cases) contributed to the limitations of this research.

3.3 Chapter Summary

This chapter provided an overview of the research approach, design, and other procedures. The research approach described the adopted research process model with its five phases and elaborated on the various documentations and requirements associated with conducting the research. In discussing the research design, the foundational structure for this research was outlined. Once the research design was established, a section on the methods of data collection was provided, where a variety of techniques for collecting data were reviewed, including the preparation and dissemination of a questionnaire and conducting the interviews. Upon reviewing the collection of data, the methods that were used to analyze the collected data were discussed. In data analysis, an overview of the statistical techniques for LSM, correlation and regression analysis was provided. Next, this chapter demonstrated how these statistical techniques were used to study and analyze the collected data for the purpose of reaching conclusions, making observations, and summarizing the findings. The process for conducting the analysis was outlined. Finally, a section is devoted to discussing the limitations of this research design and suggested ways to overcome some of them.

CHAPTER 4 RESEARCH ANALYSIS AND THE CONCEPTUAL SOLUTION

4.1 Introduction

Chapter 4 is composed of three major components: 1) the draft/initial conceptual solution, 2) the research analysis and discoveries, and 3) the refined/final conceptual solution. The draft conceptual solution is represented in a meta-model consisting of the components that make up the solution. The research analysis process compiles and aggregates all the collected data from the interviews and the questionnaire, and attempts to inference meaningful observations and conclusions. The refined/final conceptual solution leverages the outcome of the analysis, as well as the action plans generated from the interviews, to provide a robust solution to the research problem. It includes details about the systematic approach to implementing the conceptual solution in a real-world enterprise.

In the process of using the results of the analyzed data to conceptualize the solution, a number of factors were considered. These included the focal and background theories and their applications, the data collected from the literature

review, interviews and questionnaire, and some of the AIAG initiatives such as MOSS and the Supply Chain Security Initiative. In addition, a variety of techniques, frameworks, and tools were considered in order to build the conceptual solution. These include Class Diagrams using UML notation, Rummler-Brache Performance Matrixes, information analysis, requirement analysis, gap analysis, design principles, strategy hierarchy, organizational influence, project initiation framework, and levels of conformance.

This chapter begins with describing the draft conceptual model, which was created solely based on the researcher's understanding of the research problem. It did not take into consideration any input from the experts in the field, as none was available at the time because the interviews were not conducted yet. The researcher has experience in the automotive industry, GSC, and Information Technology electronic security. The initial design of the conceptual solution was drafted by relying on this experience and complementing it with the review of literature. While this effort served as a starting foundation on which a conceptual solution could be built, a more comprehensive design was needed in order to address the research problem and the needs of the industry participants. Hence, the analysis of data was needed in order to refine, validate, and finalize the

conceptual solution. So, the next major component of this chapter deals with the analysis of the data collected from the interviews and questionnaire. Finally, the outcome from data analysis served as input into the refinement of the conceptual solution, giving it the final format.

Several additional topics and issues are also discussed in chapter 4. These topics serve as factors and drivers in support of the data analysis discoveries and the validation of the conceptual solution. The artifacts that make up these topics take into consideration how ISO 12207 could be structured into Software Life Cycle Processes (LCP), which in turn could directly map to the Rummler-Brache Performance Matrix. These issues and topics are discussed in Section 4-6.

A key section in this chapter deals with the **Systematic Approach** that is mentioned in the hypothesis. This Systematic Approach is composed of a GSC IT Security Process Model coupled with a GSC Methodology that could be utilized by any given organization for the purpose of adopting the proposed conceptual solution of this research. This Systematic Approach is also referenced in Chapter 5 – Demonstration of Concept in order to show that by adopting this systematic approach organizations have a “how to” process for implementing the

conceptual solution. Appendix B contains a significant number of models that illustrate the process model associated with the systematic approach. The sections of this chapter are outlined as follows:

- Draft Conceptual Model
- Analysis of research findings
 - Information Analysis
 - Requirement Analysis
 - Gap Analysis
- Conceptual Solution Acceptance Criteria
- Refined Conceptual Solution
- Systematic Approach for Implementing the Conceptual Solution
 - Systematic Approach Process Model
 - Systematic Approach Methodology
- Summary and Conclusion

4.2 Draft Conceptual Model

Once the background theory was explored and the focal theory was further specified along with its applications, the research problem was understood and formulated. As mentioned in Section 4.1, the draft conceptual model was solely designed based on the researcher's professional experience coupled with the knowledge gained from the literature review. The intent was to establish a conceptual solution foundation to facilitate collaboration with the interviewees, so that the draft could be refined and evolve into a robust conceptual solution that addresses the research problem and meets the needs of the interviewees.

In order to conceptualize the solution, the researcher has relied on a variety of models and meta-models, assumptions, approaches, and techniques. Such artifacts include criteria for adoption (including technology selection criteria), demonstration of concept, focal theory, background theory, and other relevant solution conceptualization factors (Creswell, 2003).

The ultimate purpose of the conceptual model is to facilitate secure and efficient GSC data exchange through dynamic maintenance of a global IT Security Policy, ensuring industry participant compliance, and providing tools that enable linkage and possible integration with the existing ERP and SCM systems.

The conceptual solution also addresses other supply chain issues and complexities related to IT areas such as:

- Electronic Commerce (EDIFACT, EDI, XML, Web Services, etc).
- ERP Integration (governance, interoperability, data management, etc).
- IT Architectures (data, application, infrastructure, security, business, governance, quality, etc).
- Network security (cryptography, public key infrastructures, wireless networks, change management, privilege management, etc).

The initial conceptual model (AKA Draft Conceptual Solution) is depicted at a high level in Figure 4-1 and described as follows:

Global Supply Chain IT Security Hosted Services

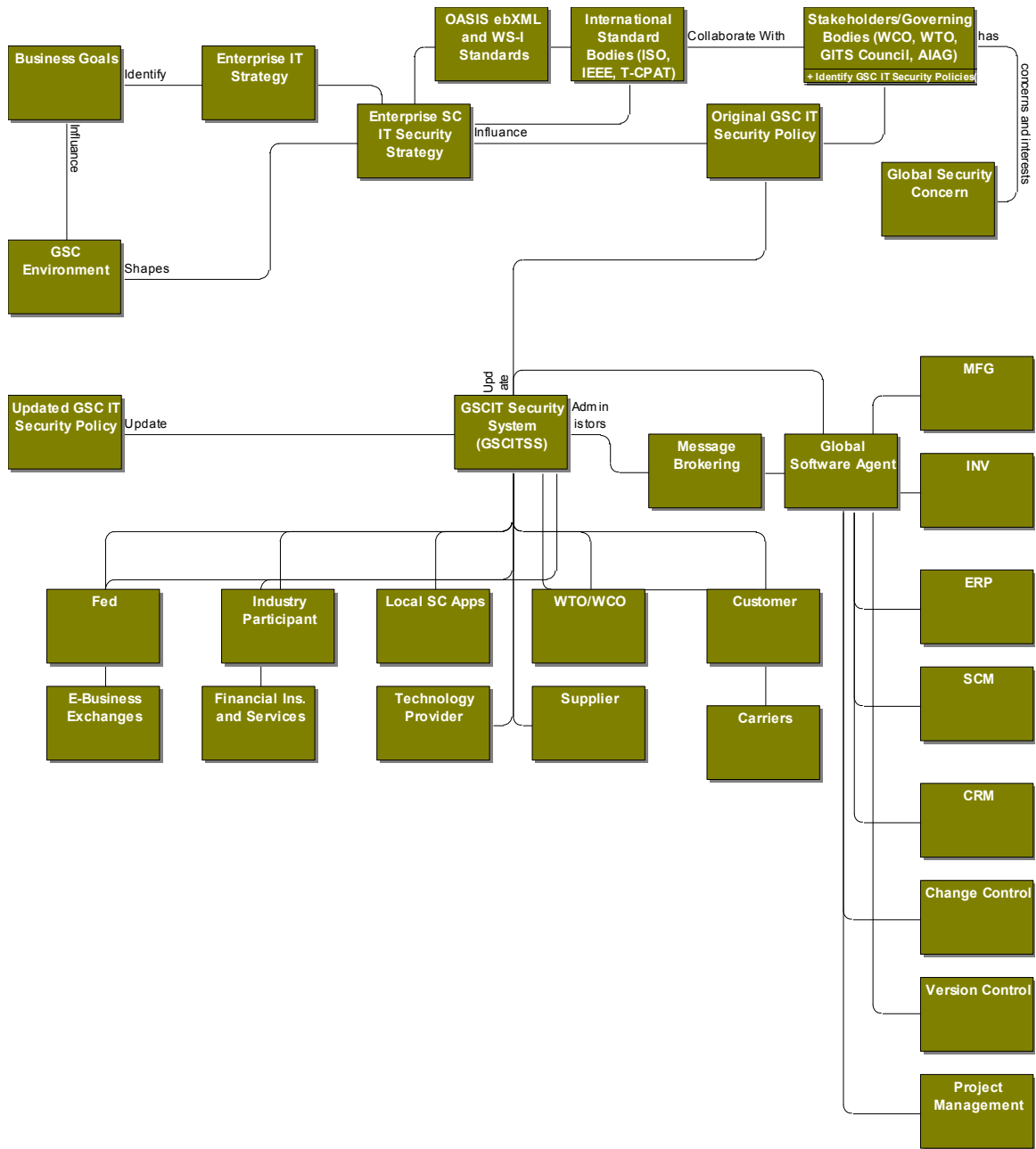


Figure 4-1: Draft Conceptual Model

A framework for GSC Hosted IT Security Services is shown in Figure 4-2, and comprises of the following components:

1. Industry Organizations (AKA Participants) - These include: OEMs (in this scenario OEMs equal US Tier-1 suppliers), Developing World Suppliers (in this case these are known as Small-to-Midsize Enterprises - SMEs), customers, World Organizations (ex: WCO, WTO, UN, etc), Regulators (ex: International Governments, US Federal Government agencies), Technology Providers (IBM, Oracle, Microsoft, etc), Carriers, Financial and Insurance Services, e-Business/e-Commerce industry marketplaces and exchanges (ex: COVISINT), retailers, and consumers.

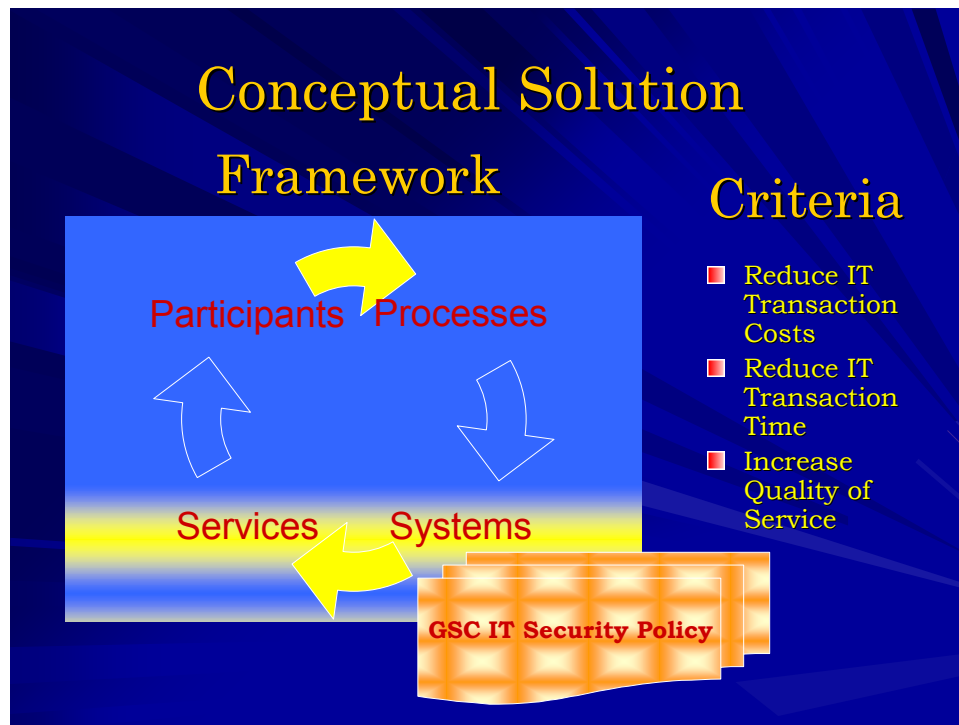


Figure 4-2: GSC IT Security Conceptual Framework

2. Processes - A set of processes (based on regulatory and business objectives) defined and agreed upon by all major industry participants. Such processes drive standards that simplify infrastructure, and provide for common means communication, interoperability, and data exchange. Standards result in quicker implementations with reduced variables. For technology providers, standards development provides a competitive advantage by building knowledge about cross-industry and intra-industry drivers, and developing products and services accordingly.

3. Systems - Technologies designed and implemented in terms of web-based software systems and tools. These web-based systems will leverage a variety of tools and technologies including web servers, network and communication servers, IT security and policy servers (for authentication and compliance), and software application servers for integration with existing ERP and SCM systems (Bowersox, et al., 2007). Figure 4-1 illustrates the technology relationship with the other components of the conceptual solution in terms of a meta-model framework. In particular, the Figure shows how the conceptual solution system (GSCITSS) integrates and/or links to Line-of-Business applications. These technologies should enable the industry participants to access automotive transaction data forward-and-backward providing secured visibility throughout the GSC.
4. Services – These include a range of support activities that enable the trading partners to exchange data securely and assure compliance of the SMEs in developing countries. The details of these services can be found in the technical design specifications, which are outside the scope of this report due to space limitations. These services will work to satisfy the pre-determined criteria of:
 - a. Reducing IT transaction costs.
 - b. Reducing IT transaction time.
 - c. Increasing the Quality of Service (as shown in Figure 4-2).
Examples of these services should manifest the ability of Tier-1 suppliers in the US to present their purchasing needs to a much larger “complying” SME base throughout the world. Equally, the same services could enable developing country suppliers to compete legitimately at a global level.

The combination of the components above working together makes up the entire conceptual solution.

The meta-model (Figure 4-1) for the conceptual solution has a number of components and entities, as follows:

1. **Stakeholders** – the stakeholders include the Global Supply Chain IT Security Council, the World Customs Organization (WCO), and the World Trade Organization (WTO). Membership into the Global Supply Chain IT Security Council is determined by the WTO and appropriate wings within the United Nations. Membership for all countries which conduct automotive business is provided by directly subscribing to GSCITSS system or the WCO, in which case they would be WCO data model subscribers.
2. **Global IT Security Concerns** – is a list of concerns compiled by AIAG for the global automotive industry, and populated by approved input from the US/DHS, other US and AIAG global project initiatives such as C-TPAT, Supply/Chain Security initiative, MOSS, Returnable Container, etc.
3. **Enterprise** - representing the industry participants (such as, Supplier, Customer), and in some cases Governmental Institutions (Federal and Local)
4. **Enterprise Strategy** – is the business strategy that is produced by each enterprise for its own business strategy relative to IT Security. It results from the enterprise evaluating/assessing its global SC IT security readiness as defined by the concerns (#2) above.
5. **Enterprise Architecture** – is the IT architecture – many would disagree about this definition. The EA is larger than the IT architecture - for the Stakeholders' enterprises, shaped by various viewpoints which include IT Infrastructure, Application, Data, and Security. The Enterprise Architecture is driven by the IT Architecture for that enterprise.
6. **IT Architecture** – is the set of models that provide an IT architectural description of the Enterprise. It contributes to, and to a large extent determines how the enterprise goes about managing its own processes. The IT Architecture is largely driven by the Enterprise IT Governance.
7. **IT Strategy** – is the strategy which is produced by each enterprise for its own IT strategy relative to IT Security. It results from the enterprise evaluating/assessing its global SC IT security readiness as defined by the concerns (#2) above, and from the IT Architecture (#6) above.
8. **GSCITSS** – is the conceptual solution system - Global Supply Chain IT Security System that is designed and implemented based on requirements that come from the Enterprise IT Architecture, Enterprise IT Strategy, Global IT Security Concerns (#2), Stakeholders (#1), Global SC IT Security Policy (recursively updates policy, and policy updates GSC/ITSS),

Enterprise IT Security Strategy, Business Goals, and the Environment. It also interacts with web-based ERP Agents, CRM Agents, and other e-business and e-commerce agents.

9. **Global SC IT Security Policy** – is a Global SC IT Security Policy that is initially established by the Stakeholders (#1), and the frequently updated by the GSC/ITSS. This policy also updates the GSC/ITSS system on regular basis.
10. **Enterprise IT Security Strategy** – is the IT Security Strategy developed by the stakeholders for the goals of the Enterprise.
11. **Business Goals** – which are driven by the business strategy
12. **Environment** – in which strategies, goals, objectives, and projects are implemented.
13. **ERP Agents, CRM Agents, and other e-business and e-commerce agents** that enable communication, and in some cases, interoperability with the GSC/ITSS.

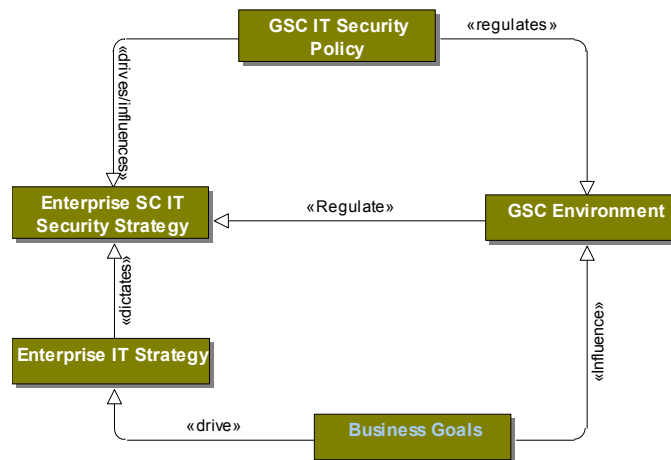


Figure 4-3: Class Model for GSC IT Security Policy

Figure 4-3 illustrates the relationships surrounding the GSC IT Security Policy, GSC Environment, Enterprise business and IT strategies, and Business Goals. Understanding these relationships is self explanatory. For a complete

interpretation of the meta-model and its components and their relationships, please refer to **Appendix B, Sections 1&2**.

4.2.1 *Conceptual Solution: Key Issues*

When it comes to conceptualizing a solution, designers' success can be undermined by preconceptions, hasty decisions, and personal biases. Therefore, it was essential for this research to take into consideration *critical issues* that has the potential to impact the outcome, even lead to new knowledge and discoveries. Such issues include Compliance, Strong Identity and Access Management, GSC Security Cost reduction, Risk mitigation, forensics analysis, integration and automation, GSC security infrastructure, continuous business operations, and the security views required to achieve continuous regulatory compliance. The following tasks were performed to identify the key issues in the GSC:

1. Mapping of industry participants' business requirements to global supply chain security solutions.
2. Applying governing security concepts and standards to the global supply chain IT infrastructure.
3. Assessing global supply chain IT process maturity.
4. Assessing the IT environment for security opportunities.
5. Aligning emerging supply chain management products with IT security improvement opportunities.
6. Assessing requirements and creating a solution design.

7. Describing business and technical advantages of supply chain IT security solutions.
8. Applying security concepts to the solution design.
9. Recommending education opportunities to industry participants based on the GSC IT security solution.
10. Supplying a transition document to interested parties.

4.2.2 *Conceptual Solution: Skills Requirements*

In addition, the following key skills and competence requirements for developing the conceptual design of the solution were identified:

1. Conceptual knowledge of IT process models (e.g. Information Technology Infrastructure Library (ITIL)).
2. Experience with IT organizational structures.
3. Conceptual knowledge of IT security services (authorization, authentication, confidentiality, data integrity, non-repudiation).
4. Conceptual knowledge of IT security standards and protocols (government and civil), regulations, and certifications.
5. Conceptual knowledge of IT security applications' features and functionality.
6. Familiarity with security aspects of key GSC management products.
7. Familiarity with other GSC emerging security products (RFID, Server Security, SSL accelerator cards, etc).
8. Familiarity with IT security education offerings.
9. Conceptual knowledge of networking environments, operating systems, relational databases, application environments (Java, .NET, etc.), key vendor environments (SAP, Siebel, PeopleSoft, Oracle, Microsoft, etc).
10. Capability to assess and analyze security maturity according to industry standards.
11. Ability to create a business case justification for an IT project, especially one of the magnitudes of the conceptual solution for this research.
12. Experience defining proof of concepts and associated success criteria.
13. Working knowledge of "Best Practices" for IT processes (measurable, repeatable, documented, etc).

4.2.3 *GSC IT Security Policy*

As eluded earlier in various sections of this dissertation, the implementation of a GSC IT Security Policy is essential to the success of the conceptual solution. Ideally, once the policy is created, it could be incorporated within the WCO Data Model. A number of attempts were made to discuss implementing this recommendation with the WCO, however, due to the lack of response (from the WCO) and the time constraints (to complete the research project), a final decision has not been made yet. Exhibits 1 and 2 illustrate the importance of a GSC IT Security Policy and explain why it is needed, and how it could fit within the SAFE Framework and the Data Model.

4.3 **Conceptual Model: Acceptance Criteria**

Section 4.2 discusses the draft conceptual solution based on the researcher's understanding of the research problem, the review of literature, and professional industry experience. However, in order to ensure that the conceptual model effectively meets the needs of the industry participants (the interviewees), an **acceptance criteria** for evaluating the effectiveness of the conceptual solution needed to be developed. Such criteria were collaborated with the interviewees and were developed to validate the conceptual solution.

The conceptual solution acceptance criteria involve three aspects:

1. Reduce IT Transaction Costs
2. Reduce IT Transaction Time
3. Increase Quality of Service

These criteria have been agreed upon by the various interviewees.

4.4 Moving Into Analysis

After presenting the draft conceptual model to the interviewees and collecting their feedback, the researcher compiled the data from the interviews and the questionnaire in order to refine the conceptual model into its final form. This was accomplished by analyzing the data collected and executing the elements of the Action Plan suggested by the interviewees.

4.4.1 Action Plan that contributed to refining the conceptual Model

The following action plan was created based on the insights gained in the interviews:

1. Change Workflow Modeler (Swim-lanes) in PV to reflect Hosted IT Services/Hub.
2. Consider/devise an approach to align with IT infrastructure providers for this market: IBM; Covisint (Hub infrastructure); GSX (Web Server Monitoring); ASXONE (Compliance); Sterling Commerce (SCM & Logistics); iConnect (iExchangeWeb - Global Web EDI & XML any-to-any)

- data transformation solution); EDS's IMDS (International Materials Data System).
3. Outline pre-certification process in order to access web-based system.
 4. Outline Compliance Certification process for SMEs and validate with US Customs and WCO.
 5. Develop XML-based Standard Data Templates for web-based system (or use the 12 XML data sets that AIAG developed).
 6. Outline GSC IT Security Policy at high level.
 7. Map GSC IT Security Policy to WCO SAFE Framework.
 8. Map relationships between GSC Hosted IT Services system and Single-Window system design.

4.5 Analyses of Research Findings

With the key data collected, the next logical step in the research is to perform adequate analyses of the data in order to create the requirements needed to design the conceptual solution. In this research, the requirements were captured by applying the Performance Matrix, Questionnaire, Interviews, and literature review.

The next logical step in the conceptual solution design process is to analyze the information contained within these requirements. To do so, the researcher leveraged the process model from "Managing the Information Technology Resource: Leadership in the Information Age" (Luftman, 2002) and Information Analysis Process suggested by Perks and Beveridge (Perks, et al., 2003).

4.5.1 *Information Analyses*

To gain an adequate functional understanding of the information requirements, it is necessary to decompose the high level organizational functions into more primitive functions, using techniques such as functional composition. The relationships between functions (or functional dependencies) should be distilled. This will provide an effective tool for communications and will aid in highlighting gaps and overlaps. For example, the following relationships were considered by the researcher in the information analysis process:

1. Mapping the identified information entities (from the questionnaire, which is a modified and customized Rummler-Brache Management Checklist) against information needs, which came from the interviews and other industry literatures. This aided in providing the models against the strategic, tactical, and operational information needs of the organization. Discovering information needs represented strategic value for the decision making process of senior management. Figure 4-4 illustrates the Information Hierarchy. The number of information entities at the top of the hierarchy is generally small and described by strategic business language. The number of entities at the bottom can potentially be enormous and have specialized business meaning. Therefore, it is important not to get bogged down in detailed analysis at the operational level. Furthermore, mapping the information entities against information needs can indirectly aid in identifying functions that satisfy information needs.
2. Mapping information entities against business functions, which were gathered from the interviews, provided an indication of the effect of functions on entities.
3. Mapping business functions and entity types to organizational units. This allowed information and function to be assigned, or pigeonholed against various parts of the organization.



Figure 4-4: The Information Hierarchy

Information analysis allows the GSC participants to model their understanding of their organizations based on an information view. This provides valuable information. Finally, a common understanding of the basic GSC IT Security Services/Facilities is needed. These **services** should be *understood, agreed to, and supported by all GSC Industry participants*, especially those who work in IT.

The services include: Operational information binding and retrieval; Cryptographic support facility; Authentication; Authorization; and Security audit. Figure 4-5 illustrates these essential IT security facilities.

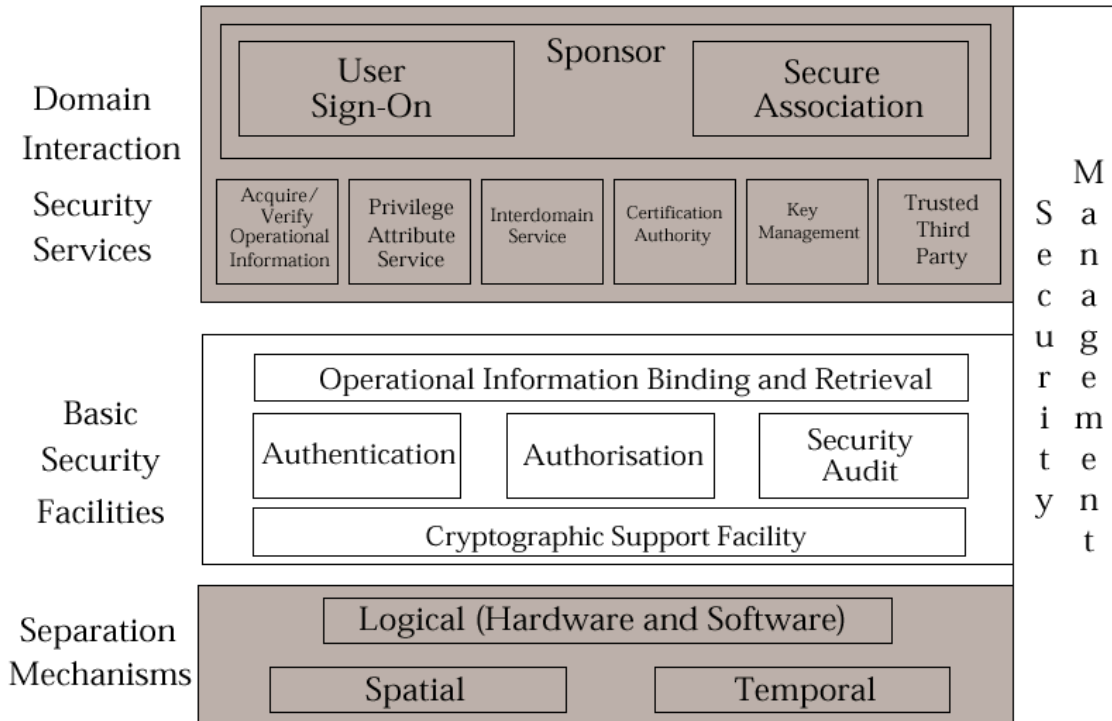


Figure 4-5: GSC IT Basic Security Services/Facilities.

4.5.1.1 Layering of Security Services

The layering of services is a common characteristic of IT system architectures. For services located at all but the lowest levels within the system, both service functional and data elements are often formed out of the more primitive elements of underlying services through the use of the interfaces to those underlying services. Incorporation of layering of security functionality into IT system architectures is particularly important because it enables a reduction in the amount of trusted code by isolating common critical security functions, and

reduces the exposure of application logic to specific security mechanisms, which are often subject to change. Figure 4-6 illustrates the concept of the layering of security services for cryptographic-based services.

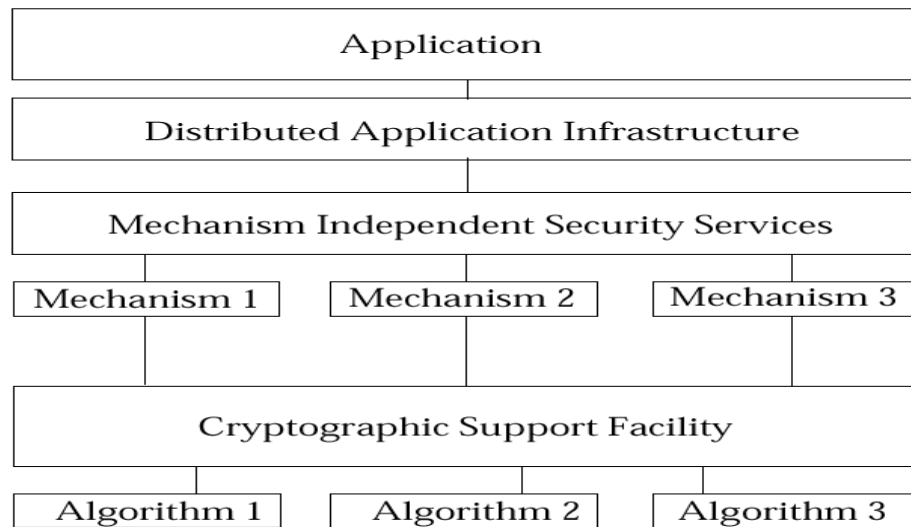


Figure 4-6: Conceptual Layering of Security Services

At the highest layers are applications that may have no security responsibilities. Security responsibility increases with each lower layer. Conversely the abstraction of security service reduces with each lower layer. The details of the security service become more visible and relevant at the lower layer.

4.5.2 *Gap Analysis*

Gap analysis is a technique for the discovery and management of gaps that result during the planning of a transition between an initial state and a target state

(Luftman, 2004). It relates to the assessment of a desired (or target) state against the current state, with the objective of understanding the gaps between the two. Figure 4-7 depicts a generic gap analysis model. State why adopt this technique here.

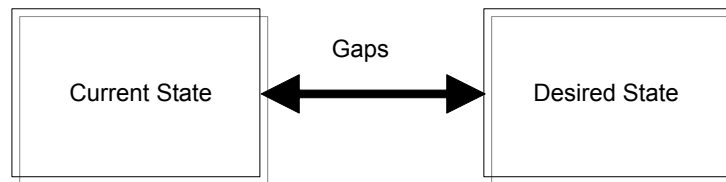


Figure 4-7: Generic Gap Analysis Model

Performing gap analysis enabled the researcher to discover the following findings:

1. Supply chain management (SCM) software is one of the most fractured groups of software applications on the planet – too colloquial. Each of the major supply chain steps composes dozens of specific tasks, many of which have their own specific software (Bowersox et al., 2007).
2. Some vendors have assembled many of these different chunks of software together under a single roof, but no one has a complete package that is right for every company.
3. Because each industry's supply chain has a unique set of challenges, many companies decide to go with targeted best of breed products instead, even if some integration is an inevitable consequence.
4. Many SCM applications are heavily reliant upon the kind of information that is stored in the most quantity inside ERP software. Most CIO's who have tried to install SCM applications say they are glad they did ERP first.
5. Security of major SCM applications is vulnerable.
6. There are significant incompatibilities among GSC security systems. This adds to the complexity of IT system integration.

7. A global secure web-based solution is needed to address several issues associated with these complexities and challenges within the GSC. For example, IT system integration, within and across the enterprise.

Global Supply Chain IT Security Application Type: Security System Service Category: Security Services				
	Sub-Category	Present? (Y/N)	Supporting Technologies	What is needed?
	Identification & Authentication	Yes and No	Mostly legacy systems, RACF	Emerging Technologies, interoperability
	unauthorized modification	Y	IDS and IPS	Advanced Cryptography
	unauthorized disclosure	Y	Variety of custom technologies	Uniformity and compliance
	denial of service	Y	Mostly imbedded in network infrastructure	Global vendor compliance
	Repudiation (assuring identifiable delivery of info)	Y	Mix of legacy and emerging tech. (RACF, TIVOLI, SMS, etc)	Uniformity and compliance
	unauthorized use of resources	Y	Variety of Asset Management and HR related ERPs.	Integration between GSC Mgt SW & ERP.

Table 4-1: Global Supply Chain IT Security Gap Analysis Model

Table 4-1 depicts a gap analysis model for the security service category within the GSC.

4.5.3 Analysis of Interview Data that Refined the Conceptual Solution

As an on-going effort to keep the data of this research timely and readily available for lessons learned and other benefits, a journal (aka “the log”) was used to document all observations and insights gained during the interviews. Some of the insights from the interviews yielded the following observations about the **refinement of the conceptual model**:

1. Narrow focus of data transactions to Order-to-Cash logistical types only.
2. Focus more on data exchange and less on design documentations and collaboration
3. Focus conceptual model on IT hosted end-to-end Order-to-Cash WCO-SAFE & C-TCPAT globally compliant infrastructure solution.
4. Bring more visibility to the Hub concept and Single Window.
5. Focus more on infrastructure and networking issues, not just IT security.
6. Focus more on off-shore OEMs and Joint Ventures (JVs) for developing countries (Korea, Russia, South Africa, Indonesia, Thailand).
7. Conceptual model is appropriate for 2nd largest aftermarket supplier.
8. Example of how this model would work with China SMEs, was given. They don't have electronic documents or tools.
9. “Compliance is not even addressed at this point. It is a huge issue”.
10. As for IT and EDI security, the assumption made is that if it works with the developed countries then it should work with the developing countries.
11. Industry participants would like to see WCO SAFE framework applied and adopted by developing countries. Most of them have NOT dealt with electronic transfer of data.
12. Infrastructure is an issue for developing countries.
13. Prepare a pre-certification process for SMEs in order to access web-based system.
14. Prepare a Certification Process similar to Quality Certification for SMEs compliance.
15. Standard XML-based data templates are necessary as single point of entry into web-based system.
16. Add to the list of countries: India, China, and countries that are no longer part of Russia.
17. Minimize and/or avoid any infrastructure costs to SMEs to encourage them to participate electronically.
18. Consider WCO Data Model Hierarchy

19. Consider UN Recommendation 34
20. Reality vs. What T1 Suppliers say vs. what they do.

4.5.4 *Analyses of Questionnaire Data.*

As explained in Section 1.10, the Questionnaire represents a modified and customized version of the Perks and Beveridge Management Checklist (Perks & Beveridge, 2003). It seeks to explain strategic issues related to the behavior of IT management and industry participants. It uses a mixed-methods (qualitative & quantitative) descriptive research design (Creswell, 2003). A response with more than 10 “yes” answers raises a red flag for action to be taken. For analysis of the Questionnaire, the “yes” answer, “no” answers, and “unsure” answers were tallied. Each answer is worth one point. A reasonable number of YES answers (say, greater than 10) indicate that the organization should review the way GSC IT Security policy and technology are managed.

The results of analyzing answers from the interviews and the questionnaire imply the following:

1. Most USA-initiated data exchange transactions are electronically secure, given adequate implementation of SCM systems and technology infrastructure

2. IT security of developing world countries data transactions is largely driven by USA OEMs and Suppliers, at least for those suppliers doing business with US manufacturers.
3. Compliance is almost non-existing among most developing country SME's. Compliance issue is one of just getting electronic capability vs. paper.
4. A Global Supply Chain IT Security Policy is necessary to improve compliance.
5. The results also demonstrated a statistical correlation between IT Security and compliance.

Table 4-2 shows the raw data of the two strategic areas: *IT Security and Trade Compliance*. This data shows the relationship, for comparison and observation purposes, between these various strategic IT related business areas that were asked of the interviewees via the questionnaire. **Appendix C** contains the raw data collected from the Questionnaire for all IT Strategic categories.

Security and Compliance						
Interview #	Security			Compliance		
	Y	N	U	Y	N	U
1	1	4	0	5	0	0
2	1	4	0	4	1	0
3	0	3	2	2	0	0
4	2	2	1	1	1	0
5	0	4	1	4	1	0
6	0	5	0	4	1	0
7	1	4	0	5	0	0
8	0	5	0	5	0	0
9	0	4	1	4	1	0
10	1	3	1	3	2	0
11	1	4	0	4	1	0

Table 4-2: Questionnaire Data for Security & Compliance

Upon plotting the “No” answers of Security with the “Yes” answers of Compliance in MS Excel™ in a XY Scatter Chart, we obtain the fitted line shown in Figure 4-8 with a coefficient of determination $R^2 = 0.7234$. Figure 4-8 illustrates the plot that resulted from analyzing the relationship between IT Security and Trade Compliance. One could clearly observe that there exists a high statistical correlation between IT Security and Trade Compliance among the eleven organizations interviewed. This correlation suggests that the more IT secure an organization is the more trade compliant it is, and visa versa. The raw data is shown in Appendix C for the entire set of categories. However, the plots that show the relationships between IT Security and the rest of the categories are shown in Figures 4-9 to 4-12.

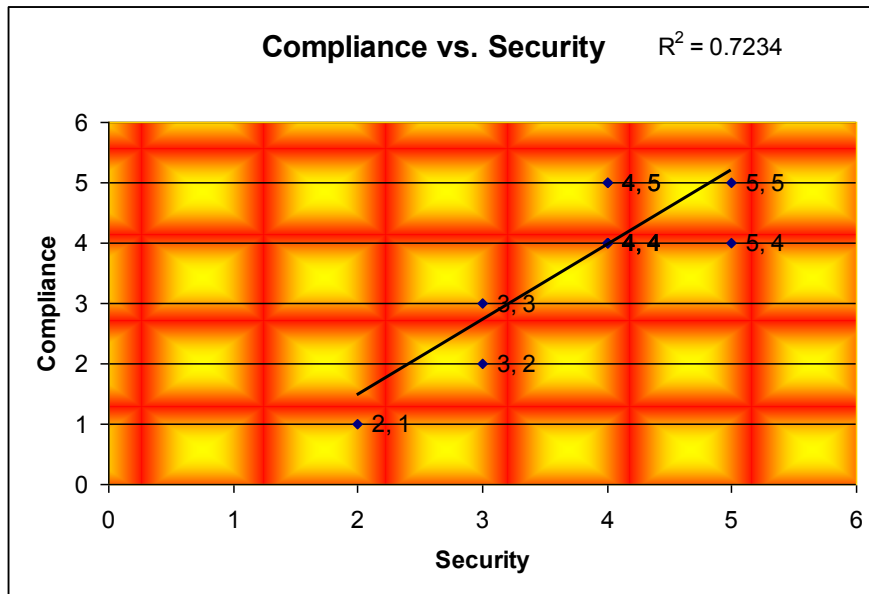


Figure 4-8: Using Least Square Method to Correlate Security & Compliance

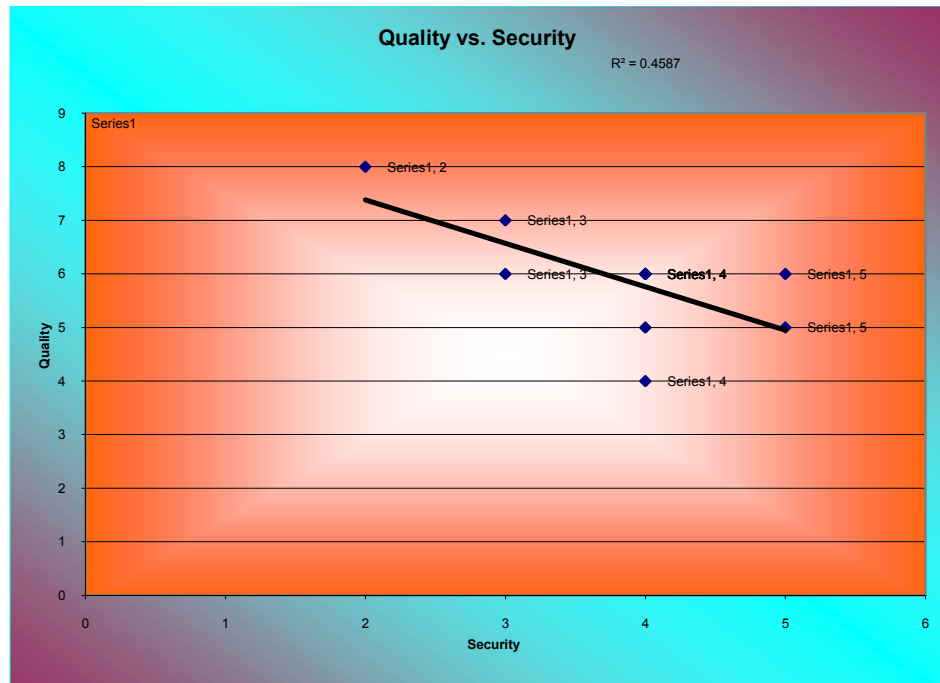


Figure 4-9: Relationship between IT Security and Quality

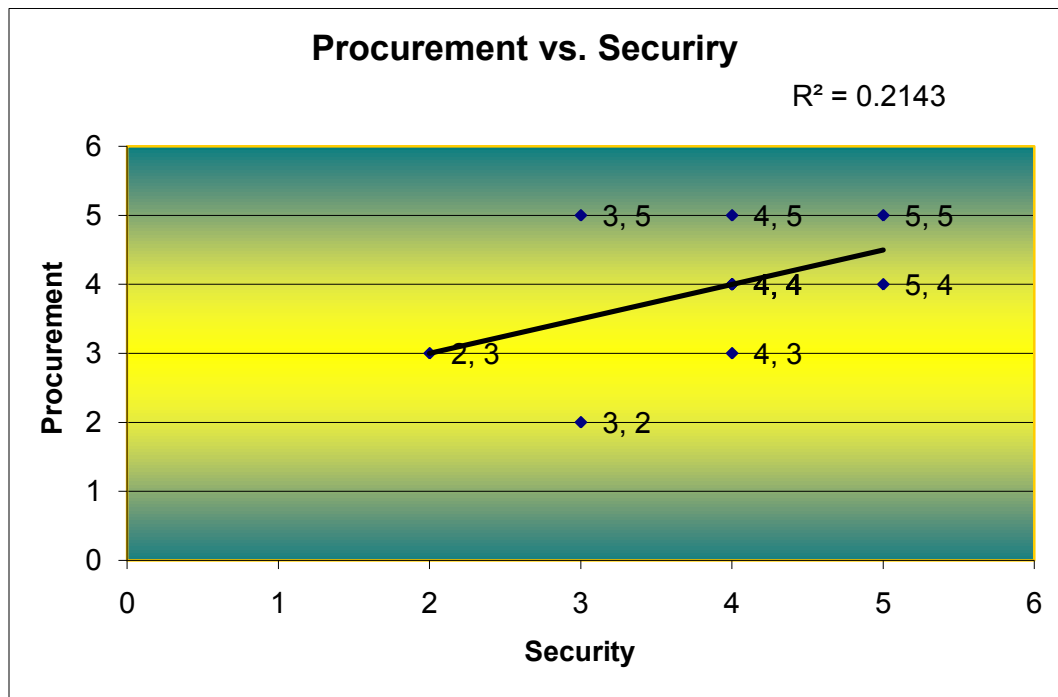


Figure 4-10: Relationship between IT Security and Procurement

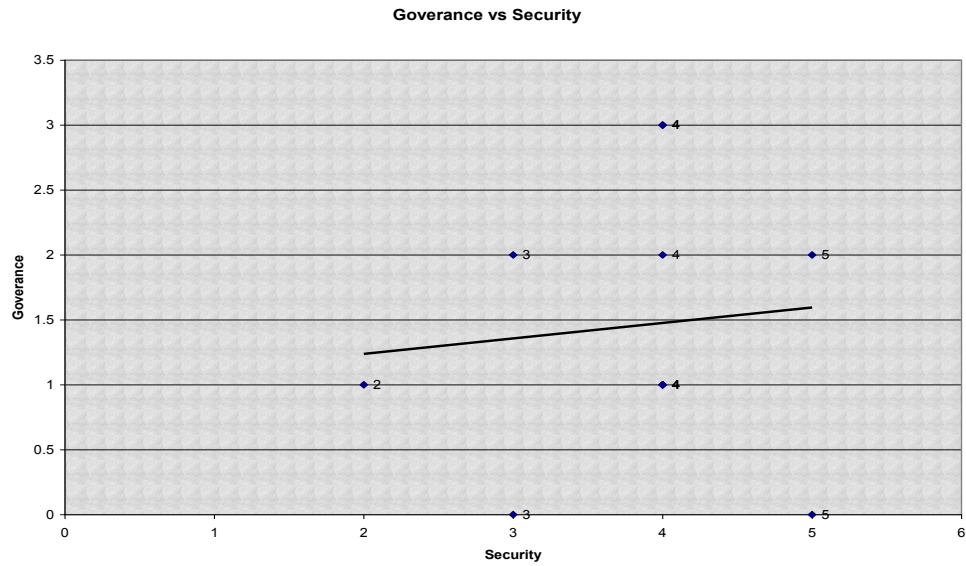


Figure 4-11: Relationship between IT Security and Governance

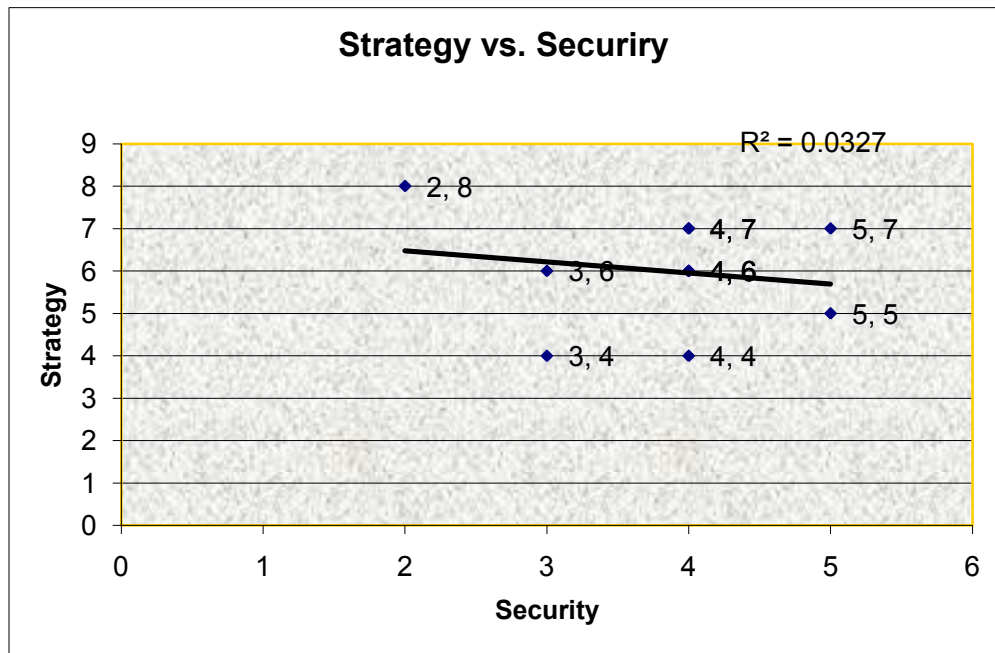


Figure 4-12: Relationship between IT Security and Business Strategy

4.6 Rummler-Brache Performance Matrix & Mappings

From the feedback to the questionnaire (refer **Appendix A Section 3**) there are a number of IT security issues (from the Y/N/U answers) within the GSC that need in-depth investigation in order to create a conceptualized solution. To do so, the researcher constructed a Rummler-Brache Performance Matrix which yielded *areas of misalignment*, a deeper understanding of key IT security GSC issues, and additional areas of investigation at operational and tactical (projects/initiatives) levels.

In keeping with the commonality of life cycle process standards, a mapping of the Rummler-Brache Performance Matrix and ISO 12207 life cycle processes is shown in Table 4-3.

ISO 12207 Life Cycle Processes		
Life Cycle Process	Maps To	Performance Matrix
Primary LCP Acquisition <ul style="list-style-type: none"> • Supply • Development • Operation • Maintenance 	Maps To	Process Level
Organizational LCP <ul style="list-style-type: none"> • Management • Infrastructure • Improvement 	Maps To	Organization Level

<ul style="list-style-type: none"> • Training 		
Supporting LCP <ul style="list-style-type: none"> • Documentation • Configuration management • Quality assurance • Verification • Validation • Joint review • Audit • Problem resolution 	Maps To	Activity Level

Table 4-3: Mapping of ISO 12207 to Rummler-Brache Performance Matrix

The complete details of the Performance Matrix are found in **Appendix A, Section 3.**

4.7 Refinement of Conceptual Solution: Key Issues and Requirements

The research analysis discussed in Section 4.5 and the discoveries of certain outcomes played a key role in refining the conceptual solution to a design that not only addresses the research problem, but meets most of the industry participants’ needs as well. With the understanding of the issues associated with GSC IT Security attained, reviewing the feedback from the interviews and questionnaire, and the analysis of data in Section 4.5, the draft conceptual model was transformed and evolved in the framework presented in Figure 4-13.

In an industry as high profile and closely watched as the automotive industry, secure and timely information is key to the success and continued advancement of the industry and its participants.

Clearly, the automotive industry today suffers from a multitude of issues related to the security and timely availability of accurate information. A number of recent studies have shown that electronic security of automotive data transactions remains a chief contributor to the inefficiencies with the automotive Global Supply Chain (Benson et al., 2005; Willis et al., 2004).

In an attempt to address these security concerns, this research strove to:

- Identify and investigate these issues and challenges.
- Identify the risks associated with these issues.
- Prototype a conceptual model that, upon validation and implementation, could address the IT security and trade compliance concerns associated with the automotive data that transacts throughout the globe on daily basis.

The conceptual solution also addresses other supply chain issues and complexities related to IT areas such as:

- Electronic Commerce (EDIFACT, EDI, XML, Web Services, etc).
- ERP Integration (governance, interoperability, data management, etc).
- IT Architectures (data, application, infrastructure, security, business, governance, quality, etc).

- Network security (cryptography, public key infrastructures, wireless networks, change management, privilege management, etc).

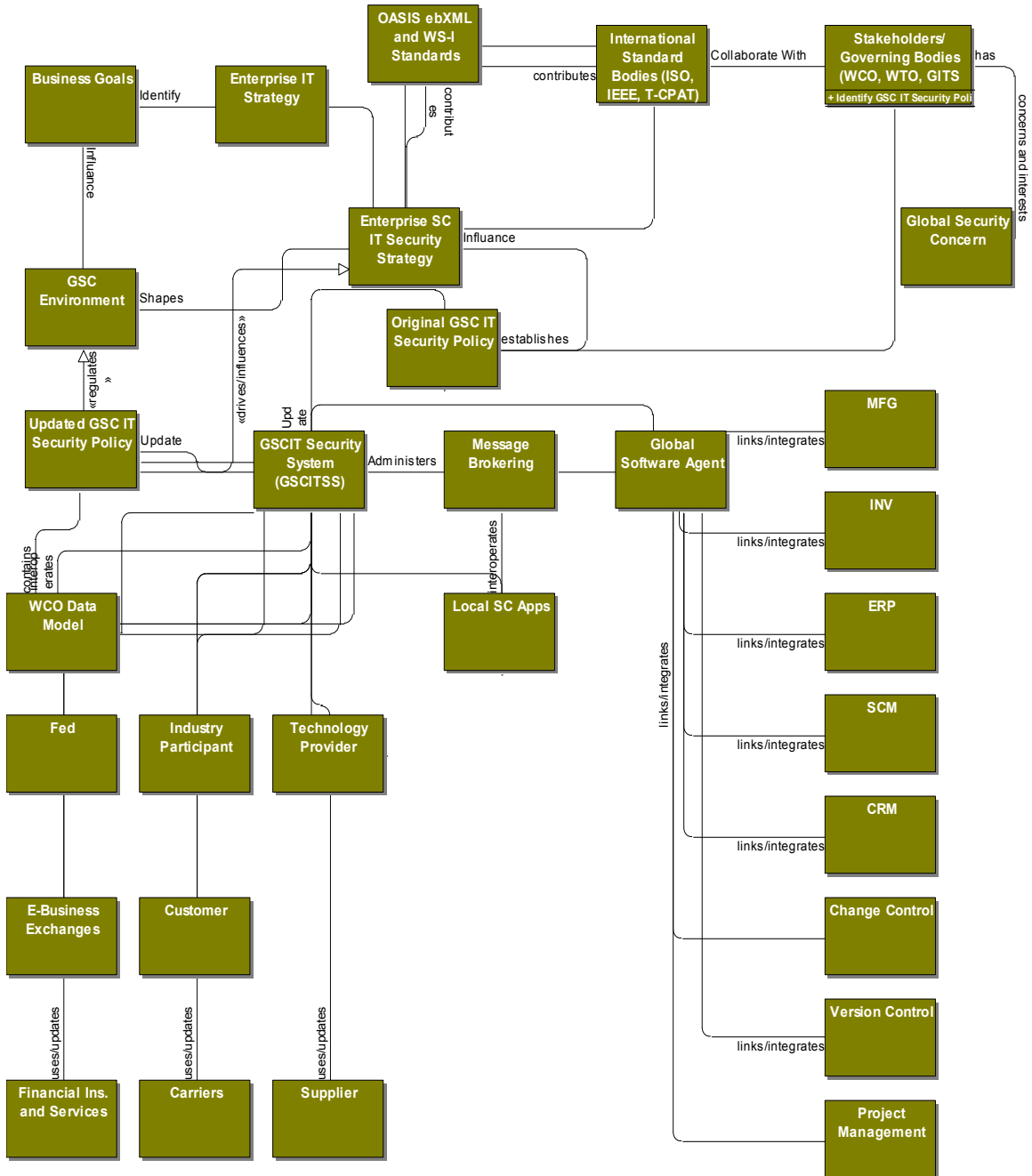


Figure 4-13: Refined Conceptual Solution

4.7.1 *Refined Conceptual Solution: Data Transportation*

The meta-model shown in Figure 4-13 is a static model showing Meta primitives and their relationships with regards to the GSC IT Security System. However, the dynamics of the logical implementation of the conceptual solution are shown in Figure 4-14. While the diagram shows data exchange between an OEM and a Tier-1 supplier, it could also show collaboration between any two or more industry participants. The mechanisms for the activities in Figure 4-15 operate as follows:

1. Suppliers can connect to the Global Supply Chain IT Security System (GSCITSS) server using a variety of methods. GSCITSS will supply the necessary authentication to enable data transaction security and collaboration. **To minimize disruption to enterprise ongoing operations, trading partners may connect to GSCITSS via a third party such as Covisint, Sterling Commerce, or any other established hub-centric type service, e.g. i-Connect.**
2. Transaction Data is securely transported from the Supplier to GSCITSS, mirrored in several locations across the globe. Transactions are validated for global policy compliance, encrypted, packaged, and ready to forward to an OEM or Industry Participant.
3. Transaction Data travels securely from the GSCITSS server to the OEM (or other IP) production server, still compliant, encrypted, and packaged. The OEM server transports periodically (every 10 minutes) transaction data to/from GSCITSS server.
4. Transaction Data travels securely from the OEM or industry participant (IP) production server to the OEM/IP Data Managers. The secure data is then routed to an OEM or IP user a specific pre-destined OEM/IP location.
5. The entire process can initiated from either end. Transaction traceability is always available to both ends.

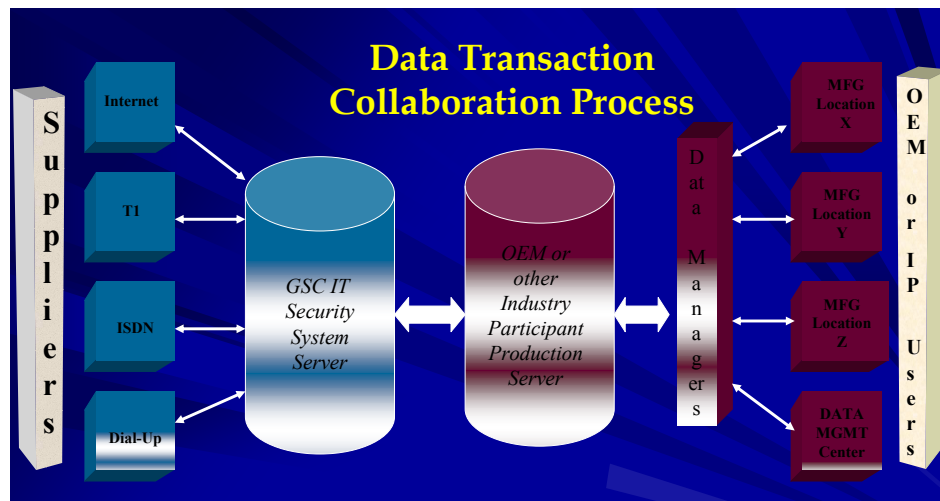


Figure 4-14: Data Transaction Collaboration Process

4.7.2 Conceptual Solution: Security Infrastructure Model

The implementation of any technology in any situation must be reliable, such that consumers, enterprises, governments, and all other trading partners and industry participants and their authorized users have the ability to access the information and services they need when they need it.

Although these service reliability issues may seem obvious, other corner-cutting issues such as limited funds, competing priorities, and scarce resources add a new dimension to the problem.

Additionally, knowing the financial potential of the conceptual solution and its Global IT Security Policy in the delivery of compliantly secure exchange of information will support the applications and potential traffic. The industry participants' acceptance and, ultimately, their actual use of the technology within the automotive industry enterprises will promote the technical infrastructure and support the data exchange applications.

Implementing conceptual solution security infrastructure is a significant undertaking, involving many stakeholders and requiring commitment from many players in both government and business. It is essential, therefore, that a *systematic approach* be adopted from the outset, as the hypothesis suggests. The systematic approach should include a process model showing the steps necessary to implement the system and a methodology that describes such an implementation.

Figure 4-15 shows the security infrastructure of a typical implementation of the conceptual solution. At a minimum, the infrastructure should have the appropriate networking installations in place with appropriate bandwidth to transport the data. A sufficient number of web servers should be installed and

configured to run the GSCITSS and to house the GSC IT Security Policy. Additional servers include firewalls, balance load servers, system auditing servers, and proxy servers.

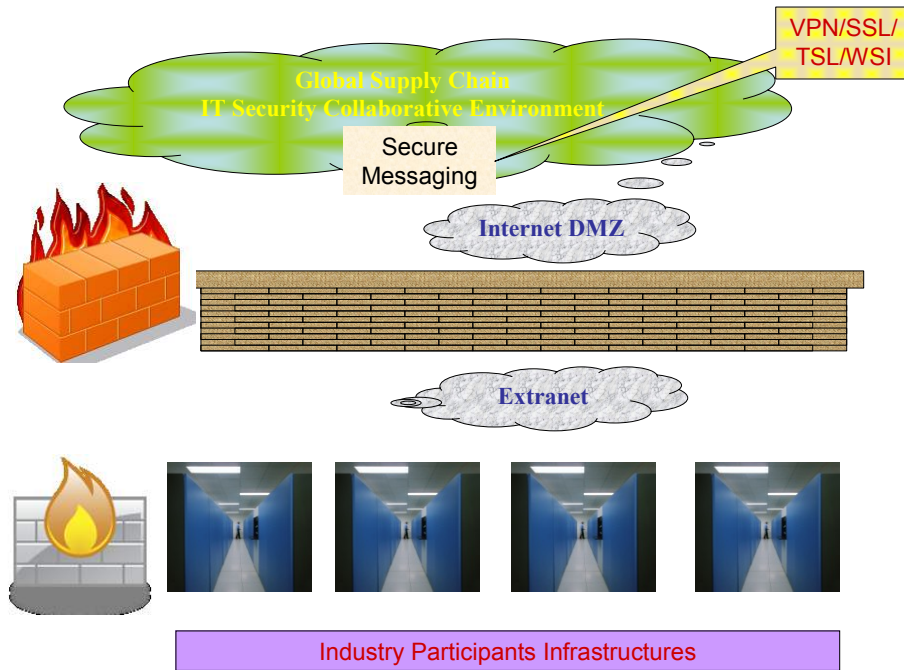


Figure 4-15: Conceptual Solution: Security Infrastructure Model

4.8 Systematic Approach for the Conceptual Solution

The “systematic approach” to data exchange is a key phrase of the hypothesis of this research. In essence, the hypothesis states that if the industry trading partners *adopt* this systematic approach, then the overall security of the GSC

could be improved. The systematic approach comprises of a *process model* and a project implementation *methodology*.

4.8.1 Systematic Approach: Process Model

For presentation purposes, the systematic approach process model is presented in two formats: 1) a simple organizational format developed as a PowerPoint™ diagram, and 2) a holistically defined business process modeled in ProVision™.

GSC IT Security Systematic Approach Process Model

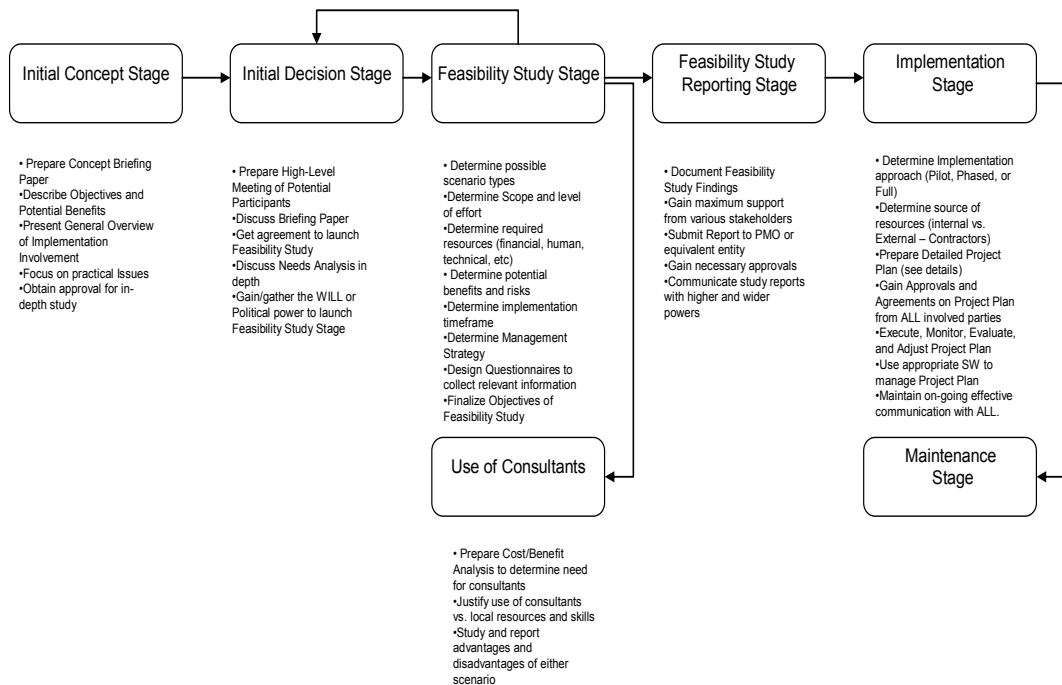


Figure 4-16: Systematic Approach Process Model Organizational Form

The organizational process model is shown in Figure 4-16. It is self explanatory. It does not contain any coding scheme. It is only intended to provide a high-level overview of the main steps necessary for an implementation of the conceptual solution.

The process model for the systematic approach was modeled in Provision™ and is depicted in Figure 4-17. It is coded into 7 stages. Each stage of the process model represents a level.

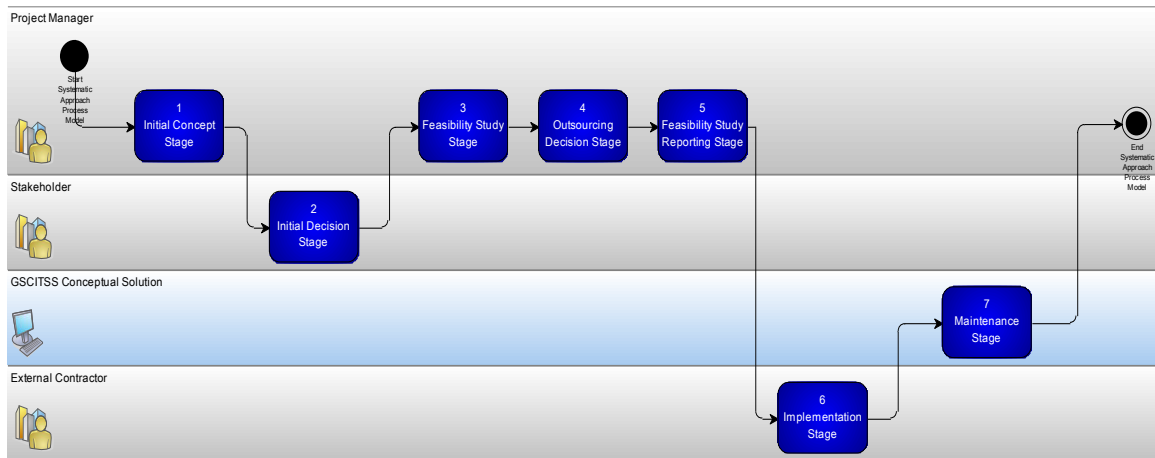


Figure 4-17: Systematic Approach Process Model Top Level

The systematic approach process model (7 stages) along with the details of each stage is shown in Figure 4-18.

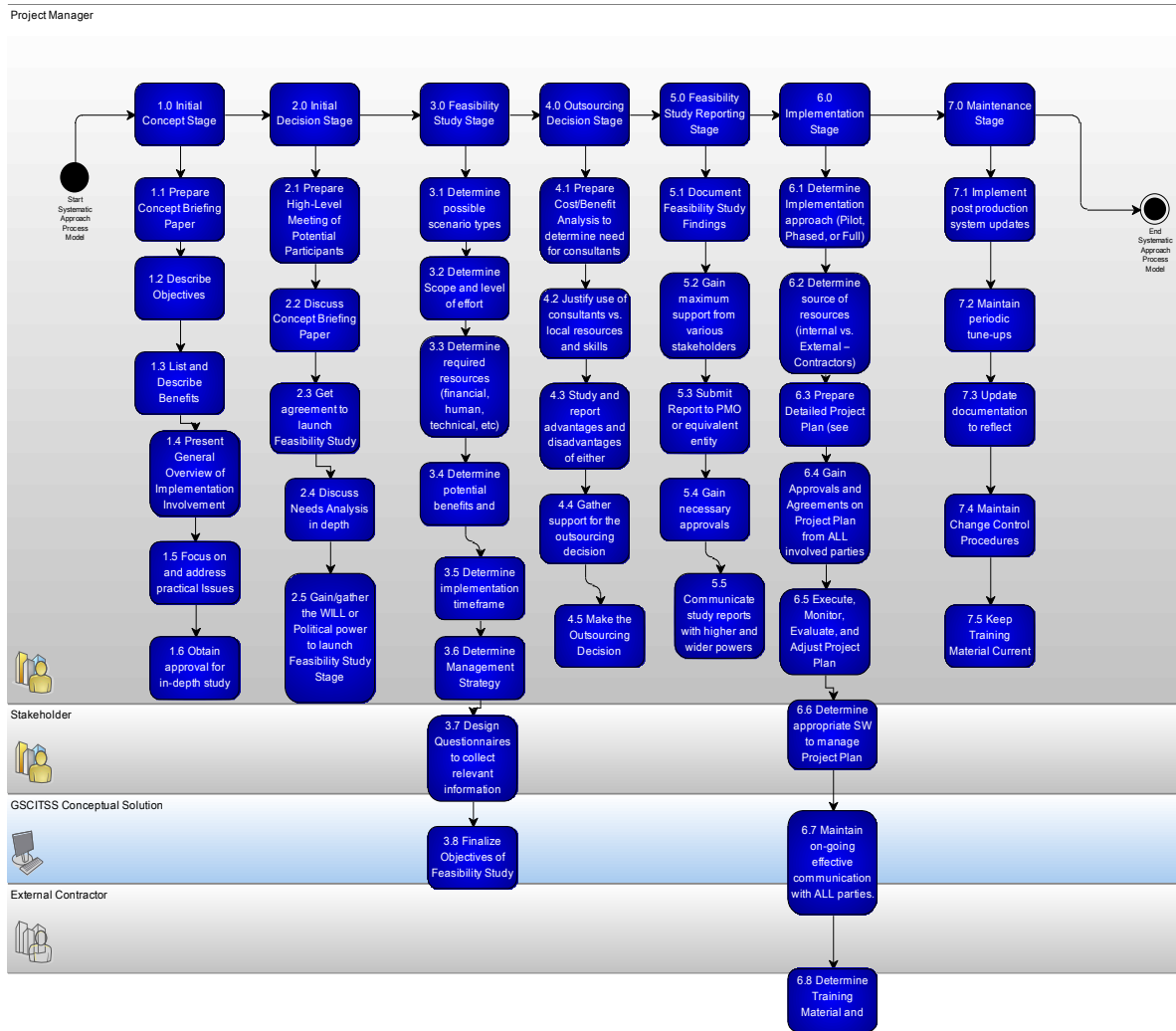


Figure 4-18: GSCITSS Systematic Approach Process Model

The next level of the systematic approach process model is Initial Concept Stage.

It is shown in Figure 4-19.

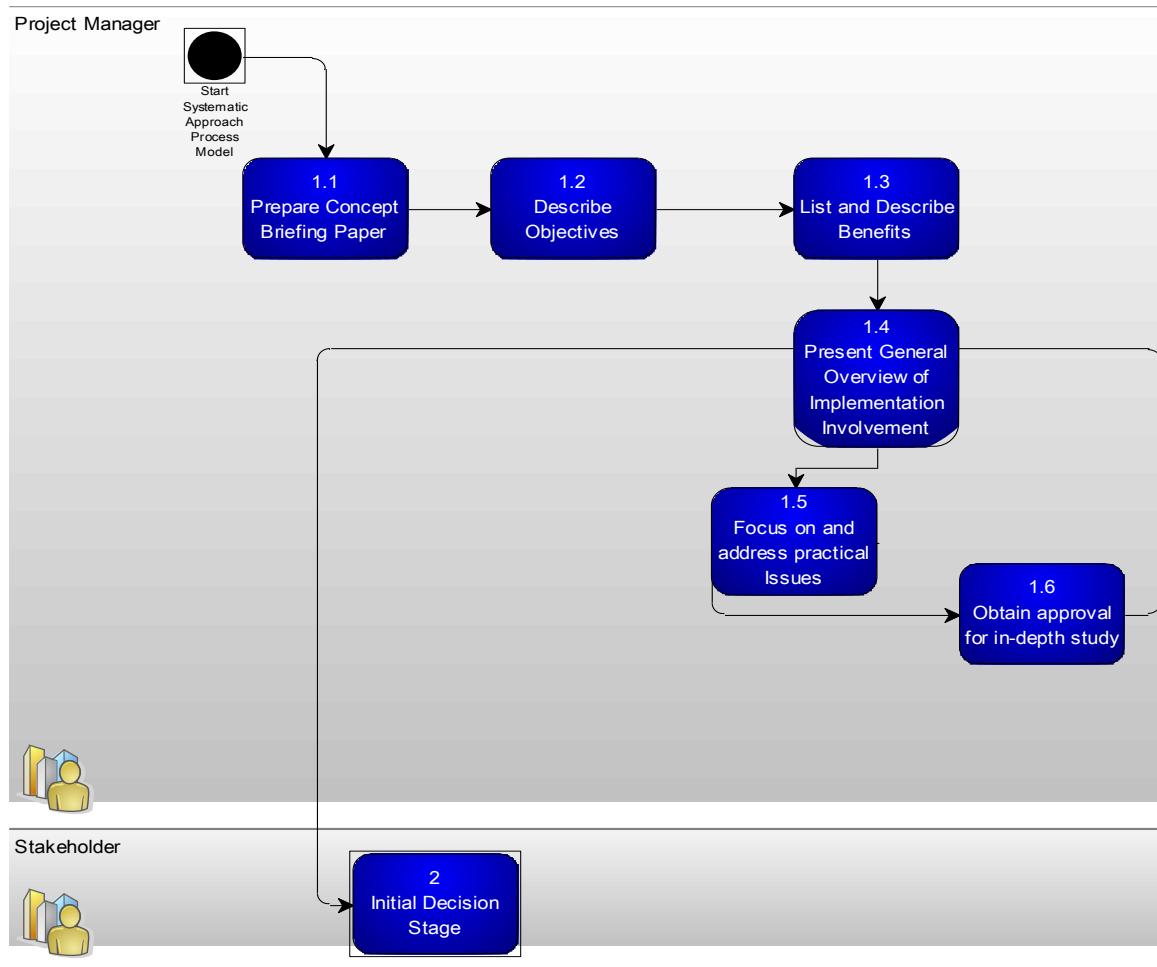


Figure 4-19: Process Model: Initial Concept Stage

For the interest of preserving limited space, the remainders of the Systematic Approach Process Model levels (Stages 2.1 to 7.5) are found in **Appendix B**.

4.8.2 Systematic Approach: Methodology

This systematic approach project implementation methodology consists of the steps that were outlined in the process model. These steps are also known as

activity usages. The GSCITSS Systematic Approach Process Model includes seven activity usages:

1. Initial Concept Stage
2. Initial Decision Stage
3. Feasibility Study Stage
4. Outsourcing Decision Stage
5. Feasibility Study Reporting Stage
6. Implementation Stage
7. Maintenance Stage

The details of each stage are outlined in Sections 4.8.2.1 to 4.8.2.7. However, for the interest of limited space, the details of each sub-stage activity usage are found in **Appendix B**.

4.8.2.1 Initial Concept Stage

The Initial Concept Stage is the responsibility of the Project Manager. It includes six activity usages:

1. Prepare Concept Briefing Paper
2. Describe Objectives
3. List and Describe Benefits
4. Present General Overview of Implementation Involvement
5. Focus on and address practical Issues
6. Obtain approval for in-depth study

It accepts workflow from “Start Systematic Approach Process Model” as a source, and delivers workflow to Activity Usage “2 Initial Decision Stage”.

4.8.2.2 *Initial Decision Stage*

The Initial Design Stage is the responsibility of the Stakeholder. It includes five activity usages:

- 2.1 Prepare High-Level Meeting of Potential Participants
 - 2.2 Discuss Concept Briefing Paper
 - 2.3 Get agreement to launch Feasibility Study
 - 2.4 Discuss Needs Analysis in depth
 - 2.5 Gain/gather the WILL or Political power to launch Feasibility Study Stage
- It accepts workflow from Activity Usage “1 Initial Concept Stage” as a source, and delivers workflow to Activity Usage “3 Feasibility Study Stage”.

4.8.2.3 *Feasibility Study Stage*

The Feasibility Study Stage is the responsibility of the Project Manager. It includes eight activity usages:

- 3.1 Determine possible scenario types
 - 3.2 Determine Scope and level of effort
 - 3.3 Determine required resources (financial, human, technical, etc)
 - 3.4 Determine potential benefits and risks
 - 3.5 Determine implementation timeframe
 - 3.6 Determine Management Strategy
 - 3.7 Design Questionnaires to collect relevant information
 - 3.8 Finalize Objectives of Feasibility Study
- It accepts workflow from Activity Usage “2 Initial Decision Stage” as a source, and delivers workflow to Activity Usage “4 Outsourcing Decision Stage”.

4.8.2.4 Outsourcing Decision Stage

The Outsourcing Decision Stage is the responsibility of the Project Manager. It includes five activity usages:

- 4.1 Prepare Cost/Benefit Analysis to determine need for consultants
- 4.2 Justify use of consultants vs. local resources and skills
- 4.3 Study and report advantages and disadvantages of either scenario
- 4.4 Make the Outsourcing Decision
- 4.5 Gather support for the outsourcing decision

It accepts workflow from Activity Usage “3 Feasibility Study Stage” as a source, and delivers workflow to Activity Usage “5 Feasibility Study Reporting Stage”.

4.8.2.5 Feasibility Study Reporting Stage

The Feasibility Study Reporting Stage is the responsibility of the Project Manager. It includes five activity usages:

- 5.1 Document Feasibility Study Findings
- 5.2 Gain maximum support from various stakeholders
- 5.3 Submit Report to PMO or equivalent entity
- 5.4 Gain necessary approvals
- 5.5 Communicate study reports with higher and wider powers

It accepts workflow from Activity Usage “4 Outsourcing Decision Stage” as a source, and delivers workflow to Activity Usage “6 Implementation Stage”.

4.8.2.6 *Implementation Stage*

The Implementation Stage is the responsibility of External Contractor (assuming that the decision was made to outsource). It includes eight activity usages:

- 6.1 Determine Implementation approach (Pilot, Phased, or Full)
- 6.2 Determine source of resources (internal vs. External – Contractors)
- 6.3 Prepare Detailed Project Plan (see details)
- 6.4 Gain Approvals and Agreements on Project Plan from ALL involved parties
- 6.5 Execute, Monitor, Evaluate, and Adjust Project Plan
- 6.6 Determine appropriate SW to manage Project Plan
- 6.7 Maintain on-going effective communication with ALL parties.
- 6.8 Determine Training Material and Schedules

It accepts workflow from Activity Usage “5 Feasibility Study Reporting Stage” as a source, and delivers workflow to Activity Usage “7 Maintenance Stage”.

4.8.2.7 *Maintenance Stage*

The Maintenance Stage is the responsibility of the System administrators (GSCITSS Conceptual Solution). It includes five activity usages:

- 7.1 Implement post production system updates
- 7.2 Maintain periodic tune-ups
- 7.3 Update documentation to reflect changes
- 7.4 Maintain Change Control Procedures
- 7.5 Keep Training Material Current

It accepts workflow from Activity Usage “6 Implementation Stage” as a source, and delivers workflow to the *Sink Point* “End Systematic Approach Process Model/Methodology”.

4.9 Summary and Conclusion

Chapter 4 is a key component of this research. It presents the key deliverables of the research project in terms of the systematic approach process model and methodology. The draft (initial) conceptual solution is discussed and a meta-model consisting of the components that make up the solution is presented. The research analysis is described and the output used to refine the conceptual solution. The research analysis process involved compiling the collected data from the interviews and the questionnaire, and observations and conclusions emanating from this process are presented. The analysis performed on the raw data of the questionnaire, and the review of the interview data enabled conclusions to be drawn regarding the relationships among IT Security and various business areas such as governance, quality, integration, procurement, and compliance. Most of the findings from the questionnaire are supported by the actual feedback collected from the interviews. The interviews served to be a very valuable research technique.

This chapter also includes details about the *systematic approach* to implement the conceptual solution in a real-world enterprise. The majority of the models and diagrams produced by following the proposed systematic approach, as well

as the implementation methodology can be found in Appendix B. The main conclusion obtained from the research deliverables reported in this chapter supports the hypothesis of this research. That is, by adopting the **Systematic Approach**, any given organization will be able to implement the proposed conceptual solution of this research. The application of this Systematic Approach is described in Chapter 5 – Demonstration of Concept for the purpose of showing a “how to” process for implementing the conceptual solution.

CHAPTER 5 DEMONSTRATION OF CONCEPT

5.1 Introduction

This chapter illustrates how the conceptual solution could be implemented in a real life situation, for any given enterprise within the GSC automotive industry. This is known as the “demonstration of concept” and is one of the techniques used to validate the conceptual solution. The concept is illustrated by applying the systematic approach discussed in Chapter 4 (the process model and the methodology, and the artifacts that are produced during implementation) and show how the conceptual solution could be implemented and effectively work in any given enterprise. The demonstration of concept represents the approach followed in this research project to implement a GSC system in a representative automotive company.

To demonstrate the conceptual solution of a Global Supply Chain IT Security System (GSCITSS), much effort has been spent in gathering meaningful data from resources ranging from the front of the line technical experts, all the way up to the C-level strategic leaderships of IT and the automotive, governmental, and international GSC organizations.

To facilitate the demonstration of a *systematic approach* an **implementation scenario is used**, which is representative of a fictitious automotive company in North America. The name “Global Motors Corp – GMC” is given to this company for modeling and implementation purposes.

Chapter 5 is structured as follows: an overview, the validation criteria and the technology selection criteria are presented first. The criteria were selected as foundation for the technology used in implementing the demonstration of concept. Next, the implementation model is described in terms of a conceptual solution for the **GMC USA Model**. The description of the GMC USA implementation in terms of the execution of the steps and activities of the *systematic approach methodology* provides the reader with a clear understanding of how the concept is demonstrated.

Key success factors of the implementation are discussed, including additional structures, procedures, and models that are needed in order to support the implementation. The chapter ends with a summary and conclusion.

5.2 Overview

As mentioned in Section 5.1, there are several implementation models in which a deployment of the conceptual solution could be implemented. This chapter discusses USA-based implementation. However, two other models representing implementations in Europe or other parts of the world are briefly discussed as additional support for the approach. The real-world implementations are supported with Provision™ models, presented in **Appendix B**.

In this research, it was established early on that the most pragmatic validation for the conceptual solution would be based on interviewing real-world IT professionals from junior supply chain experts to senior level executives. However, in order to confirm support for the conceptual solution a demonstration of an implementation based on a real world scenario is also given. The validation of the demonstration of concept relies on pre-determined evaluation criteria presented next.

5.3 Demonstration of Concept Validation Criteria

During the interviews, the key question asked by the researcher and used as a benchmark for unbiased support for the conceptual solution was:

“If you see value in this conceptual solution, would you be willing to partially fund a small implementation?”

If the answer was “yes”, then one concluded that such willingness to support the implementation of the conceptual solution validated the concept. This also implies that the GSC IT Security executive is willing to consider funding an implementation of the conceptual solution, and actively participate in it from a cost/benefit point of view. IT Budget dollars have been tight for the last five years, and it has become increasingly difficult to obtain additional IT Funds. Of course, each interviewee was given the freedom to view the applicability of the conceptual solution from their own perspectives and based on their own needs and objectives. The criteria for validating the conceptual solution (reduce IT transaction cost, reduce IT transaction time, and improve the quality of service for the IT transaction) were also used to evaluate the demonstration of concept.

5.4 Technology Selection Criteria

The demonstration of concept validation criteria, discussed in Section 5.3., include criteria of technology selection. However, in order to effectively implement the conceptual solution in a real-world situation, similar criteria of technology selection must be held to the same standard. A survey of available

technologies was done based on established Technology Selection Criteria. This ensured adherence to proven design principles and appropriate evaluation of the final product of this dissertation. Table 5-1 contains the technology selection criteria that were identified.

	<i>Current Technology</i>	State-of-the-Art Technology
Forecasting	What are current technologies for collecting, maintaining, and developing forecasts?	How are the best firms developing forecasts?
Order Entry	What order entry technologies are currently used? What order entry technology are customers requiring?	How are the best firms performing order entry? What new technologies are available to improve order entry effectiveness?
Order Processing	What is the process to allocate available inventory to customer orders? What are the limitations of the current approach to order processing?	How are the best firms performing order processing? What new technologies (HW and SW) are available to improve order processing effectiveness?
<i>Requirements Planning</i>	<i>What decision processes are used to determine production and distribution inventory requirements? How are these processes supported with current information and decision aids?</i>	<i>How are the best firms making production and inventory planning decisions? What new technologies are available to improve requirements planning effectiveness?</i>
Invoicing and EDI	How are invoices, inquiries, advanced shipment notifications, and payments currently transmitted?	How are the best firms using EDI? What new communications and data exchange technologies are available to improve invoicing and other forms of customer communication?
Warehouse	How are warehouse personnel	How are the best firms using

	<i>Current Technology</i>	State-of-the-Art Technology
Operations	and scheduling decisions made? How are warehousing operating instructions provided to supervisors and material handlers? How do warehouse supervisors and material handlers track activities and performance?	information and materials handling technologies in the warehouse? What new information and materials handling technologies are available to improve warehouse operating effectiveness?
Transportation	How are transportation consolidation, routing, and scheduling decisions made? How is transportation documentation developed and communicated with carriers and customers? How are transportation costs determined, assessed, and monitored? What packaging and loading technologies are used?	How are the best firms using information, packaging, and loading technologies with carriers? What new information, packaging, loading, and communication technologies are available to improve transportation operating effectiveness?
<i>Decision Support</i>	<i>How are logistical, tactical, and strategic planning decisions made? What information is used and what analysis is completed?</i>	<i>How are the best companies making similar tactical or strategic decisions? What information and evaluation technologies are available to enhance decision making effectiveness?</i>
Global Networking	How are the communications and networking decisions made? How is capacity planning (bandwidth, etc) for networking performed?	How are the best companies implementing global networks? What technologies are available that can improve the performance of networks and reduce the costs?
Infrastructure	How are infrastructure (servers, data centers, etc) decisions made? What	How do the best companies implement infrastructure effectively? What technologies

	<i>Current Technology</i>	State-of-the-Art Technology
Security Software	<p>infrastructure assessment techniques are available?</p> <p>How are IT security decisions made? What are the IT security policies or regulations available?</p> <p>What security controls and measures are implanted and effective?</p>	<p>are available to help assess the state of the infrastructure and stabilize or improve it?</p> <p>How do best firms make IT security decisions? What technologies are available that could enforce IT security policies? What technologies are available to improve IT security?</p>
Compliance SW	<p>How are the decisions for trade compliance made? What are the compliance procedures and controls in place?</p> <p>What technologies are used in automating the compliance process?</p>	<p>How do best firms make compliance decisions? What technologies are available that could expedite the compliance process? What technologies are available to promote trade compliance and reduce its cost?</p>

Table 5-1: Technology Assessment Selection Criteria

5.5 Global Motors Corp USA Business Case

The Conceptual Solution (here called the GSCITSS) can provide a wide variety of services and facilities depending on its design and coverage. For example, the GMC USA system – GSCITSS is capable of enabling any two or more trading partners within the automotive industry to trade securely and efficiently. The system can also enable USA Tier 1 suppliers to pre-qualify 3rd world country SME’s in terms of WCO trade compliance.

5.5.1 *Implementation Model*

The GSCITSS in any central location (ex: USA, UK, Australia, etc) allows the submission of customs declarations, their processing and their return by electronic means through a subset of the conceptual solution, which is simply a **data exchange system**. The system can accept EDI-based, ebXML-based, or WSI-based messages. It is a **network application** that allows the electronic transmission of documents between various parties involved in the movement of import and export goods, namely the Customs & Excise Department, Freight Forwarders, Shipping Agents, Customs Brokers, the Cargo Handling Corporation, and the Department of Commerce, Operators within the Freeport, and Importers and Exporters. Banks could also be connected to the data exchange system to allow for the electronic payment of duties and taxes via an Automated Clearing House (ACH) and/or Automated Clearing Settlement System (ACSS) of the Bank of their choice.

The details of this implementation model (ProVision™ Models) for the GMC USA Company can be found in **APPENDIX B GMC USA Implementation Model ProVision Details**. The three models provided below serve as

demonstration of the concept with real-world systems that are operating effectively today.

Finally, by following the Systematic Approach, discussed in Chapter 4, Section 4.8.2, the GMC USA deployment could be effectively achieved.

5.5.1.1 USA Model

The GMC USA GSCITSS is a real-world solution with the vision to use a *secure, integrated automotive industry to government trading system*. It offers a common hub for the private sector to meet with Customs organizations for the electronic collection, use, and dissemination of standard trade and transportation data. It can be easily integrated with or installed on top of an existing UN Single Window Facilitation (Known in the US as ITDS). It has the capability to automatically update the GSCITSS GSC IT Security Policy in the same manner it updates the exchange rates. The system includes all trade-related regulations and can provide traders with automated updates on changes via Internet and/or SMS-services. In order to be able to give the other enforcement agencies the relevant information they need to perform their tasks, these agencies provide Customs with *risk-profiles* on the basis of which Customs analyzes the

information and passes it on, either electronically to the other agencies. In rare cases, the information is exchanged on paper. The other agencies inform Customs in return if they want to check the goods. If more than one agency (including Customs) wants to check the goods, the GSCITSS co-ordinates the checks of all the agencies involved. The aim is to prevent multiple checks that will unnecessarily disrupt the logistical process.

5.5.1.2 European Models

There are two European Single Window installations that could be used as models for implementing the conceptual solution in Europe and other global locations. They are 1) The Swedish Single Window system, known as “The Virtual Customs Office” (VCO), and the VIPPROG system, at Schiphol International Airport. Both of these systems allow for electronic Customs declarations and application for import and export licenses and licenses for strategic products. The two systems can be integrated into the industry participants business system (ex: ERP and/or SCM), and can automatically update changes in exchange rates, tariff codes and duty rates. They both have the capability to automatically update the GSCITSS’ GSC IT Security Policy in the same manner it updates the exchange rates. The Single Window also includes all

trade-related regulations and can provide traders with automated updates on changes via Internet and/or SMS-services. The VCO also offers interactive training courses and possibility to customize and create personal virtual customs offices, which contain all information and processes that each trader uses and finds relevant to its needs and wants.

5.6 Implementing GMC USA using the Systematic Approach

One of the most important steps in the demonstration of concept is the ability to exhibit how a typical implementation of the conceptual solution in a real world scenario could be executed using the steps of the seven stages of the systematic methodology to the GMC USA Company as follows below.

5.6.1 Initial Concept Stage

In the Initial Concept Stage, the GMC USA GSCITSS Project Manager prepares a “Concept Briefing Paper” to be submitted to the stakeholders. The concept briefing paper describes the objectives of the GSCITSS implantation, lists and describes the benefits of implementing the GSCITSS, and presents a general overview of implementation involvement. The concept briefing paper also focuses on practical Issues and addresses any area that may seem obscure. The final step in this stage is for the PM to obtain approval for in-depth study to

further determine the feasibility of the implementation. This stage passes the approval process over to the next stage, the Initial Decision Stage.

5.6.2 Initial Decision Stage

Now that approval for further study has been obtained, the Initial Design Stage requires Stakeholder to prepare a high-level meeting of potential participants in order to discuss the concept briefing paper which was developed in the previous stage. The objective at this point is to get agreement to launch a Feasibility Study and to discuss and analyze the needs of the GMC organization in depth. It is important that at this stage the stakeholders gain or gather the political clout to launch Feasibility Study Stage, which comes next.

5.6.3 Feasibility Study Stage

The Feasibility Study Stage is one of the most important stages in the implementation process for GMC, as it will determine several key issues regarding the GMC GSCITSS implementation. During this stage, the PM along with various IT and management support, determine possible scenario types for the implementation. In addition, the scope and level of effort are also determined during this stage. The PM also needs to determine the required resources (financial, human, technical, etc), and the potential benefits and risks. An

implementation timeframe should be determined along with the management strategy for carrying out the implementation in a manner that aligns with GMC's business objectives (refer Appendix B). Finally, if necessary, Questionnaires are designed to collect relevant information. The last step in this stage is for the PM and stakeholders to finalize the objectives of the Feasibility Study.

5.6.4 Outsourcing Decision Stage

As with any IT implementation methodology, a decision regarding outsourcing must be made, and this systematic approach methodology is no different. In some cases, the Outsourcing Decision is the responsibility of the PM while in others it lies on the shoulders of the stakeholders. Regardless of who makes the decision, a Cost/Benefit Analysis is needed to determine need for consultants. The use of consultants vs. local resources and skills must be justified. The decision maker must study and report the advantages and disadvantages of either scenario, then make the Outsourcing Decision. The final step is to gather support for the outsourcing decision.

5.6.5 Feasibility Study Reporting Stage

The Feasibility Study Reporting Stage documents the Feasibility Study Findings. During this stage the PM must strive to gain maximum support from various

stakeholders. The generated Feasibility Study Findings report must be submitted to a Program Management Office (PMO) or equivalent entity to gain necessary approvals. The PM should communicate the study reports with higher and wider powers in the GMC organization.

5.6.6 Implementation Stage

The Implementation Stage is where the systematic approach is best manifested. During this stage, the GMC USA Company will (assuming that the decision was made to outsource) determine the implementation approach (ex: will the company implement a Pilot, a Phased, or a Full implementation). Next, the management of GMC USA must determine the source of resources needed to implement the GSCITSS (internal GMC employees vs. External Contractors).

The PM must prepare a Detailed Project Plan as follows:

1. A clear statement of the project's scope, goals and objectives (refer Appendix B).
2. A statement on key deliverables, responsibility for delivery, time frame and milestones for completion
3. Definition of the roles and responsibilities of the various participants, including a clear agreement on who is in charge of the project (the project manager) and the level of authority of this manager
4. Specification of the management and monitoring responsibilities of the project manager and the line of authority and communication between the project manager, Project Management Group and any Task Force
5. A clear strategy for communicating with project stakeholders and potential users on a regular basis throughout the implementation, including an agreement on what information needs to be communicated with what groups and in what manner and frequency.

6. A clear and agreed project budget, including financial and human resources. It is essential that the necessary funds and personnel be allocated to the project from the outset.
7. A clear statement of the project risks (such as a cutback in budget, delay in required legal reforms, etc.) and an agreed response plan (to the best extent possible) to manage these risks, including contingency plans for high-level risks.
8. Agreement on the criteria for measuring the project success.
9. An agreed project review and feedback mechanism to provide ongoing monitoring of the project process and to deal with any changes in the implementation that may be required.

Once the project management plan is in place, then the PM must gain approvals and agreements on project plan from all involved parties. As the implementation efforts begin, the PM (on weekly basis) must execute, monitor, evaluate, and adjust the Project Plan. In addition, the PM should determine the appropriate software application that helps with the management of the Project Plan.

Finally, training and communication must be promoted. The PM should maintain on-going and effective communication with ALL parties, and determine training material and schedules.

5.6.7 Maintenance Stage

The last stage in the systematic approach methodology is the Maintenance Stage, where the GMC GSCITSS system administrators implement post production system updates, maintain periodic tune-ups, update the system documentation

to reflect any changes made, maintain Change Control Procedures, and keep the training material current.

This is the end of the implementation of the GSCITSS for GMC USA Company applying the proposed systematic methodology.

5.6.8 Key Factors In Establishing a Successful GSCITSS

As Section 5.5 demonstrated, the implementation of the conceptual solution is a well-structured process. However, no implementation could be considered successful without serious consideration of some key factors that revolve around the implementation. Therefore, the successful implementation of a GSCITSS depends to a considerable extent on certain pre-conditions and success factors that vary from country to country and from project to project. This section lists some of the success factors.

5.6.8.1 Political Will

The existence of strong political will on the part of **both** government and business to implement a GSCITSS is one of the most critical factors for its successful implementation. Achieving this political will requires proper dissemination of clear and impartial information on objectives, implications,

benefits and possible obstacles in the establishment of the GSCITSS. The availability of resources to establish a GSCITSS is often directly related to the level of political will and commitment to the project. Establishing the necessary political will is the foundation stone upon which all the other success factors have to rest.

5.6.8.2 Establishment of Clear Project Boundaries and Objectives

Establishing clearly defined goals and objectives at the outset helps guide the project through its various development stages. These should be based on a careful analysis of the needs, aspirations and resources of the key stakeholders, and on the existing infrastructure and current approaches to the submission of trade-related data to government. This analysis should involve all key stakeholders from both government and trade. A GSCITSS should generally be perceived as part of a country's overall strategy to improve trade facilitation.

5.6.8.3 Partnership between Government and Trade

A GSCITSS is a practical model for cooperation between agencies within government and also between government and the industry participants. It presents a good opportunity for a public-private partnership in the establishment

and operation of the GSCIT Security system. Consequently, representatives from **all relevant public and private sector agencies** should participate in the development of the system from the outset. This should include participation in all stages of the project, from the initial development of project objectives, situational analysis, and project design through to implementation. The ultimate success of GSCITSS will depend critically on the involvement, commitment and readiness of these parties, to ensure that the system becomes a regular feature of their business process.

5.6.8.4 Communications Strategy

Establishing a proper mechanism for keeping all stakeholders informed on project goals, objectives, targets, progress, and challenging difficulties creates trust and avoids the type of misunderstanding that can lead to the undoing of an otherwise good project. Within this context, it is extremely important to handle stakeholders' expectations properly, and it is worth remembering the business adage of *promising less and delivering more, instead of the other way round*.

5.6.8.5 Strong Advocacy

The requirement of a strong, resourceful, and empowered lead organization is essential for the launch of the project and to see it through its various development stages. This organization must have the appropriate political support (both internal and external), legal authority, human and financial resources, and links with the business community. In addition, it is essential to have a strong individual within the organization who is considered the “project champion.”

5.6.8.6 User Friendliness and Accessibility

Two of the key factors for the success of a GSCITSS project are accessibility and user friendliness. Additionally, comprehensive operating instructions and guidelines should be created for users. Help Desk and user support services, including training, should be established, especially in the early implementation phase of the project. The Help Desk can be a useful means for collecting feedback information on areas of difficulty and bottlenecks in the system. This information can be a valuable tool further development of the GSCITSS. Effective training courses for users cannot be over-emphasized, especially in the early

implementation phase of the project. It is also important to address the multilingual requirements in some countries.

Finally, it is essential that the design of the system be attuned to the real IT capacities, capabilities, and infrastructure readiness of the country or region in which it will operate.

5.6.8.7 Legal Environment

Establishing the necessary legal environment is a pre-requisite for any GSCITSS implementation. Related laws and legal restrictions must be identified and carefully analyzed. For example, changes in legislation could be required sometimes in order to facilitate electronic data submission or exchange. Further, restrictions concerning the sharing of information among authorities and agencies, as well as organizational arrangements for the operation of a GSCITSS, may need to be overcome. As such, the legal issues involved in delegating power and authority to a lead agency needs to be examined.

5.6.8.8 International Standards and Recommendations

The implementation of a GSCITSS generally entails the harmonization and alignment of the relevant trade documents and data sets. In order to ensure

compatibility with other international systems and applications, these documents and data models must be based on international standards and recommendations. Whenever electronic data interchange is involved, the harmonization, simplification and standardization of all data used in international trade are an essential requirement for smooth automatic operation of the GSCITSS. Of course, there are several translation and mapping software applications, but they do not address this harmonization effectively. The harmonization of data used by different participants in their legacy system can be one of the biggest challenges for automated GSCITSS implementations. UN/CEFACT trade facilitation recommendations (such as UN/CEFACT Recommendations Number 1 and 18) contain valuable information for similar implementations of GSCITSS.

5.6.8.9 Identification of Possible Obstacles

It is possible that all industry participants and government personnel may not welcome the implementation of a GSCITSS. In such cases, the specific concerns of opponents should be identified and addressed as early as possible in the project. Identified obstacles should be considered individually, taking into account the local situation and requirements.

Clearly, cost can be a major obstacle but this must be balanced against future benefits as described in Section 1.7. However, it is important to be clear about the financial implications of the project so that the decision regarding full or phased implementation can be made. Legal issues also constitute a significant potential problem area.

5.6.8.10 Financial Model

A decision on the financial model for the GSCITSS should be reached as early as possible in the project. This could range from a system totally financed by government to an entirely self-sustainable model. Also, possibilities for public-private partnerships should be explored, if this is deemed a preferred approach. Clarity on this point can significantly influence decision-makers to support the implementation of the system.

5.6.8.11 Payment Possibility

A system for the payment of government fees, taxes, duties and other charges could be integrated with the GSCITSS. This can be a very attractive feature for both government and the Industry participants, and is especially important when the system is required to generate revenue. However, it should be noted

that adding payment features often requires a considerable amount of additional work with harmonization and especially IT security.

5.6.8.12 Promotion and Marketing

Promotion and marketing of a GSCITSS is very important and should be carefully planned. The promotion campaign should involve representatives from all the key Industry participants and their stakeholders in the system. These parties could yield valuable information on the expectations of the user community and help to direct the promotion and marketing messages.

A clear implementation timetable should be established and promoted at the earliest possible stage of a GSCITSS project, as this will assist in the marketing of the project and will help potential users to plan their related operations and investments according to this schedule. Marketing should clearly identify the benefits and cost savings as well as specific points relating to the increased efficiency derived from the implementation of GSCITSS operation.

5.7 Chapter Summary and Conclusion

Demonstration of concept is performed when a conceptual solution to a research problem is to be illustrated to show the feasibility of the solution. In any given research, applying the disciplines of well-grounded and proven research methods and approaches is essential to the soundness of the research. This chapter is summarized with the following key points:

- Implementing a systematic approach methodology based project has the potential to streamline operations, reduce inventories, shorten lead times, improve predictability, and enhance compliance and security.
- Knowledge of all partners in the GSC, including security processes and business models, is critical to managing effective IT Security properly.
- When applied correctly to the challenges of the GSC IT security issues, the conceptual solution can translate to measurable bottom line benefits to the national and local governments, industry enterprises and participants.
- Securing GSC electronic networks and the content being transported over the globally connected infrastructures demonstrates how improved IT security processes can create value across all the business functions throughout an entire value chain. A breach early in the chain can negate all of the measures that may be taken further downstream. The opposite also holds true: effective security in the beginning and middle stages of an electronic transaction can be rendered meaningless by a breach at the end.
- This research has supported and confirmed the hypothesis that adapting a systematic approach to data exchange and GSC IT security management philosophy.

CHAPTER 6 FINDINGS, CONCLUSIONS, AND CONTRIBUTIONS

While the results of this research should not be considered fully representative of the automotive industry, the findings discussed here clearly indicate that investing in GSC IT security yields significant business value. A reasonable conclusion from conducting this research is that the innovative GSC automotive industry participants who invest in GSC IT security research could easily receive the expected security benefits from their investments. These benefits include collaterals such as higher supply chain visibility, improved supply chain efficiency, better customer satisfaction, improved inventory management, reduced cycle time and shipping time; and cost reduction following these benefits.

The final chapter of this dissertation is devoted to findings, conclusions, limitations, and recommendations. The purpose of this chapter is to provide a discussion of the overall summary of the research. The chapter begins by discussing the findings relative to the hypothesis in terms of a number of issues that include findings relative to:

- Electronic Data Exchange.
- Trade Compliance.

- Best Practices.
- Situational Awareness.
- Training.
- Additional Findings.

This chapter continues by answering the research questions, and then links these answers to support and confirm the conclusions related to the hypothesis. Other conclusions are also discussed. A discussion regarding the summary of contributions made by conducting this research is explored, followed by a discussion of the limitations of this research. The final sections of this chapter discuss the recommendations this research yielded, and the need for additional future research.

6.1 Findings Relative to Hypothesis

GSC Industry participants traditionally find it hard to justify IT security-related investments because they focus largely on the direct expenses and not on the collateral benefits (ex: supply chain efficiency, improved customer satisfaction, improved inventory management, improved visibility, etc.) that may be realized. Limited research has been completed regarding the creation of collateral benefits from security investments. Upon collecting and analyzing the data, several categories of finding were obtained based on the interpretation of the collected

data. These hypothesis-related important findings brought forth a wealth of discoveries that were unidentified prior to this research. These include enablers and challengers that cover the gamut of electronic data exchange, best practices, situational awareness, training and additional findings.

The data collected from both the interviews and the questionnaires were essential to the successful completion of this research. Although the data population is somewhat limited (11 organizational interviews and 21 Industry participants), the opportunity of quantitative analysis was presented. Therefore, a portion of the overall data analysis for this research came from studying the responses that were collected during the interviews, and from various other times for the questionnaire answers.

6.1.1 Findings Relative to Electronic Data Exchange

The GSCITSS conceptual model was presented to the interviewees with the aim of securing GSC electronic data exchange. The GSCITSS is a partnership program involving all Industry participants. It aims to support and promote the electronic exchange of information through effective and secure systems and providing

access to high quality trade compliant SME's in 3rd world countries. The major findings, which are not ranked in any particular order, included the following:

- A significant number of paper-based transactional data sets still exist. The entire cycle of transactional data exchange is fragmented across a number of points within the GSC. Only in rare cases will one find a complete **global** electronic roundtrip of data exchange, especially when dealing with third world countries. The situation in North America and some parts of Europe is an exception to this finding.
- The GSCITSS is seen to be able to support and promote the IT security of electronic exchange of data. This is evidenced by the feedback from the interviews and questionnaires. The quality of data collected is also perceived to result in improvement.
- There is increased reliance on IT providers or other Industry participants' staff to provide support, training and guidance to GSCITSS users.
- The qualitative data from the interviews showed that there was a degree of confusion among USA Industry participants regarding the quality and readiness of data sets formats and requirements among 3rd world country SME's.
- There's been notable increase in tight data synchronization between Suppliers and OEM's in the USA in the last couple of years.
- There was a perception that GSCITSS could help to make data collection easier than previously, but that requests for data exchange have increased. So while the bureaucratic burden of data collection and provision is seen to have decreased, many respondents perceived workloads in relation to additional data collection and provision to have increased.
- The quantitative and qualitative data also showed that the bureaucratic burden on IT professionals has decreased.
- In terms of the effectiveness of the GSCITSS, key roles attributed were the collection, collation and dissemination of data. A notable proportion of IT executives were unable to attribute specific roles. Other stakeholders primarily viewed the GSCITSS as a tool for policy development and evaluation.
- Validations of the conceptual model for the GSCITSS were largely positive, especially in terms of its ability to increase the security of global data being exchanged.

- Notable proportions of respondents and interviewees were unable to comment constructively on the impact of the GSCITSS across a number of dimensions, such as its responsiveness to changing policy requirements. This was largely because respondents viewed the GSCITSS solely as a mechanism for the collation and provision of data.
- GSCITSS is perceived as a valuable tool that can be used for improving performance and identifying good practices for the security of globally exchanged data.
- This evaluation indicates that GSCITSS is achieving many of its objectives.

6.1.2 *Findings Relative to Trade Compliance*

In the early phases of conducting this research, the issue of trade compliance was not very high on the objectives list. However, shortly after embarking on the review of literature, it became apparent that trade compliance should play a significant role in the design of the conceptual solution. This is due to the rapid changes in the GSC laws and regulations, especially since the events of 9/11/2001.

The major trade compliance findings included the following:

- Most GSC IT executives in the USA would support a compliance verification system, such as the GSCITSS, in operation. Many believed that funding the implementation of a prototype will yield a positive ROI simply by eliminating much of the developing countries' trade compliance qualification costs.
- In an effort to support the Industry participants at a global level, the Trade Compliance Center (TCC) provides access to commercial and economic information to help U.S. exporters understand and evaluate opportunities created by trade agreements the United States has negotiated. The WTO Trade Policy Review Summaries are fully searchable market access reports with information on foreign trade policies and regulations. Links are also provided to the National Trade Estimate Report on Foreign Trade Barriers

- and to Country Market Research Library. The TCC also provides suppliers information on Global Procurement Opportunities (TCC, 2006).
- Since the WTO established the “Multilateral Agreements On Trade In Goods – Pre-shipment Inspection” in 1986, progress in achieving the objectives (articles) of the agreement has not been fully met in the following areas:
 - A number of developing country Members still doesn’t have adequate recourse to pre-shipment inspection.
 - The need of developing countries to verify the quality, quantity or price of imported goods in a reasonably timely manner has not been achieved.
 - Several WTO programs were delayed or did not get equal treatment among all developing world countries.
 - Although an agreed international framework of rights and obligations of both user members and exporter members was established, several advanced countries, especially the USA, did not fully comply. Instead, they dictated their own requirements to the exporter members.
 - Transparency of the operation of pre-shipment inspection entities and of laws and regulations relating to pre-shipment inspection were not always provided as stated by the Agreement.
 - Speedy, effective and equitable resolution of disputes between exporters and pre-shipment inspection entities arising under the Agreement were seldom attainable.
 - Although the USA has attempted to resolve problems with a pre-shipment inspection by providing the Trade Compliance Center's hotline, the ability of the U.S. Department of Commerce to resolve compliance problems was limited.
 - Bribery in some developing countries continues to cause compliance problems. The U.S. Secretary of Commerce is required by statute to provide an annual report to Congress on implementation of the Organization for Economic Cooperation and Development’s Convention on Combating Bribery of Foreign Public Officials in International Business Transactions (Anti-bribery Convention).

6.1.3 Findings Relative to Best Practices

When considering GSC information security technologies, hardware or software used to process the mechanisms of IT security is important but not enough. One must acknowledge that the security focus is placed on the assurance and security of the information as well. The underlying goal of IT security, especially within the dynamic automotive GSC, is to provide confidentiality, integrity, and availability - the “CIA” of security. The increased reliance on IT networks for e-commerce, authentication and non-repudiation highlights the need to adopt the CIA philosophy. According to the operational model of computer security, **protection** is provided by establishing *prevention, detection, and response*. Figure 6-1 illustrates this concept.

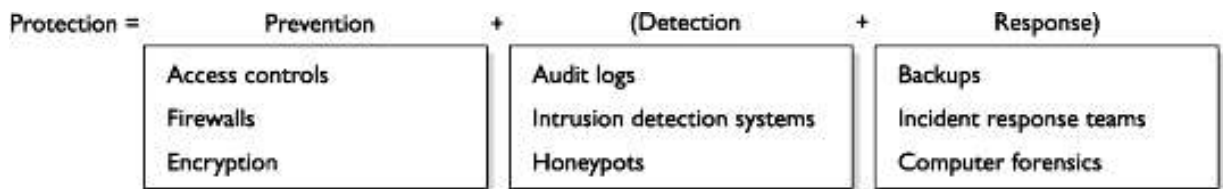


Figure 6-1: Information Security Operational Model

With this basic understanding of the CIA and security operational model, it was necessary to research the security practices of the most successful Industry participants within the GSC. The literature review coupled with the interviews and questionnaire revealed that what is considered as “best practices” by many

average performing companies is considered standard operating procedures (SOP) among the successful Industry participants. Therefore, the researcher deemed it necessary to reflect on how today's IT security best practices map to such the conceptual solution model - GSCITSS. The following findings summarize the GSC IT security best practices (Kakish and Steenkamp, 2005):

1. The best practice industry participant spends more on IT security. While the global spending averages is around 11% of the total IT budget, the average for the best practice Industry participants was 14%.
2. Best practice organizations separate information security from IT and then merge it with physical security. These disciplines can either exist under a single Computer Security Organization (CSO) or as separate entities governed by an executive security committee. The GSCITSS fits this mold properly with the administration of the GSC IT Security Policy.
3. Best practice Industry participants regularly conduct penetration tests to patch up network and application security. Best practice Industry participants are 60% more likely to do this than the average trading partner. These organizations also perform a complete security audit to identify threats to employees and intellectual property.
4. Best practice organizations create a comprehensive risk assessment process to classify and prioritize threats and vulnerabilities.
5. Best practice organizations define their overall security architecture and plan from the previous three steps.
6. Best practice organizations establish a quarterly review process, using metrics (for example, employee compliance rates) to measure their security's effectiveness. This helps to use the increased resources more efficiently.
7. The following best practices relate to technology. They were found to be common among some GSC trading partners:
 - Password Selection - create an effective and manageable password policy that can be used by system administrators and users. There are many tools available to help enforce the selection of strong, difficult passwords. Selecting passwords based on "pass phrases"

can be an easy and effective method of selecting a good password. Changing passwords frequently (say, every 60 to 90 days) is equally important.

- Operating System and Network Operating System Hardening - Securing operating systems among GSC Industry participants consisted of the following best practices:
 - Removing or disabling unnecessary services.
 - Restricting permissions on files and directories.
 - Removing unnecessary software (or not installing it in the first place),
 - Applying the latest patches
 - Removing unnecessary user accounts.
- Network Hardening - Securing network resources among best practices organizations consisted of the following: Disabling unnecessary functions, restricting access to ports and services, ensuring strong passwords are used, ensuring the code on the network devices is patched and updated, and controlling the types and amount of traffic allowed moving through network devices in order to ensure effective, secure operations.
- Application Hardening - Securing applications depends heavily on the application involved, and consists of removing samples and default materials, preventing reconnaissance attempts, and ensuring the software is patched and updated. Application patches should be tested before they are placed on a production system.

This research also looked ahead to future developments and "best practices" in the following strategic areas:

- Creating a framework for realizing a return on security investments by integrating it as a core business process.
- Details how the automotive industry GSC participants can measure and reward smart security practices.
- Globalization's impact on electronic GSC transportation networks.
- Establishing and maintaining a proven chain of custody – visibility, tracking, and monitoring the flow of data throughout the entire roundtrip within the GSC networks.
- Confirming and accepting the IT security practices which include, but are not limited to, the following:

- Knowing all that is needed to be known about the Industry participants in terms of their IT security policies and infrastructures.
- Verifying the credentials of all personnel involved in the movement of data across the GSC.
- Establishing and verifying controlled physical access to the Industry participants IT infrastructures and facilities.
- Being prepared to handle and respond to disasters, crisis, and catastrophes.

6.1.4 *Findings Relative to Situational Awareness*

Situational awareness for securing the exchange of data within the GSC should be focused on the information needed to track and trace the exchanged data from the point of origin to the point of destination. This should also include points and stations within the GSC where the exchanged electronic data takes on the form of paper-based data.

End-to-end information sharing in real time can improve the ability to monitor for anomalies and to improve processes. Needless to say, the amount of electronic data is very large, very complex, and is maintained in a variety of formats.

Findings relative to Situational Awareness included the following:

- By working toward the goal of optimizing network visibility into information about the location and condition of every shipment,

knowledge of the likely bottlenecks or “choke points”, and alternative sources of restoring the critical data, Industry participants can manage their assets better and allocate resources more efficiently.

- Being prepared to address important factors could solve a variety of short-term problems. These factors include:
- Knowing about other relevant data (EDI data, Customs data, backup data, etc) that can be brought into play.
 - Length of time customers could operate without having their goods.
 - Having backup procedures in place, ready to be invoked upon a trigger of something that might go wrong.
- Use of RFID tags can provide the means to capture and move the data with the shipment.
- Use of GPS tags allow for global tracking of goods, while real time information sharing and electronic container seals allow real-time monitoring of container security.
- In addition to the benefits of data security, the use of these technologies also enables Industry participants to monitor stocks and automatically generate re-orders.
- Inspection costs could be greatly reduced by managing and disseminating information on shipments in transit in a timely manner.
- The documentation screening process performed by Customs organizations can be expedited through effective monitoring and management of electronic data.
- Providing real-time information could contribute to reducing and/or deterring criminal activity.
- With secure data and timely availability of needed information, misrouted shipments could be stopped and corrected faster.
- Knowing Industry participants and their IT security practices, policies, and infrastructures could heavily influence situational awareness.

6.1.5 *Findings Relative to Training*

Technology alone will not solve the GSC IT security problem. No matter how advanced the technology is it will be deployed in an environment where humans

exist. This situation becomes more complicated within the GSC environments because of additional factors such as language and cultural differences. Moreover, technological infrastructures in many third world countries are narrowband when compared to the advanced countries. The following findings relate to IT security training:

- The human element is a major cause of security compromises, especially when not adequately trained. It is difficult to make up for the deliberate or accidental loss caused by humans. It is also difficult to predict how humans would circumvent security mechanisms. Despite the technology, the security procedures, or the security training provided by an organization, people would invariably fail to do what they are supposed to and will create security vulnerabilities (Kakish et al., 2005).
- A significant portion of employee-created security problems arise from poor security practices. For many years, computer intruders have relied on users selecting poor passwords to help them in their attempts to gain unauthorized access to a system or network.
- Organizations should have a policy that restricts the ability of normal users to install software and new hardware on their systems. Contractors, consultants, and partners may frequently not only have physical access to the facility but also have network access. Other groups that are given unrestricted, and unobserved, access to a facility are night-time custodial crewmembers and security guards. Both are potential security problems.
- Social engineering is a technique in which the attacker uses various deceptive practices to obtain information which the attacker would not be privileged to, or to convince the target to do something they normally would not. In reverse social engineering, the attacker hopes to convince the target to initiate contact.
- Contrary to the first finding (people are a major cause of security compromises), people could also be a major cause of security capability and stability. The human element can be the best line of defense against a social engineering attack. The single most effective method to counter potential social engineering attacks, after establishment of the

organization's security goals and policies, is an active security awareness and training program.

6.2 Additional Findings

Undertaking a global level IT research of this magnitude may prove to be a complex and daunting task. However, given adequate funding and support (in terms of corporate sponsorship of a large-scale prototype), it remains to be reasonably possible to advance the improvement of IT security and compliance within the GSC. This effort has somewhat dealt with identifying the GSC IT security and trade compliance problems. Implementing a robust conceptual solution globally could achieve the desired improvement.

Conducting the interviews with a comprehensive representation of the industry's IT Security and GSC executives made it clear that such an implementation is possible and within reach. The greatest majority of the interviewees validated the conceptual solution positively and indicated interest in supporting the implementation of a prototype by their willingness to participate in a pilot and by funding the implementation.

A logical next step would be to design and implement a prototype across the globe. As discussed in Section 5.5, one of the effective scenarios of implementing the conceptual solution prototype would be on top of existing UN Single Window Facilitation® implementation, where the IT infrastructure is already available and operational. The current instances of the UN Single Window implementations discussed in Section 5.5.1 could be expanded to include the GSCITSS prototype to developing countries.

Ultimately, a full-fledge implementation of the conceptual solution model could be implemented across the globe, and administered and regulated via international organizations such as the WCO, the UN, and the WTO.

6.3 Answers to Research Questions

In Section 1.5 of this dissertation document, several research questions were presented. These questions collectively led to the formation of the hypothesis. Most of these questions were asked during the interviews. Furthermore, these questions were equally placed under the revealing light of the review of literature as well.

The initial literature review (which was conducted prior to the proposal of this research) has shown that the common perception among the majority of government and industry executives is one of major concern regarding the security of the GSC. Clearly, there have been copious observations and assumptions linking the impact that security technologies and processes have on the stability of world trade and the global economy, but further research was necessary to serve as evidence to the validity of such assumptions.

From the onset of this research, the question at hand had to deal with *the extent to which IT security improves the overall safety and stability of world trade and the global economy*, which can be translated directly to the bottom line objectives of world governments and businesses alike. Clearly, the research questions were carefully formulated and closely related to the hypothesis of this dissertation. This section attempts to answer such questions based on input from the interviews, questionnaires, and the review of literature. These answers lead to the validation of the research hypothesis.

1. Based on your experience, what weaknesses in the global supply chain are impacting the security of your transactions?

Most answers to this question focused on some of the exploits we have experienced, especially since the events of 9/11. The GSC has several

bottlenecks or “points of weakness” or “choke points” that could impact the security of the data transactions. These choke points include, but are not limited to, the following:

- Weaknesses in current inspection systems and ports of entry, including the *inadequate inspection* of all types of vehicles and vessels entering the country. Senator Coleman requested that the Congressional Budget Office (CBO) initiate a study of the economic consequences of an attack on the Ports of Los Angeles and Long Beach. This study found that the United States’ gross domestic product (GDP) would decline by about \$150 million per day for each day that the ports were closed and that the annual cost would be approximately \$70 billion. Recommendations that would help to enhance the security of entry points are discussed in Section 6.6.
- Inconsistency of transaction data formats being exchange. Data often needed to be translated and mapped from one format into another (ex: EDI to ebXML, etc). The potential for exploiting this data is significant.
- Fragmented transportation of data transactions. Data exchanged electronically is transported and processed at a much faster rate than paper-based data, obviously.
- Lack of full and frequent audits.
- Lack of trade compliance.
- Corruption (such as bribery in some 3rd world countries).

2. What technologies have you deployed to secure your global SC transactions? How did these technologies help you to secure the global supply chain and enhance your operational effectiveness?

The answer to this question varied significantly from one IP to another due to a number of factors including the *diversity of technologies* available in the global marketplace. However, all Industry participants agreed on the

commonality of taking serious technological measures against potential cyber crimes and IT security exploits.

Legacy systems used older security technologies (ex: RACF™) while mid-range systems used UNIX-based security products (ex: CA-Unicenter, Tivoli, etc). For many suppliers and OEM's the use of RFID tags and GPS has become an essential ingredient in the SCM processes. Local and remote firewalls, proxy servers, load balancing servers, SSL certificates, and VPNs are some of the common technologies being deployed across a plethora of disparate systems and infrastructures. Intrusion detection and preventions software has become a necessity to many Industry participants.

Most responses indicated that the deployment of these technologies had a noticeable positive impact on the operational effectiveness of the GSC transactions.

- 3. What security measures do you use to monitor the security of your transactions in the global supply chain? Why did you select these measures? How often do you collect these measures? What do you use these measures for and how do you report them? What are the effects of these measures? How effective do you consider these measures? Why?**

This question was one of that received considerable attention by the interviewees, especially CIO's and IT professionals. While most replies were

expected to be textbook type answers, the interviews revealed some key point that could help in further protection of the GSC exchanged data.

Clearly, securing data means protecting any form of information that is vital to the industry participants' business interests. In essence, an industry participant's entire *survivability* is **directly linked to the protection of their data**. However, once that data leaves the perimeter walls of that industry participant, only robust data security mechanisms can ensure total protection and integrity of the data. This is nowhere more true than within the GSC. Data travels across thousands of miles across the globe every hour. When security issues arise, the entire well being of the industry participants becomes in danger.

All business networks are subject to network attacks, yet not all businesses have the resources necessary to proactively monitor, manage, and keep current with the latest security advances to prevent a network attack from being successful. Fortunately, we live in an era where small and mid size industry participants can have access to the same information security techniques and technologies that large industry participants employ.

The requirement to measure IT security performance is driven by regulatory, financial, and organizational reasons. A number of existing laws, rules, and regulations cite IT performance measurement in general, and IT security performance measurement in particular, as a requirement.

Before beginning to talk about the security measures, most interviewees elaborated on the need to assess their company's *risks* in order to determine the best strategies for managing it. As such, they discussed metrics which they could use to perform the following:

- Benchmark software counterparts.
- Develop clear path towards improving software security in a measurable fashion.
- Feed the information into an existing risk management system to determine the impact on the business in particular and on their relationship with other Industry participants.

The security measures used to monitor the security of automotive GSC transactions were broken into two fold: *business metrics* and *technical metrics*.

Business measures included the number of data transactions the failed or did not make the complete round trip cycle between the two trading partners, amount of time it took to complete the cycle of data exchange, loss of business

opportunity due to the failure, the overall impact on the productivity of the business in terms of “deliverable units” or dollars, and the organization’s ability to respond to an security breach incident. The technical metrics included security defects found in source code, quality defects found in source code, and potential exploits that failed an intrusion test, among others.

Some of the interviewees alluded to their interest in creating a descriptive model that could present them with everything they need to know about the software and utilize some of their project artifacts to gauge the security of the data exchange security software by utilizing existing tool which could enable them to have useful, high-level information about their GSC environment. Any tool that produces objective, repeatable, and easily digested security information would be considered a good candidate for the descriptive model.

These measures were selected because they align with the business objectives and reflect the success factors for that particular business. Although the measure were collected frequently, on daily basis in most cases, many of the interviewees indicated that they reported these measures as part of the

monthly dashboard that is presented to the executive committee, and on quarterly basis to the board of directors.

The effects of these measures yielded a close monitoring of the overall movement and exchange of data, and provided the ability to most IT departments to act swiftly in correcting any problems or potential exploits that may arise.

The process of data collection and reporting will enable the management to pinpoint specific technical, operational, or management controls that are not being implemented or are implemented incorrectly. IT security metrics can be created to measure each aspect of the organization's security. For example, the results of risk assessments, penetration testing, security testing and evaluation, and other security-related activities can be quantified and used as data sources for metrics. Using the results of the metrics analysis, program managers and system owners can isolate problems, use collected data to justify investment requests, and then target investments specifically to the areas in need of improvement. By using metrics to target security investments, organizations can get the best value from available resources.

Most interviewed executives considered these measures very effective because they established control limits on what the business could tolerate in terms of deviation from what is considered normal business operations.

4. What security standards do you adopt/follow for your GSC transactions, if any? Why? How might compliance to such standards improve inventory visibility and interoperability?

The majority of the interviewees had developed and maintained their own IT security policy. Some were outdated while others were being constantly revised and update to reflect compliance to new laws and regulations. Most had an issue with the additional on-going requirements for maintenance and updates of such policies. None of the interviewees were aware of any existing GSC IT security policy, and most welcomed the idea as feasible. Some considered such policy would provide common ground for everyone to operate from. Furthermore, none of the answers to this question indicated any recognition of an automotive industry IT security policy.

At a minimum, the majority of the interviewees maintained a common ground in terms of their adherence to the C-TPAT security standards. These included container and conveyance security, cargo tracing and physical access controls, personnel and procedural security, threat awareness and

physical security, and IT security. The IT security included internal and external measures. Internal procedures included password protection and access restrictions. External procedures included viruses, firewalls, and tampering prevention. Additional IT standards included IT security policies, procedures, management support, training, system backup and recovery plans.

Additionally, a number of the Industry participants had maintained some level of adherence to the UN and WCO security standards. Such standards include Simplification and Harmonization of Trade Procedures, UN trade documents, UN Codes for International Trade, and Recommendations for Information and Communications Technology (ICT).

Most interviewees indicated that compliance to such standards had improved inventory visibility and interoperability to a certain extent.

5. How has compliance impacted your security improvement efforts and IT budget?

This question was one that was not completely clear to the interviewees because it did not specifically identify the type of compliance. Some understood it compliance as IT security standards while others thought of it as compliance to trade standards and requirements (ex: WCO standards). In

either case, the answers were similar and seemed to support, and in some cases confirm the findings of the AMR research which was discussed in Chapter 2.

The commonality in these answers were that indeed, compliance to standards (whether IT security or trade) had played a positive role in improving the overall security. However, at the same time, it caused most companies to hire additional IT security personnel to respond to auditors, and caused additional expenses in their IT budgets. As discussed in Section 2.1, some IT organization had to make certain cuts of some of their IT programs in order to accommodate the added compliance requirements.

6. What new ways or methods would you like to see implemented at a global level for the sake of improving your GSC security procedures?

The answers to this question varied significantly from one interviewee to another. It is important to note that this question was presented at a time when the recommended GSC IT Security Policy was not emphasized or elaborated on directly. However, upon demonstrating the need for such a global policy as a response to the WCO SAFE Standard, which is outlined briefly in Exhibit One, the majority of the interviewees were in agreement

that a GSC IT Security Policy was necessary and needed in order to improve their GSC security procedures.

Other answers included methods and techniques which gave the OEM's too much control over the suppliers, and especially 3rd world country SME's.

Generally speaking, many interviewees' answers led the researcher to believe that they would be happy with a global methodology, or a set of methodologies, that would improve the GSC security procedures, especially when dealing with 3rd world SME's.

7. How can the powers of technology be leveraged to secure the global supply chain and enhance its effectiveness?

As discussed in various sections of this research earlier, technology alone is not enough to secure the GSC. Participants in the automotive GSC need to focus on key strategies to implement in order to secure data and exchange it safely and within a timely manner. These *key strategies* include:

- Diversity of defense. This is a concept that complements the idea of various layers of security. It aims to make the security layers dissimilar so that if one layer is penetrated, the next layer cannot be penetrated using the same method.
- Access management. The objective of access management is to provide the ability of a subject to interact with an object. Access controls are those devices and methods used to limit which subjects may interact with specific objects.

- Authentication mechanisms ensure that only valid users are provided access to a computer system or network. The three general methods used in authentication involve the users providing either of the following: 1) Something they know, 2) Something they have, or 3) Something unique about them (something they are – ex: Biometrics).
- Multifactor authentication is a term used to describe the use of more than one authentication mechanism at the same time. Mutual authentication is a term used to describe a process in which each side of an electronic communication verifies the authenticity of the other.
- Intrusion detection systems (IDS) and Intrusion prevention systems (IPS) are mechanisms for detecting and preventing unexpected or unauthorized activity on computer systems. These are systems that watch for and block unusual network or server activity that could indicate a security threat. Their goals are to protect critical information systems proactively and reduce risk that a single event could halt the network. IPS and IDS can be host-based or network-based.
- Digital Signatures are pre-defined patterns used to spot malicious or suspicious traffic. They may be either content- or context-based. Anomaly-based IDSs look for activities that do not match “normal” patterns. Misuse-based IDSs match suspicious or malicious patterns using signatures. Some IDSs include prevention capabilities that automatically block suspicious or malicious traffic before it reaches its intended destination.
- Honeypots are based on the concept of luring attackers away from legitimate systems by presenting more tempting or interesting systems that, in most cases, appear to be easy targets. Security personnel monitor traffic in and out of a honeypot to better identify potential attackers along with their tools and capabilities. Honeypots create virtual servers and services that offer inviting targets for potential attackers.
- Incident response is the formalized response of reacting to a situation such as a security breach or system outage. While many incident response systems are based on threats from potential attackers, incident response can be used to deal with other situations such as virus outbreaks, hardware outages, and loss of network connectivity. Incident response requires procedures that outline steps to take for notification, analysis, and remediation.

- Wireless Application Protocol (WAP) is used on small, hand-held devices like cell phones for out-of-the-office connectivity. The IEEE 802.11 is the standard for wireless local area networks. The different specifications of the standard include 802.11b, 802.11a, and 802.11g. Problems with the IEEE 802.11 are that it does not allow physical control of the transport mechanism, allowing data to be transmitted to all wireless machines not just a single client. A second issue is poor authentication since the SSID is broadcast to anyone listening.

8. What knowledge can be discovered that may yield creative new ways of applying security procedures to the global trading process?

The general understanding one could obtain from conducting the interviews and reviewing the questionnaires answers is that most solutions that are put in place to date have been reactive rather than proactive. Technologies are developed everyday, but only to answer to situations that have already occurred. This is considered old knowledge. What the GSC needs in terms of securing its data exchange is anticipated knowledge of potential threats and security exploits.

Several interviewee executives suggested the establishment and maintenance of a Threat Awareness Program to recognize and foster awareness of the threat posed by terrorists at each point in the GSC. Such a program can be maintained by security personnel coming from the various Industry participants within the automotive industry. Within this awareness program,

employees could be made aware of the procedures the company has in place to address a situation long before it actually happens. They will also be able to know how to report it, and who to report it to. In addition, it was also suggested that additional training should be provided to employees in the shipping and receiving areas as well as to those receiving and opening mail.

Additionally, it was recommended that specific training should be offered to assist employees in maintaining cargo integrity, recognizing internal conspiracies, and protecting access controls. These programs should offer incentives for active employee participation. In essence, the idea is: the more security related information can be anticipated in advance, the better prepared the automotive industry can be before a security incidence actually happens.

Another knowledge area that could be discovered which may yield creative new ways of applying security procedures to the global trading process is the effective use of security metrics. The common understanding of the role of metrics and their value to IT security in the GSC was consistent among the interviewees. They viewed metrics as tools designed to facilitate decision

making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. IT security metrics must be based on IT security performance goals and objectives. IT security performance goals state the desired results of a system security program implementation. IT security performance objectives enable accomplishment of goals by identifying practices defined by security policies and procedures that direct consistent implementation of security controls across the automotive organizations. IT security metrics monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls and the effectiveness and efficiency of the controls, analyzing the adequacy of security activities and identifying possible improvement actions.

6.4 Conclusions Related to Hypothesis

In view of the identified realities of GSC IT Security the goal of this research was to design and validate a conceptual model, which would be refined into a conceptual solution, to support the hypothesis proposed in Section 1.5. The hypothesis stated that:

“The security of the global supply chain may be improved if all participating trading partners adopt a systematic approach to information exchange.”

Examining this hypothesis eight research questions were formulated in Section 1.5, and answered in Section 6.1 from the interviews, questionnaires, and the studies of the theories and their applications. Additionally, a demonstration of concept section was discussed and presented in chapter 5.

All the research findings show that there are great benefits that may be obtained by implementing a solution similar in concept to the conceptual solution proposed, prototyped, and demonstrated in this dissertation. Coupled with a GSC IT Security Policy embedded within the WCO Data Model, discussed in Chapters 4 and 5, it is clear, based on this research, that if all participating trading partners adopt the “systematic approach”, proposed in Chapter 4, to information exchange, then security improvement in the global supply chain would be improved.

The findings discussed in Section 6.1 are summarized in Table 6-1 as to show how each finding addresses one or more of the research questions as follows:

<i>Conclusions Related to Hypothesis</i>		
Findings Relative to:	Summary of Findings	Research Questions Addressed
Electronic Data Exchanged	The ability to promote the electronic exchange of information through effective and secure systems and providing access to high quality trade compliant SME's in developing countries. Detailed findings discussed in Section 5.7.1.	1, 2, 4, 7, and 8
Trade Compliance	Common need for compliance verification system, such as the GSCITSS, in operation, and the need to further support the WTO "Multilateral Agreements On Trade In Goods". Detailed findings discussed in Section 5.7.2.	4, 5, 7, and 8
Best Practices	A summary of GSC IT security best practices based on the increased reliance on IT networks for e-commerce, authentication and non-repudiation by adopting the CIA philosophy. Detailed findings discussed in Section 5.7.3.	All research questions
Situational Awareness	End-to-end information sharing in real time can improve the ability to monitor for anomalies and to improve processes when such processes conform to robust situational awareness principles. Detailed findings discussed in Section 5.7.4.	1, 3, 6, 7, and 8
Hypothesis	A number of enablers and challengers which include electronic data exchange, best practices, situational awareness, training and additional findings. Detailed findings discussed in Section 5.7.	All research questions

Table 6-1: Correspondence between Findings and Research Questions

6.5 Evaluation of Demonstration of Concept in Terms of Hypothesis

Once the conceptual solution was developed and evaluated, and the criteria for the demonstration of concept were evaluated, now is the time to demonstrate how the evaluation of the demonstration of concept supports the hypothesis. This research set out to study the hypothesis that states the following: “The security of the global supply chain may be improved if all participating trading partners adopt a systematic approach to information exchange.”

Upon evaluating the demonstration of concept in terms of the hypothesis according to the technology selection criteria discussed in Section 5.2, systematic approach discussed in Section 4.8, and implementation model discussed in Section 5.5, one finds that such hypothesis is not negated, and indeed confirmed. This means that the initial contemplation of the impact of IT security on the GSC was valid.

6.6 Other Conclusions

This research has performed several empirical investigations, including research instruments such as conducting interviews with key industry participants in the automotive industry and several US and international standards and regulatory bodies (ex: NIST, UN, WCO).

Ultimately, the research focused on providing an innovative approach for improving the security of transactional data being exchanged within any two points of the GSC. To do so, Section 1.2.1 discussed the approach of providing a layered security architecture which employs several security methods. Such architecture makes it increasingly difficult for a potential attacker to penetrate deep into these secured layers. In essence, it forces a compromise that consumes more time and effort than it is worth. The more layers the architecture provides, the more difficult it becomes to attack or intrude. Also, implementing different layers is equally important because if intruders succeed at one layer, they could be stopped at the next. Therefore, the redundancy of different layers assures that there is no one single point of failure pertaining to security.

In addition, the deployment of the conceptual solution could be manifested in various configurations: 1) as a standalone system (GSCITSS), 2) with or on top of a Single Window Facilitation (GSCITSS/SW), and 3) with or without the deployment of a GSC IT Security Policy. Depending on the configuration of the conceptual solution implementation, the system as a whole or some of its subsystems could be used by a variety of end users to achieve certain objectives. But in the end, the deployment of the conceptual solution, regardless of its configuration, will satisfy the objectives of this research and improve security of exchange of data within the GSC.

By promoting the concept of the GSC IT Security Policy and adopting this systematic approach to data exchange, automotive Industry participants and their employees can continue to enhance and extend the applicability of the solution and keep the GSC IT Security Policy current. Furthermore, industry participants and all users of the system can document their lessons learned and share their knowledge and experiences toward an ever increasing electronically secure and compliant GSC.

Finally, the design of the conceptual solution provides flexibility, thereby allowing all Industry participants to contribute to the efforts securing the GSC further. The design enables the decision makers and the users of the GSCITSS to add more features to the system and reflect the addition of new regulations and laws into the GSC security policy until a more innovative or breakthrough approach to GSC security is discovered.

6.7 Summary of Contribution

The purpose of this section is to show the contributions to the advancement of GSC and IT as a result of conducting this research. Based on the data analysis and hypothesis results, the researcher was able to respond to the research questions and validate the research hypothesis. Performing this investigative research by applying the combined research process model (Steenkamp, 2005) and the Inductive-Hypothetic Research Strategy (Sol, 1982) has resulted in significant contributions as follows:

1. Clearly defined research problem and research focus. Investigating issues of IT security within the GSC has proven to be a massive undertaking. The ability to sort through the myriad of issues in order to clearly define the research problem contributed to identifying a well-defined and manageable research problem. Moving forward, the research focused on finding an innovative IT management solution to the documented problem. Therefore, the first contribution is identifying a well defined research problem.

2. Summary of literature review. Once the research problem was clearly defined, the review of literature was focused on the areas surrounding the research problem and focus, without the need to deviate into areas that are not directly related. Therefore, this contribution is a concise list of findings that resulted from a focused review of the available literature.
3. Research strategy and design. Armed with the research problem and the findings of the literature review, this contribution was the ability to create a research strategy that was capable of driving the appropriate research design to handle the investigation.
4. Research data. An effective research design leads to adequate data collection. Based on the appropriate research design, the next contribution of this project was to determine the methods by which useful research data would be collected. These methods included interviews, questionnaires, and additional literature review. The participants of the interviews were carefully selected and provided a comprehensive representation of Industry participants with senior IT and business executives as well as governmental and international standards and regulatory bodies' representatives. Therefore, this contribution is a useful set of collected data which could be analyzed qualitatively and quantitatively.
5. The conceptualizing a solution. The conceptual model served as foundation for the design of the conceptual solution. A meta-model was first developed to provide the blueprint for the design of the conceptual solution. Entities, or components, of the meta-model were defined along with their attributes, messages, data flows, and relationships and interrelationships.
6. Based on the conceptual model, the conceptual solution was designed and developed. Therefore, this is regarded as the most valuable contribution of this research project. The conceptual solution contributed several innovative logical components (ex: GSC IT Security Policy) and tangible subsystems (ex: GSCITSS, GSCITSS/SW, ERP integration agents, etc). In essence, deployment of the conceptual solution promises to deliver the innovative answers to the research problems.
7. Demonstrating the conceptual solution. Using ProVision™ Enterprise versions 5.2 and 6.0 as an enterprise case tool, the conceptual solution was modeled in over 20 different types of models and diagrams, along with their narrated reports. The conceptual solution ProVision™ models included business and technical diagrams. Some of these models include business class and interaction diagrams, communication diagrams, event models and

- diagrams, organizational diagrams, business process improvement diagrams, technical and data requirement diagrams, sequence diagrams, strategy models, system interaction diagrams, technology modelers (data, network, transaction, and security services, etc), use case diagrams, workflow models, and many more. The entire set of models for the conceptual solution is found in Appendix B of this dissertation document.
8. Several other models were created throughout this dissertation. These include risk models, financial models, and configuration models.

6.8 Limitations

Undertaking an investigative research effort of this magnitude is a tremendous effort by any stretch of the imagination. Inherent in the nature of conducting this research are several requirements that could cause stringent mandates and conditions. The most difficult aspect of performing this research is the ability to physically prototype the conceptual solution. Other methods such as simulation, virtualization, and modeling are much more pragmatic in carrying out this research. Therefore, the biggest limitation of performing this proof of concept is the difficulty in being able to implement or install a **physical prototype** of the conceptual solution. The reasons are plenty, and they are discussed below.

By default, performing an IT related research within the GSC means the involvement of the following ingredients:

1. Vast geographies that span the globe. Studying the supply chain within the US alone is a daunting task. Performing research across the globe complicates the issue further.
2. Large numbers of industry participants. The number of trading partners around the world is in the millions of suppliers, vendors, government agencies, etc. For example, although paired down significantly in recent years, any one of the big 3 OEM's in the US automotive industry has several thousands of trading partners. General Motors alone has nearly 3,000 suppliers. Ford Motor Company and Chrysler have similar numbers of suppliers each.
3. Very large and complex IT systems. Within the GSC, ERP and SCM systems are core to the daily operations of any business. Other systems (ex: MRP) are needed as well. A breakdown of any ERP system could easily be flushed into several very large modules (HR, financials, etc). Any subsystem alone qualifies as a major IT application.
4. Governments dictate different laws. Within the GSC, one needs to consider various types and shapes of governmental agencies. For example, in the US alone, there are significant complexities between the DHS and US Customs, and between their un-integrated IT systems. Although IT technologies are advanced in the US, there is very little to no interoperability among these systems. The rest of the world is yet behind.
5. Data standards and types are diverse and incompatible in many cases. Chapter one discussed the issues associated with the multitude of available standards between the UN, WCO, and other international regulatory bodies.
6. Other factors such as cost, availability of resources with adequate technical skills to implement a physical prototype add to the issues of difficulty.

Despite these issues, this research project succeeded in making some initial contributions.

6.9 Recommendations

Based on the results of this research, several recommendations may be made. First, this study was conducted based on one industry, namely automotive. Most of the non-automotive interviewees were mostly government and regulatory body personnel, and did not have expertise in the automotive industry. Yet, they were experts in their fields (customs, standards, laws and regulations, etc). For the results discovered in the research to have greater generalization, it is recommended that other studies should be conducted using populations from other industries as well. It would be beneficial for future studies to draw from different suppliers, especially third world countries SME's.

Second, an experimental research may be undertaken to determine what contributes to third world countries SME's perception of US suppliers' requirements for trade compliance. Without further study the effects of trade compliance on developing countries' SME's could not be known. Therefore, it is recommended to conduct similar research abroad, especially in 3rd world countries that work closely with the US, such as China, India, Russia, and some parts of Eastern Europe.

A third recommendation is that a research may be conducted with international regulatory and standard bodies such as the UN and the WCO to further determine the applicability of implementing the recommended GSC IT Security Policy within one of the UN Single Window Facilitation implementations, such as the Netherlands. Conducting such research could yield valuable findings that could further promote the implementation of a GSC IT Security Policy even without the implementation of the GSCITSS presented in this dissertation.

6.10 Opportunities for Future Research

It has been already established that undertaking a global level IT research of this magnitude can be a complex task. However, given adequate funding and support (in terms of corporate sponsorship of a large-scale prototype), it remains to be reasonably possible to advance the improvement of IT security and compliance within the GSC.

This research effort has barely scratched the tip of the iceberg in terms of identifying the GSC IT security and compliance problems, and proposing a robust conceptual model that when implemented globally could achieve the desired improvement. Additional work remains to be done, but one trusts that

the significant and numerous collateral business benefits presented in this dissertation will serve to encourage other more Industry participants and their trading partners to further invest in the security of the global supply chain.

Conducting the interviews with a comprehensive representation of the industry's IT Security and GSC executives made it clear that such an implementation is possible and within reach. The greatest majority of the interviewees validated the conceptual solution positively and indicated interest in supporting the implementation of a prototype by their willingness to participate in a pilot and by funding the implementation.

A logical next step would be to design and implement a physical prototype across the globe, as described in Chapter 5. One of the effective areas of implementing the conceptual solution prototype would be on top of existing UN Single Window Facilitation® implementation (United Nations, 2007), where the IT infrastructure is already available and operational. Ultimately, a full-fledge implementation of the conceptual solution model could be implemented across the globe and administered and regulated via international organizations such as the WCO, the UN, and the WTO.

6.11 Summary and Conclusion

This chapter discussed the research findings relative to the hypothesis, conclusions, the research limitations, and the recommendations in light of the limitations and conclusions. In essence, this part of the dissertation document has served to confirm that the initial hypothesis of the ability to improve the security of the global supply chain through the secure use of IT is valid and stood the test. This chapter has demonstrated such conclusions, research limitations, and provided recommendations for further and future research.

Complexities in the automotive GSC cause several entities to tolerate compliance and electronic information security pressures. A research in the space of IT management and industry participants' behavior became necessary. The researcher defined the problems and challenges facing the electronic GSC, and devised a conceptual solution to mitigate the risks of these problems. To validate the conceptual solution, the researcher interviewed with eleven industry representative organizations and twenty-two individuals using a variety of communication methods. Upon careful analysis of the data, it became apparent that by adapting a systematic approach to data exchange and collaboration, industry participants could promote the electronic security of information and

data sets across the global supply chain. The study involved a doctoral-level research in information technology. Ample literature was reviewed and a hypothesis was stated. The conceptual model was pre-faced by a Meta model, in the form of a business class diagram. An inventory of over twenty various models and diagrams was created using the ProVision™ Enterprise Modeling Suite. The literature review showed that a significant portion of processing GSC documents in the automotive industry is still paper based. This causes significant transport delays and increases the potential for errors and IT security exposures. The conceptual model involves establishing a GSC Hosted IT Security Infrastructure Framework coupled with a GSC IT Security Policy that aligns and interoperates with UN Recommendation 33 and the WCO Data Model. The study sought to explain strategic issues related to IT management and industry participants behavior. The study used a qualitative descriptive research design using a questionnaire and a set of interviews as the primary means of data collection. The interviews covered a wide representation of global Industry participants. The results of this study demonstrated a statistical correlation between IT Security and compliance. These results are beneficial to GSC IT Security administrators, technical, and operational specialists.

APPENDIX A TWO-PART INTERVIEWEE QUESTIONNAIRE

The information that follows represents the research questionnaire and interview contents, as described in the body of the dissertation document.

Greetings,

My name is Kamal Kakish. I am a doctoral student in the management of information technology (DMIT) at Lawrence Technological University.

Thank you for your willingness to participate in answering this questionnaire. This document contains 2 parts:

1. The first part is a quick yes/no/unsure questionnaire (checklist) that covers strategic enterprise IT security issues.
2. The 2nd part involves answering GSC IT Security discipline questions relative to your environment in terms of IT security metrics, standards, and compliance.

The purpose of the questionnaire and questions is to obtain an understanding of the Global Supply Chain (GSC) IT Security issues in the Automotive Industry as they relate to a number of enterprise strategic issues.

The first questionnaire “**Part I**” is based on Col Perks and Tony Beveridge’s Management Checklist (Perks and Beveridge Guide to Enterprise Architecture, 2003, pp 18-20). It is intended to be used as a mean of identifying the current state of IT security within the global supply chain.

The 2nd set of questions “**Part II**” is free-form. You may answer all questions applicable to your enterprise/organization. If you encounter any questions that do not apply to your environment, simply answer with “N/A”.

Information about Interviewee

Name of Organization: _____

Type of Business (ex: OEM, Supplier, etc): _____

Scope/Specialty of Business: _____

Your Name: _____

Your Title or Scope of Work: _____

Size of your IT Organization (Headcount/Contract) _____

Size of your IT Budget (\$) _____

Appendix A Section 1

Part I

The table of questions below illustrates a GSC IT Security checklist designed to focus on the strategic business issues that can be resolved by adopting a conceptual solution approach. It represents a rapid health check of the current state of GSC IT Security disciplines within your organization, and could be used to provide an indicator to the extent of problems within the environment.

Analysis of answers: A reasonable number of YES answers (say, greater than 10) indicate that the organization should review the way GSC IT Security policy and technology are managed.

Please fill in the blank all the information to the best of your knowledge based on the current situation for your organization, then answer Yes, No, or Unsure to the questions below.

Please complete the following tables with Y, N, or U.

Subject Area	Indicator Question	Yes/No/Unsure
Strategy	Can the success of the IT Security Strategy be easily measured in meeting the business strategy within the global supply chain?	
	Does the cost of IT security appear higher in the global supply chain than other sectors of the global economy?	
	Do we know the cost of securing the IT environment in the global supply chain?	
	Are the systems failing to deliver to all the GSC participants' information needs?	
	Is there lack of common understanding of key organizational information and business terms?	
	Is it difficult to measure how well the enterprises' IT systems within the GSC meet the needs of the participants'?	

Global Supply Chain IT Security Hosted Services

Subject Area	Indicator Question	Yes/No/Unsure
	organizations?	
	Do we find that a project approach to IT implementation introduces tactical decisions that have a negative effect on the overall IT security environment within the GSC?	
	Is the ability to make in-source out-source decisions hampered by currently existing technology?	
	Does GSC business success appear to be hampered/not enabled enough by the participants' current information technology?	
Governance	Are IT security project prioritization mechanisms limited, non-existent or compete with other IT projects?	
	Do we experience difficulty ensuring the IT security projects meet quality requirements?	
	Do IT security projects within the GSC lack concrete technical quality standards or guidelines?	
	Is it difficult to ensure that the strategic requirements of the participants' organizations are maintained by each IT security project?	
	Are deviations from the intended strategic IT direction difficult to spot and correct?	
	Do battles ensue (within an organization and among industry participants) over technology choices?	
	Are there limited mediation mechanisms for addressing differences of opinions regarding technology choices?	
Integration	Do GSC industry participants complain about their inability to maintain accurate and consistent information about their businesses?	
	Do we find that changes required in one system manifest themselves in costly changes in other systems?	
	Do we find that integrating electronic information from customers and partners is costly and lacks integrity?	
	Do management information reports represent an inconsistent view of the current operational state of the organization?	

Global Supply Chain IT Security Hosted Services

Subject Area	Indicator Question	Yes/No/Unsure
	Are there problems with internal business units communicating with each other about GSC transactions electronically?	
	Are there problems with GSC industry participants communicating with each other electronically?	
	Has there been a lack of success in developing a corporate-wide shared knowledge base?	
	Has there been a lack of success in developing an industry-wide shared knowledge base?	
	Do IT projects sponsored directly by the GSC participants exhibit integration and quality problems when introduced into the IT environment?	
	Is the integration between legacy and contemporary systems ineffective and costly?	
Quality	Are there difficulties in measuring how the IT security environment supports service levels for the industry participants and other IT customers?	
	Do we find that GSC security applications look and behave differently to their users?	
	Do GSC participants regularly experience performance difficulties with new and existing systems?	
	Do we find IT security systems within the GSC are difficult and costly to extend?	
	Is the resolution of operational IT problems ineffective and non-timely?	
	Do GSC participants feel at the mercy of their technology vendors?	
	Does the delivery of systems into international business units require significant system change?	
	Do systems experience more down-time than is deemed necessary?	
	Do the GSC participant organizations lack business continuity plans for their IT systems?	
Procurement	Are GSC participants continually considering the replacement of existing systems in new technology?	

Global Supply Chain IT Security Hosted Services

Subject Area	Indicator Question	Yes/No/Unsure
	Does the procurement process for technology projects require continual re-invention, and appear ad-hoc?	
	Is the technology procurement process for most GSC participants unnecessarily cumbersome and time consuming?	
	Is there more than one GSC management package within the organization?	
	Is there more than one ERP package within the organization?	
Security	Has the organization's IT function been disrupted by a security attack?	
	Does the organization "fear" connecting to the Internet for their e-Business?	
	Is there limited or no information that would prove to the GSC participants that there have been no internal or external security breaches of their IT systems?	
	Do most GSC participants lack a security policy that sets out how security will be achieved in their organizations and across the GSC?	
	Do employees exhibit limited knowledge of their responsibilities with respect to IT security?	

Appendix A Section 2

Part II

Below is a set of GSC IT Security related questions. Unlike the checklist in Part I, these questions are designed to focus on discovering the impact of certain GSC IT Security measures within your organization.

Clearly, there is no right or wrong answers. The answers you provide are mere description of the IT Security related activities, policies, and strategies within your organization.

Of course, the answers will vary depending on their source. For example, a Tier-1 automotive supplier's answers might vary significantly from those of a Regulatory/Standards body.

The answers you provide are kept according to strict Privacy and Confidentiality guidelines, and will be used for educational research purposes only.

Analysis of answers: The answers will be stratified according to a number of categories including Type-of-Business, Scope-of-Business, Size of Organization, etc. Averages and percentages will be compiled and calculated to show how various Industry Participants responded to IT Security discipline areas including impact of having IT security metrics, impact of Compliance on IT Security procedures, and impact of IT Security standards and policies.

Please complete the following questions to the best of your knowledge. If the answer is not applicable or unknown, simply answer with "N/A" or "Unknown".

1. Based on your experience, what **weaknesses** in the global supply chain are impacting the security of your transactions? Please list:
 - 1.1. _____
 - 1.2. _____
 - 1.3. _____
 - 1.4. _____

2. What **technologies** have you deployed to secure of your global SC transactions? Please list technology product types (ex: VPN, SSL, Firewalls, encryption, etc):
 - 2.1. _____
 - 2.2. _____

 - 2.3. How did these technologies help you to secure the global supply chain and enhance your operational effectiveness? Please list (ex: reduced transaction coding/recoding by x %):
 - 2.3.1. _____
 - 2.3.2. _____
 - 2.3.3. _____

3. What security **measures** do you use to monitor the security of your transactions in the global supply chain? Please list (ex: number of failed transactions)
 - 3.1. _____
 - 3.2. _____

Global Supply Chain IT Security Hosted Services

3.3. _____

3.4. _____

3.5. Why did you select these measures in particular? Please list your reasons (ex: Direct alignment with corporate objectives)

3.5.1. _____

3.5.2. _____

3.5.3. _____

3.6. How often do you collect these measures? Please list (ex: daily, weekly, monthly, etc)

3.6.1. _____

3.7. How often do you report on these measures? Please list (ex: daily, weekly, monthly, as needed, etc)

3.7.1. _____

3.8. What is the purpose of using these measures? Please list (ex: determine Problem Recording & Reporting - PR&R, or Report on CIO/CEO monthly dashboard)

3.8.1. _____

3.8.2. _____

3.9. What are the effects of these measures? Please list (ex: improved transaction processing time, improved Quality of Service Level, etc)

3.9.1. _____

3.9.2. _____

3.9.3. _____

3.10. How effective do you consider these IT security measures? Why? Please list (ex: somewhat effective because they expedite transaction processing time and ultimately impact revenue)

3.10.1. _____

4. What **IT Security Standards** do you adopt/follow for your GSC transactions, if any? Why? Please list (ex: Corporate IT Security Policy, OR Standards dictated by our Customer, OR International IT Security Standards such as UN/WCO/ISO/IEEE etc)

4.1. _____

4.2. _____

4.3. _____

Global Supply Chain IT Security Hosted Services

5. How might **compliance** to such standards improve inventory visibility and interoperability? Please list (ex: improves end-to-end inventory visibility)

5.1. _____

5.2. _____

5.3. _____

5.4. How has compliance impacted your security improvement efforts and IT budget?

5.4.1. _____

5.4.2. _____

6. What new ways or methods would you like to see implemented at a global level for the sake of improving your GSC security procedures?

6.1. _____

6.2. _____

6.3. _____

Thank You very much for your participation.

Please forward your completed questionnaire to profkakash@gmail.com

If I may answer any questions over the phone, please feel free to call me at 248-703-6882.

Appendix A Section 3 - Performance Matrix

Goals & Measures	Design & Implementation	Management
<ul style="list-style-type: none"> ➤ Establish Security Management Strategy Alignment ➤ Ensure inventory visibility throughout the GSC ➤ Facilitate GSC security environments for interoperability ➤ Establish common regulations to promote compliance ➤ Comply with global security regulatory laws ➤ Improve GSC participants' responsiveness and satisfaction ➤ Consolidate real-time cargo reporting ➤ Improve project management methodologies ➤ Reduce inventory write-offs and costs ➤ Reduce scrap and waste costs ➤ Increase profitability ➤ Have accurate and timely (updated) data centrally available from various localities in the GSC ➤ Improve service levels 	<ul style="list-style-type: none"> ➤ Address and map goals and objectives of common to GSC IT Security requirements gathering. ➤ Define Information flows and processes for each major GSC participant organization (internal flows) ➤ Define Information flows among GSC participants and governmental ports of authority (external flows) ➤ Define data flows between business units, value chains, and key business process models ➤ Model AS-IS processes and information flows. ➤ Model SHOULD be processes and information flow ➤ Analyze and document Gaps ➤ Consider consolidation of IT Security package into single instance instead of multiple instances to reduce interoperability complexities ➤ Consider vendor consolidation to minimize customization efforts ➤ Data Flow Modeling and 	<ul style="list-style-type: none"> ➤ Enable the <i>measurement</i> of the IT Security Strategy to easily meet the business strategy. ➤ Reduce the <i>cost</i> of IT security in the global supply chain to compete with other sectors of the global economy ➤ Determine the cost of securing the IT environment in the global supply chain ➤ Deliver the information needs necessary to all the GSC participants. ➤ Ensure common understanding of key organizational information and business terms ➤ Measure how well the enterprises' IT systems within the GSC meet the needs of the participants' organizations ➤ Commonize a project approach to implementations of IT security systems within the GSC ➤ Resource allocation for personnel, HW, SW, facilities, etc ➤ Alignment of Corporate

Global Supply Chain IT Security Hosted Services

Goals & Measures	Design & Implementation	Management
within and among participant organizations ➤ Provide one comprehensive database to house all GSC freight information (ability to trace shipment from origin to destination)	Business Process Modeling ➤ Performance metrics for major business activities	Business Goals, Strategy and Objectives with GSC IT security systems Requirements and business processes

GSC Performance Matrix at the Organizational Level

Goals & Measures	Design & Implementation	Management
➤ Map organizational level identified information entities against information needs. ➤ Model against the strategic, tactical, and operational information needs of the GSC participant organizations ➤ Identifying functions that satisfy information needs. ➤ Map information entities against business functions to indicate of the effect of functions on entities. ➤ Map business functions and entity types to organizational units to assign security functions against various parts of the organization.	➤ Develop common business processes and data models across all participant organizations for the major IT Security target areas ➤ Implement measures to minimize the disruption for the IT function due to a security attack ➤ Design and implement robust mechanisms to securely connect to the Internet ➤ Design and implement processes that would detect and prevent internal and/or external	➤ Management of Process performance at process level for each participant major activities including: Inventory visibility reports, shipment status reports, shipper and receiver reports, government authority reports, management decision making reports, etc ➤ Improved Change Management ➤ Establishing common security settings across participant organizations ➤ Minimizing the number of disparate IT security modules ➤ Leverage PMO services and other project management best practices

Global Supply Chain IT Security Hosted Services

Goals & Measures	Design & Implementation	Management
<ul style="list-style-type: none"> ➤ Improve materials management ➤ Improve production planning ➤ Improve management and financial reporting ➤ Improve data integration across the GSC ➤ Ensure that proliferating the use of enterprise security systems gains the needed/necessary benefits 	<ul style="list-style-type: none"> security breaches of the participants' IT systems ➤ Design and implement comprehensive security policies that set out how IT security will be achieved across the GSC. ➤ Deploy GSC Security Awareness Training to employees of GSC participants and assign responsibilities with respect to IT security 	<ul style="list-style-type: none"> ➤ Minimize the frequency of replacement of existing systems in new technology ➤ Commonize the IT security systems procurement process across participant organizations ➤ Simplify the technology procurement process for GSC participants

GSC Performance Matrix at the Process Level

Goals & Measures	Design & Implementation	Management
<ul style="list-style-type: none"> ➤ Timely responsiveness to GSC security incidents ➤ Responsiveness to participants' security requirements ➤ Effective Identity and Access Management solutions ➤ Automatically managing who has access to which resources and 	<ul style="list-style-type: none"> ➤ Clarify strategic and organizational needs, and business implications of integration, before implementing ➤ Install enterprise IT security systems gradually, using a phased approach, one participant pilot group at a time, as compliance is confirmed by governing body ➤ Pay attention to regulatory compliance requirements 	<ul style="list-style-type: none"> ➤ Clarify strategy before planning GSC enterprise security system ➤ Minimize the number of security incidents ➤ Put the right people in the right place ➤ Fill the perpetual gap between package functionality and business needs ➤ Streamline unnecessary overhead

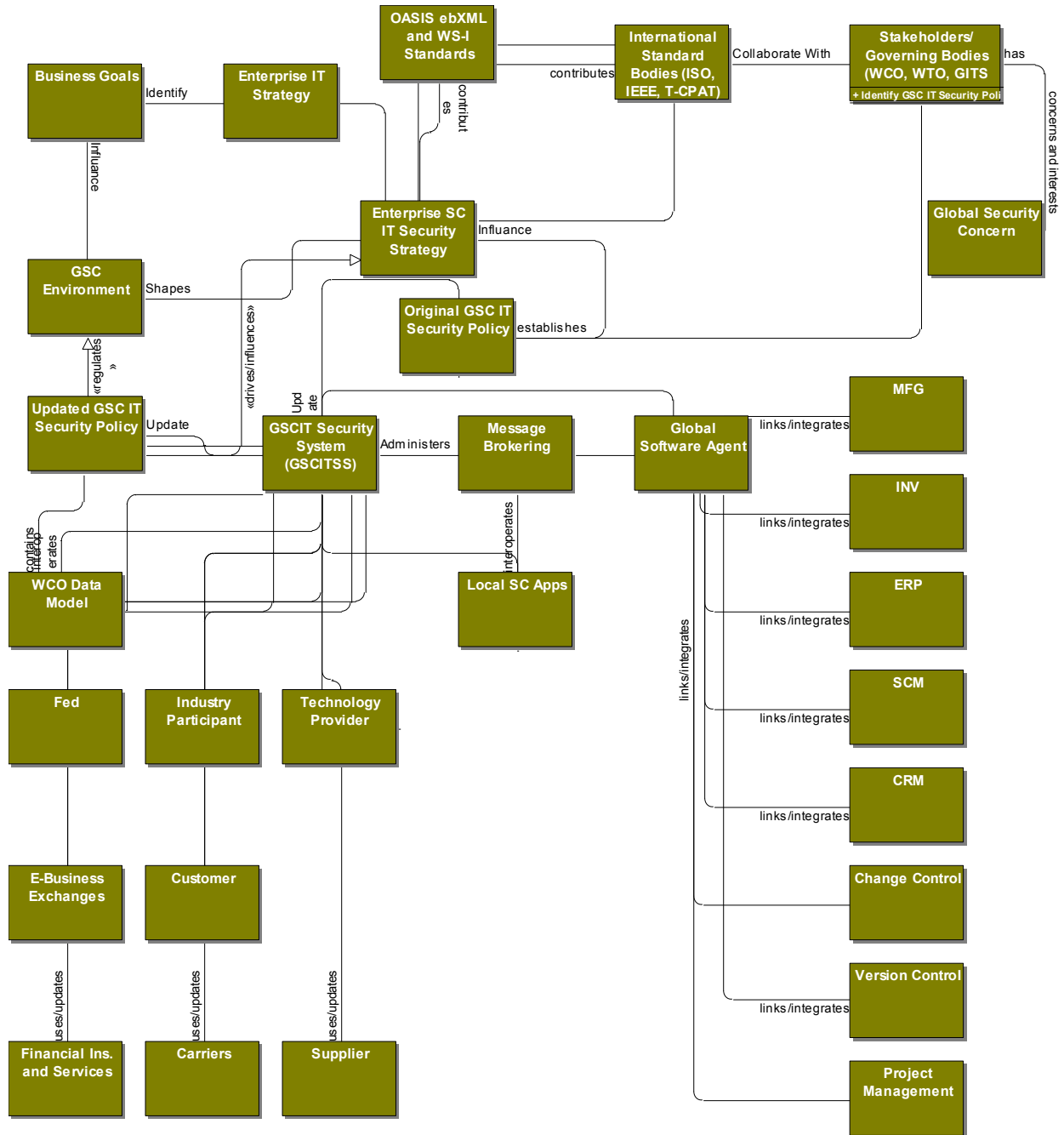
Global Supply Chain IT Security Hosted Services

Goals & Measures	Design & Implementation	Management
<p>services</p> <ul style="list-style-type: none"> ➤ Logging and reporting what users have done ➤ Enforcing business, privacy and security policies ➤ Reduce IT Security SW installation and configuration complexities ➤ Improving customer satisfaction according to SLA levels ➤ Improve ease of searching for inventory visibility ➤ Improve response time to attack incidents ➤ Enhance ease of generating accurate and timely reports ➤ Provide flexibility in generating queries and report for GSC participants 	<ul style="list-style-type: none"> ➤ Consider and deploy appropriate alternatives to reduce maintenance cost of GSC security solutions ➤ Consider off-the-shelf application interfaces to reduce integration design efforts ➤ Strengthen and gain greater control over total security ➤ Add a practical and affordable second authentication factor ➤ Better enforce both physical and logical security policies ➤ Achieve compliance with multiple regulations 	<p>activities</p> <ul style="list-style-type: none"> ➤ Consider outsourcing non-strategic activities and/or tasks ➤ Employ solid project planning mechanisms ➤ Establish robust communication plans with participant team members, management, and government port authorities

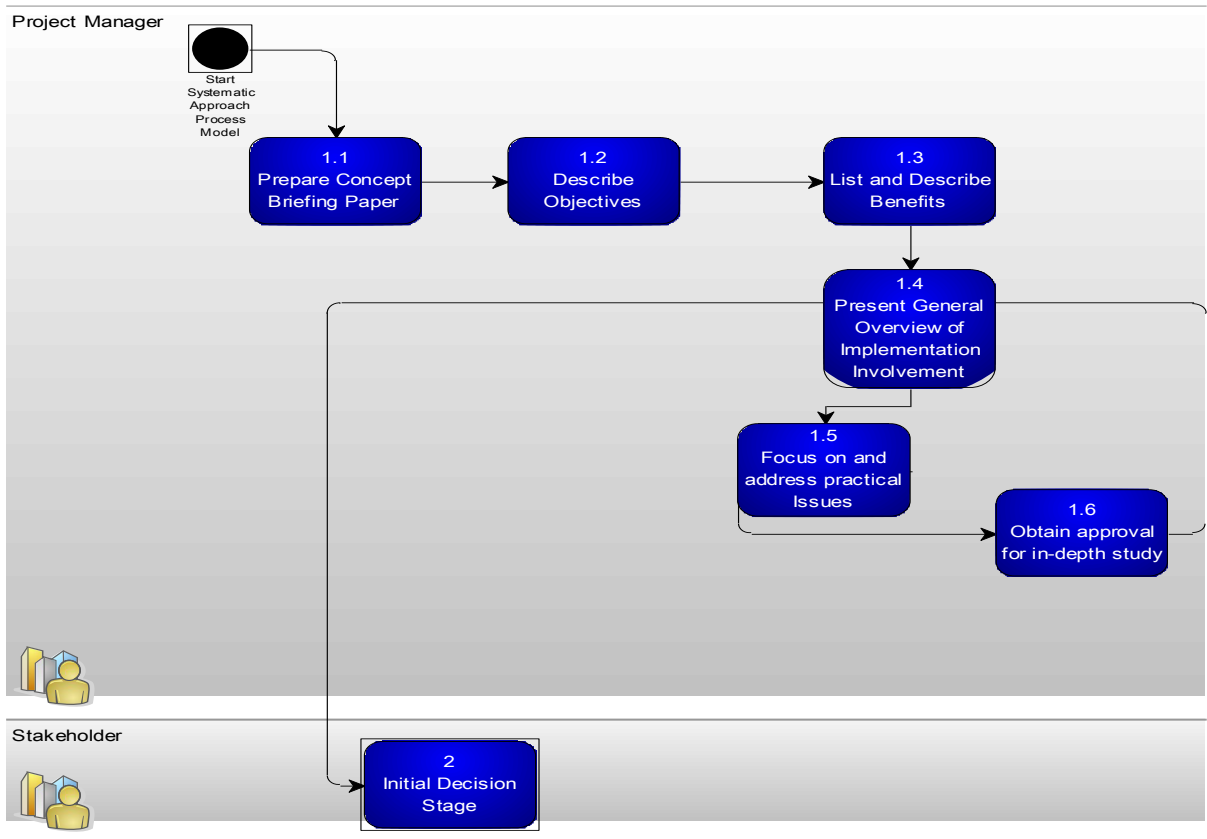
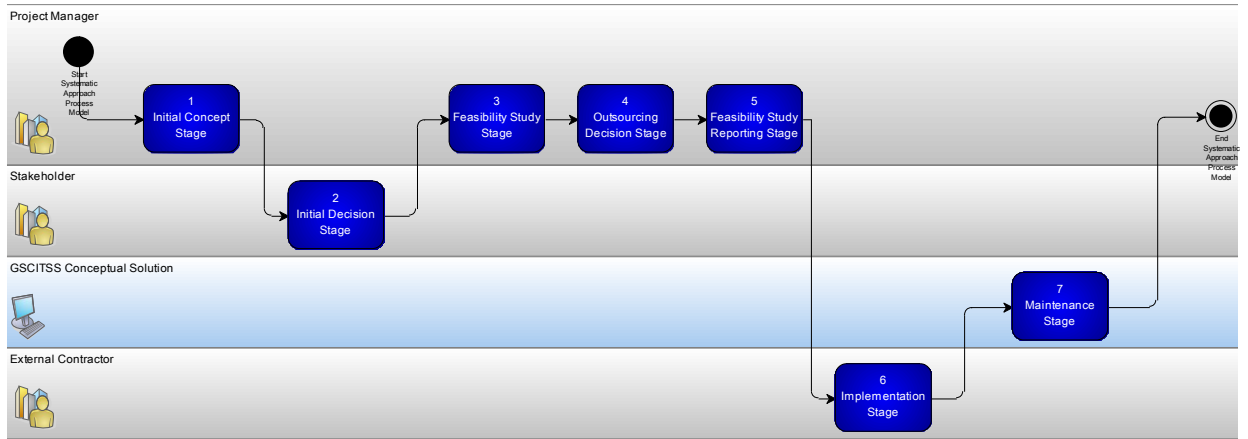
GSC Performance Matrix at the Operational Level

APPENDIX B RESEARCH MODELS AND DIAGRAMS

Section 1 Meta Model

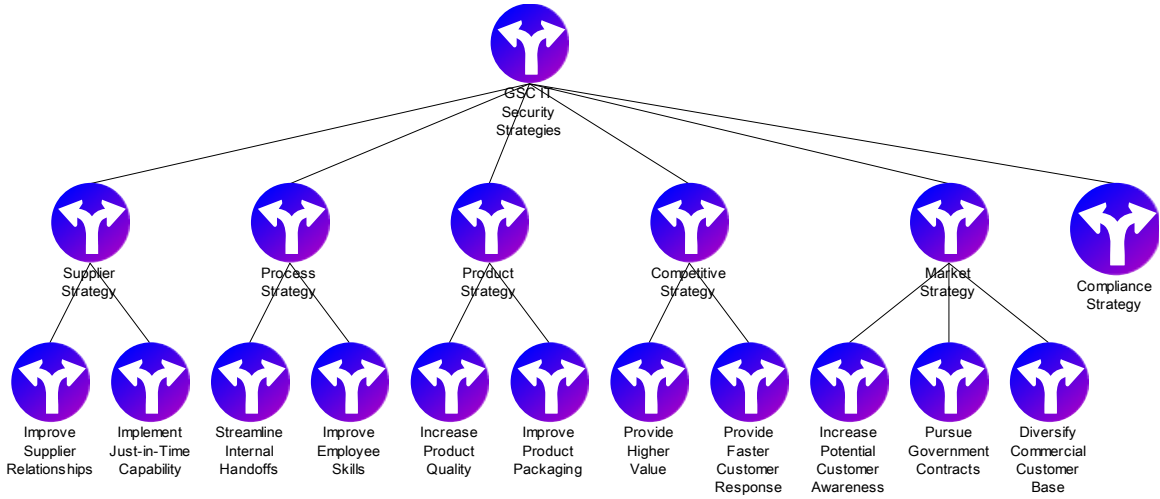


Section 2 – Systematic Approach Process Model Details

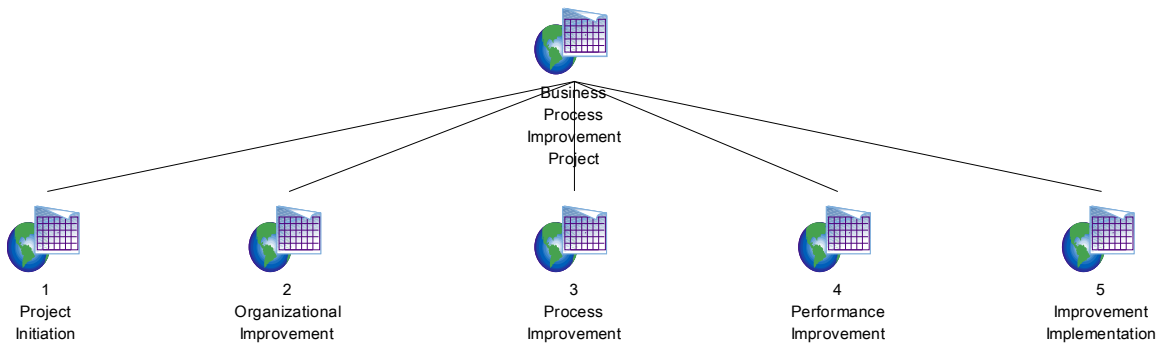


Section 3 – GMC USA Implementation Model ProVision Details

GMC USA Strategy

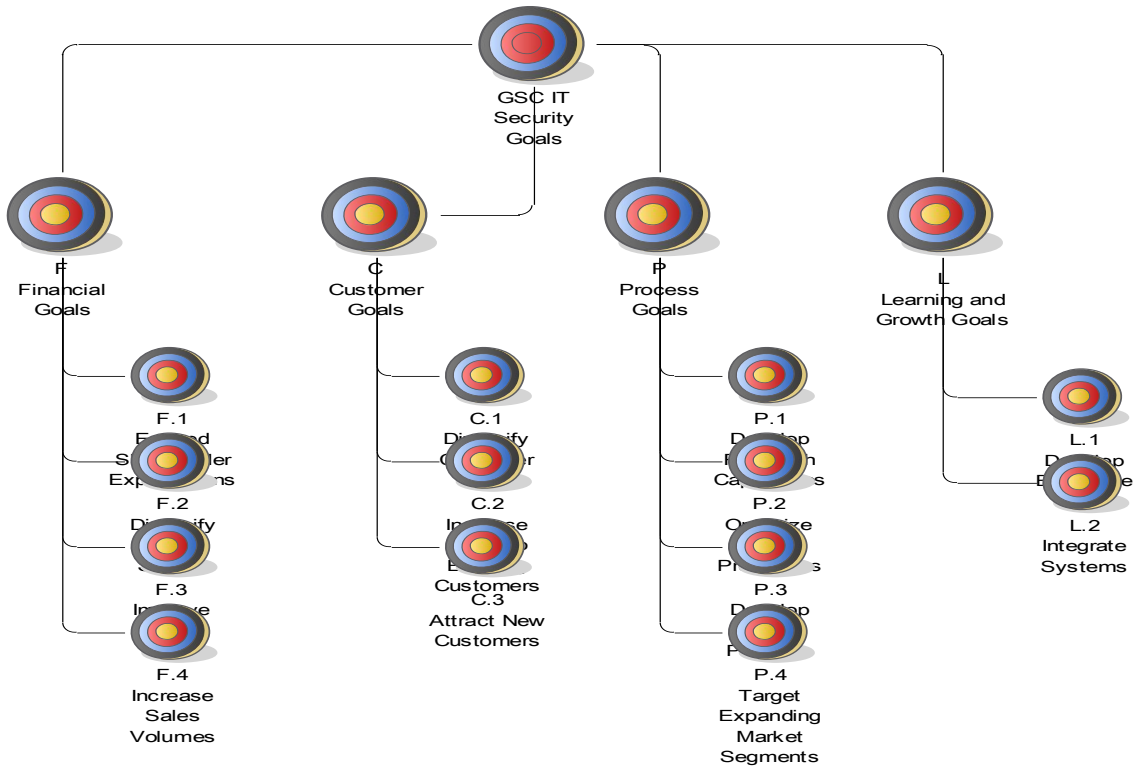


GMC USA Business Process Improvement

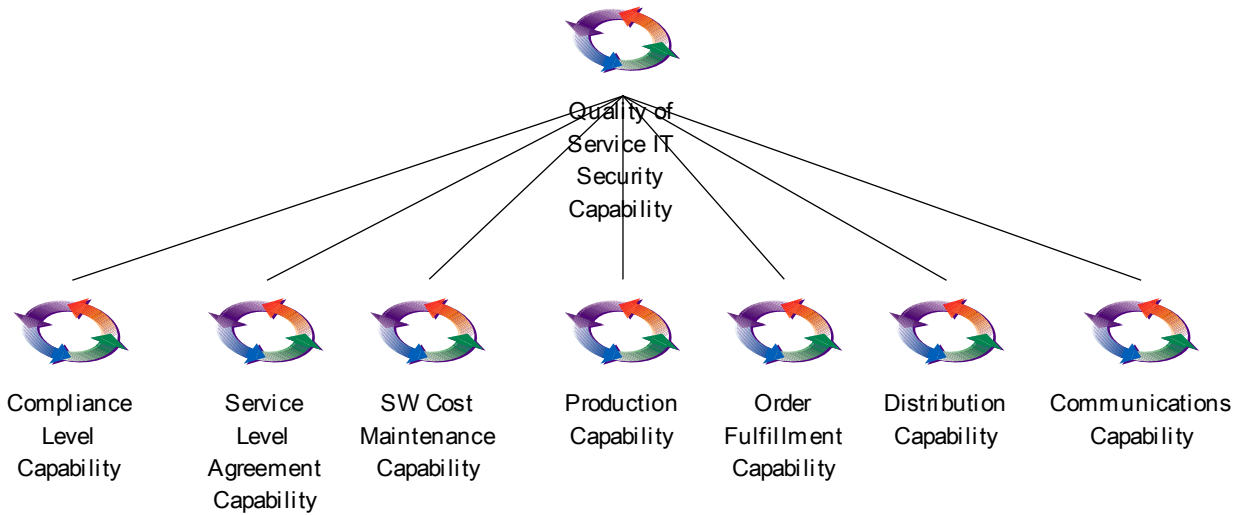


GMC USA Goals

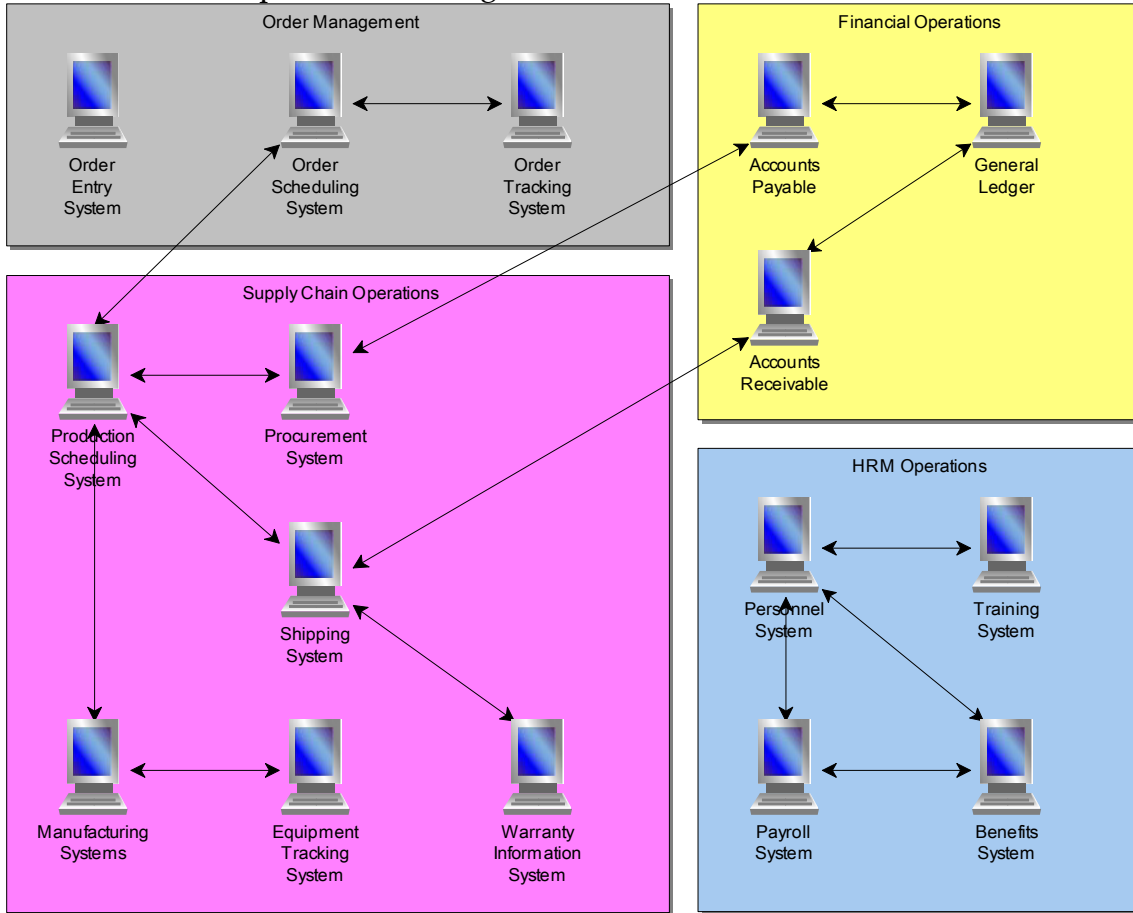
Global Supply Chain IT Security Hosted Services



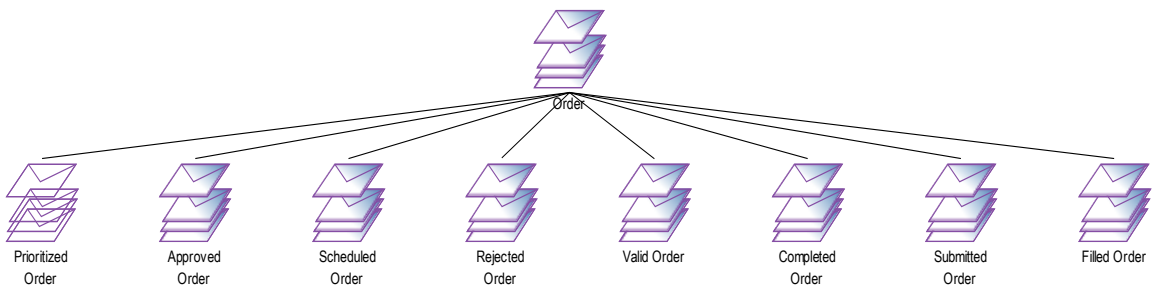
GMC USA Quality of Service Capabilities

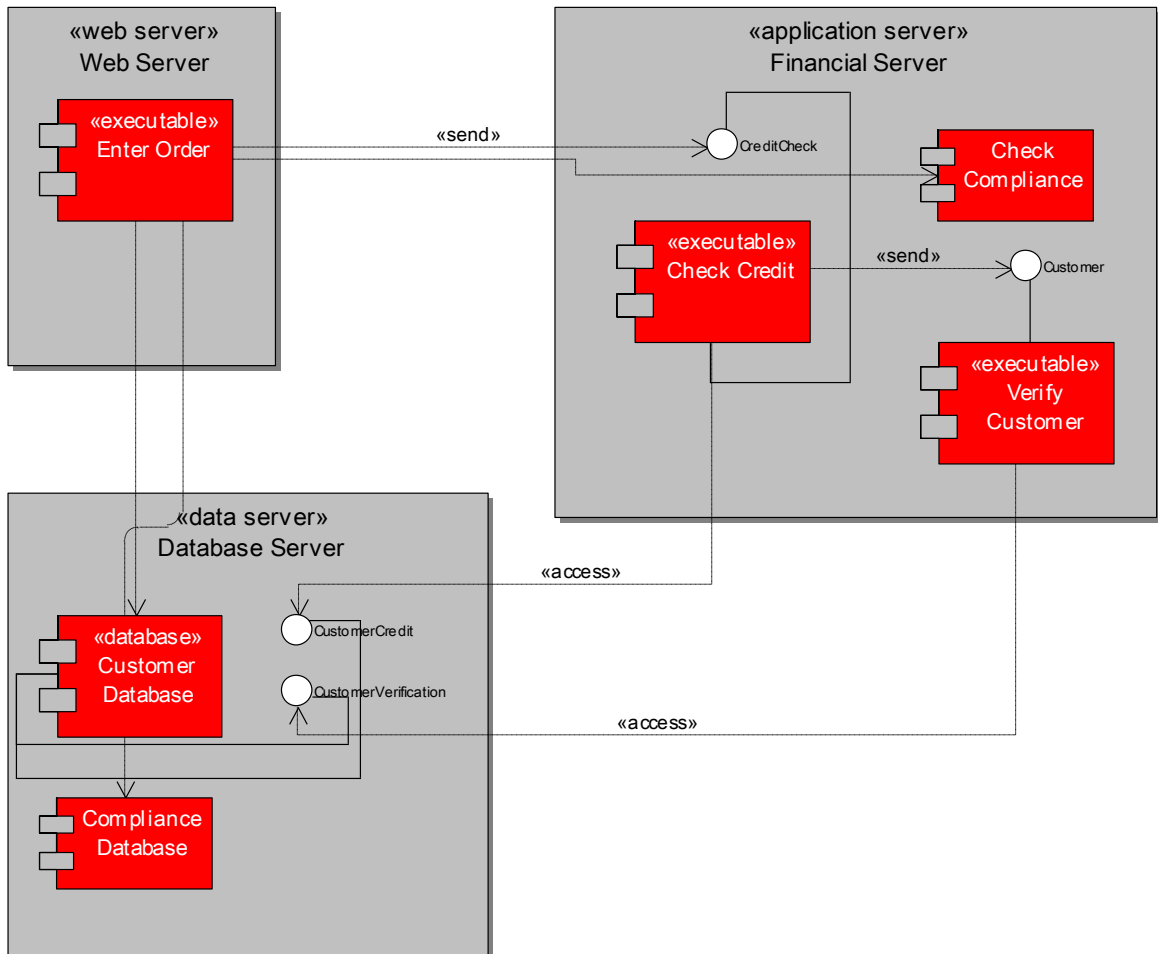


GMC USA GSC Operations Management



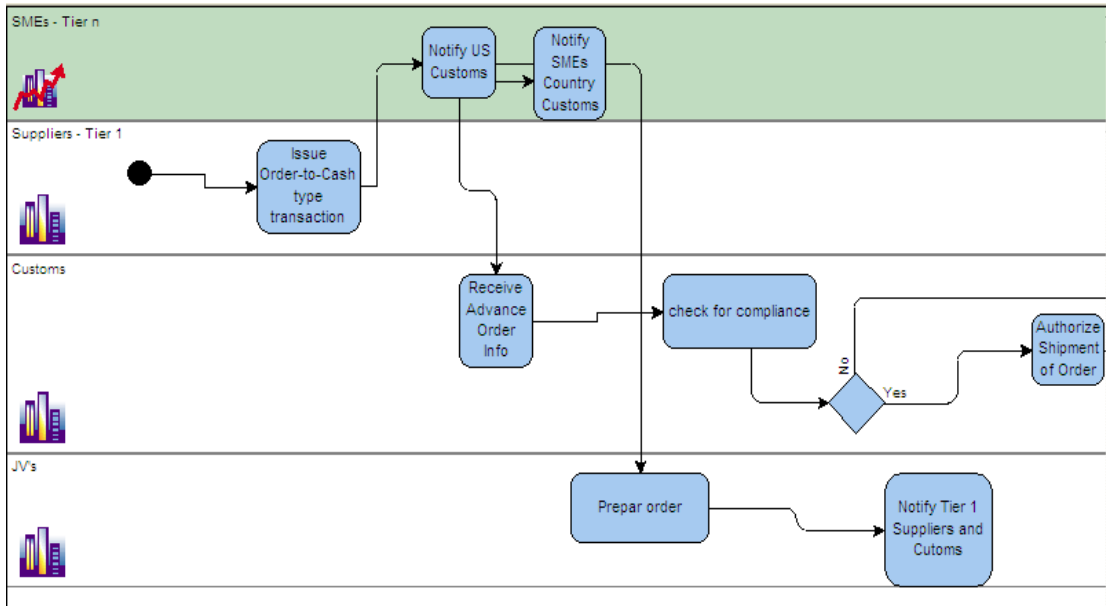
GMC USA Order Processing



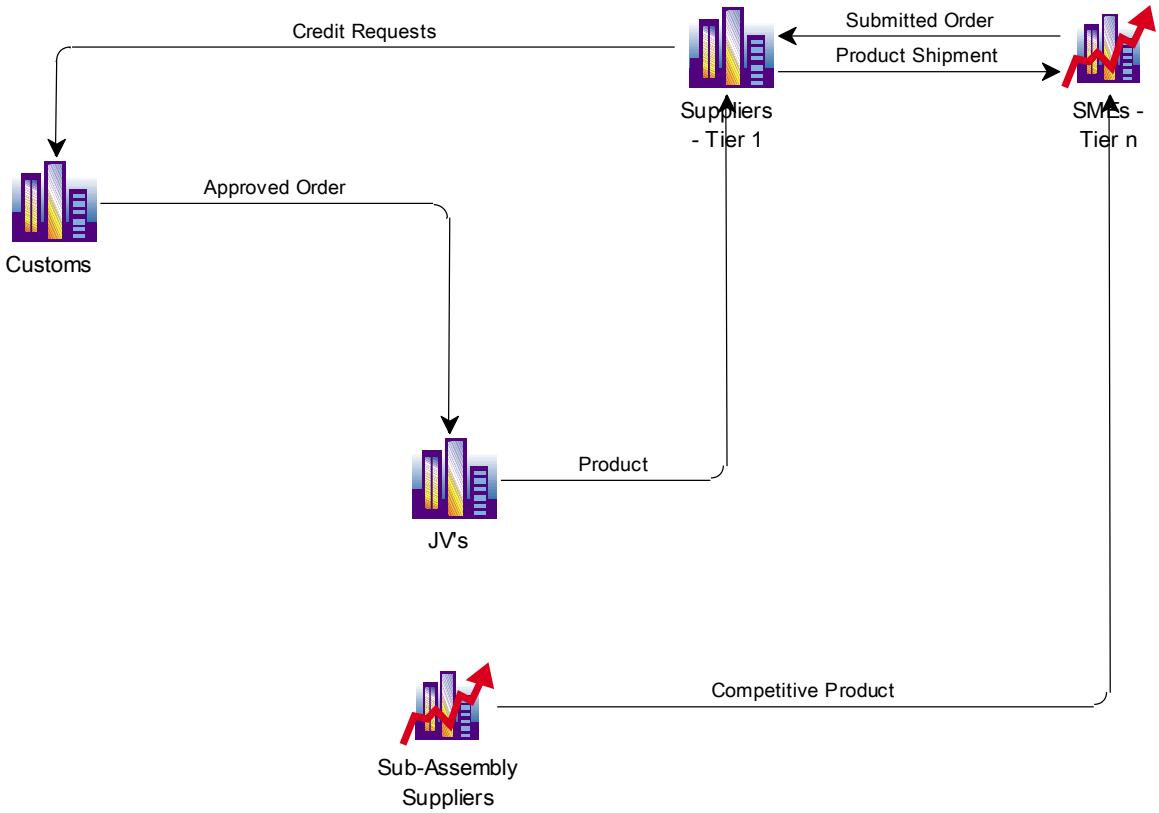


GMC USA Electronic Data Transaction Process

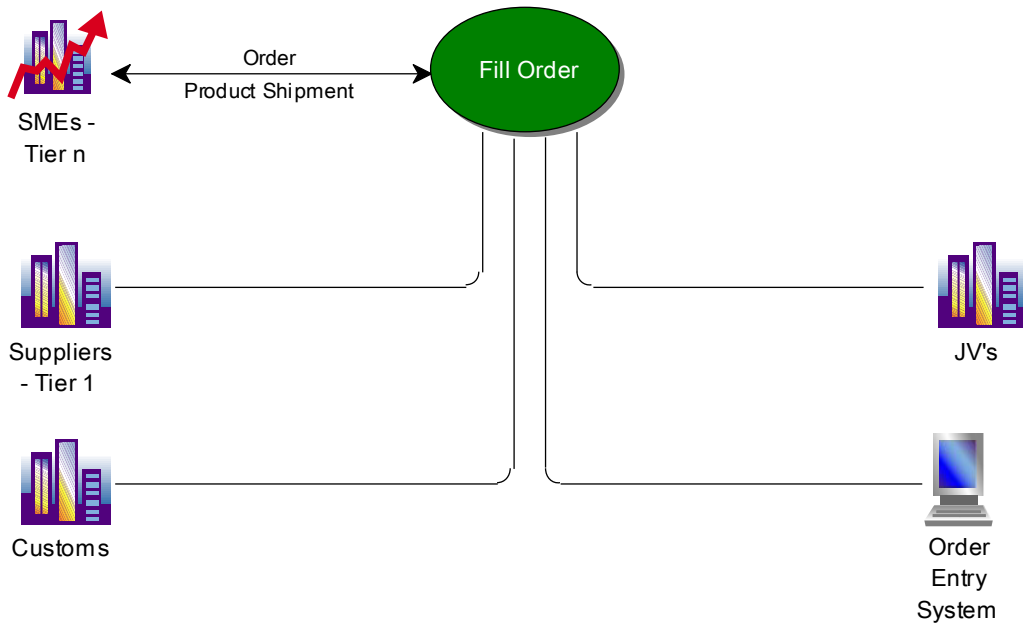
Global Supply Chain IT Security Hosted Services



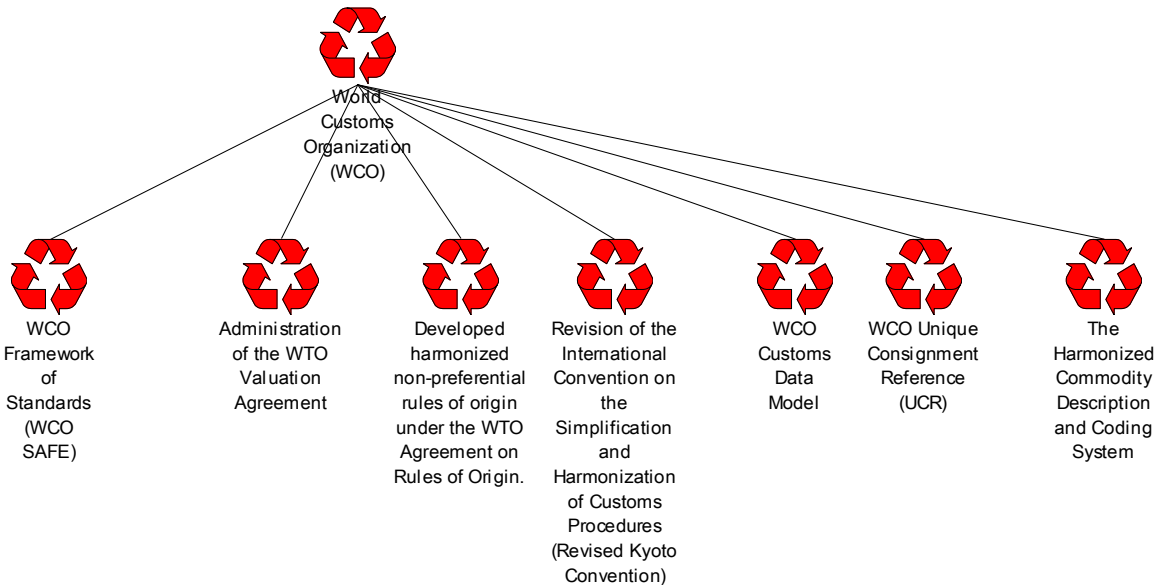
GMC USA PO Processing



GMC USA Fill Order

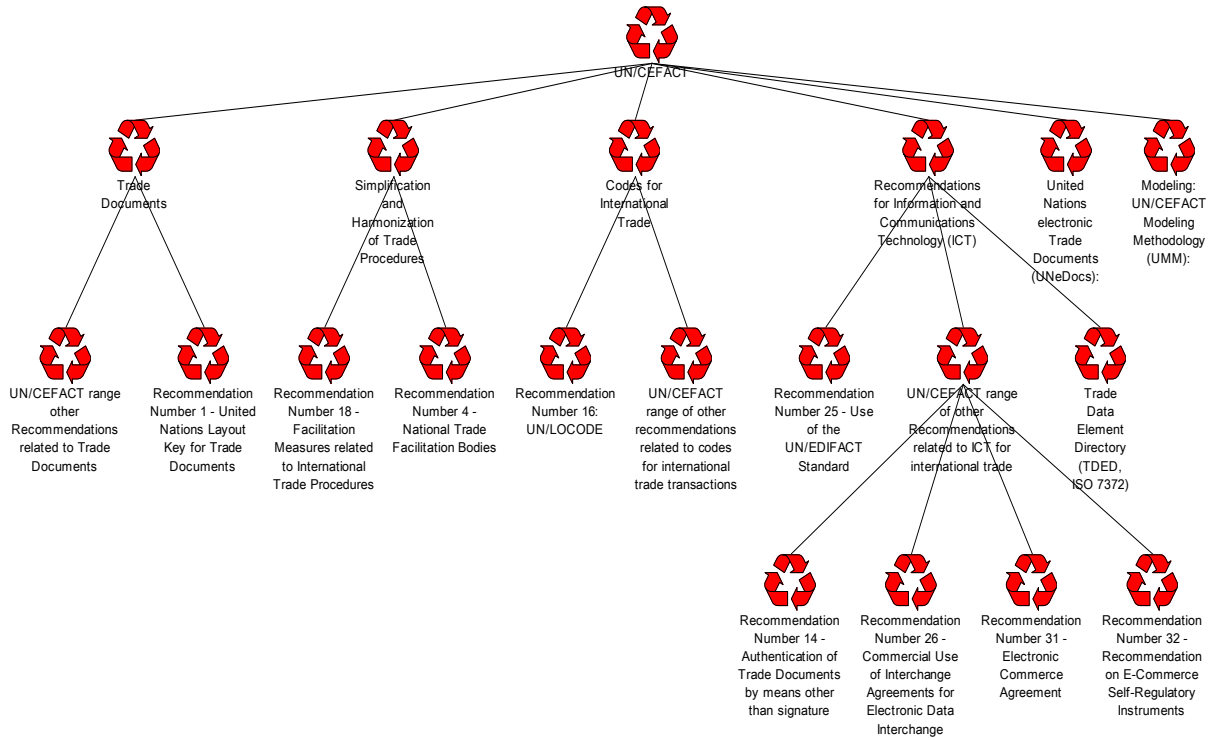


GMC USA WCO Standards

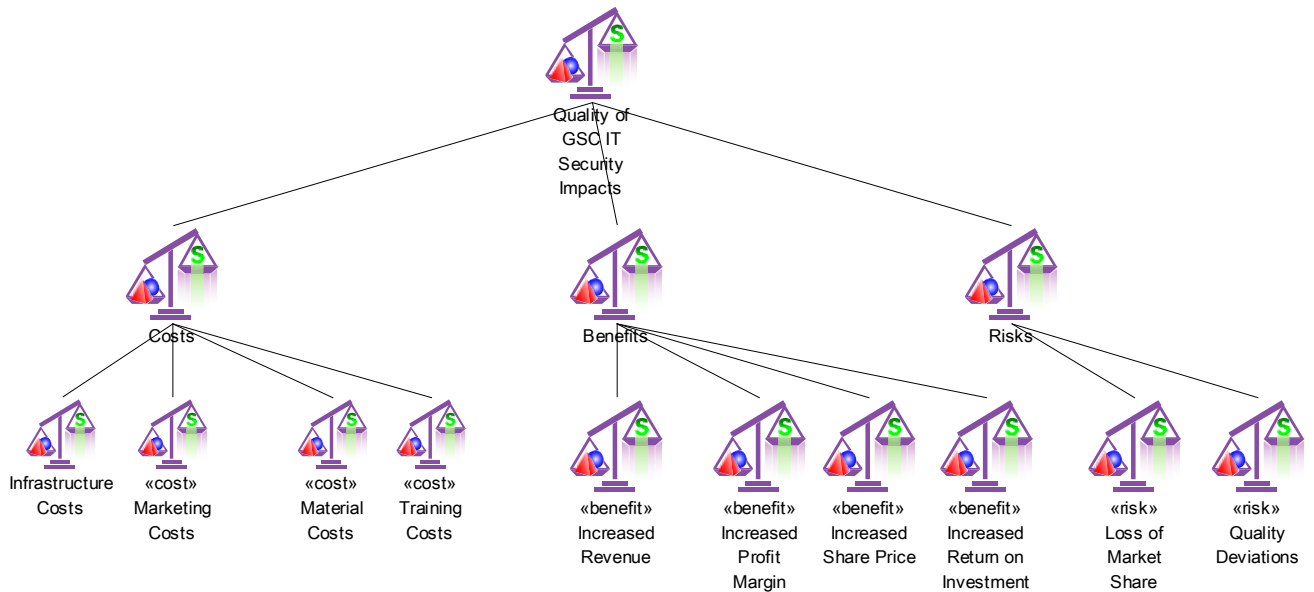


GMC USA UN Standards

Global Supply Chain IT Security Hosted Services

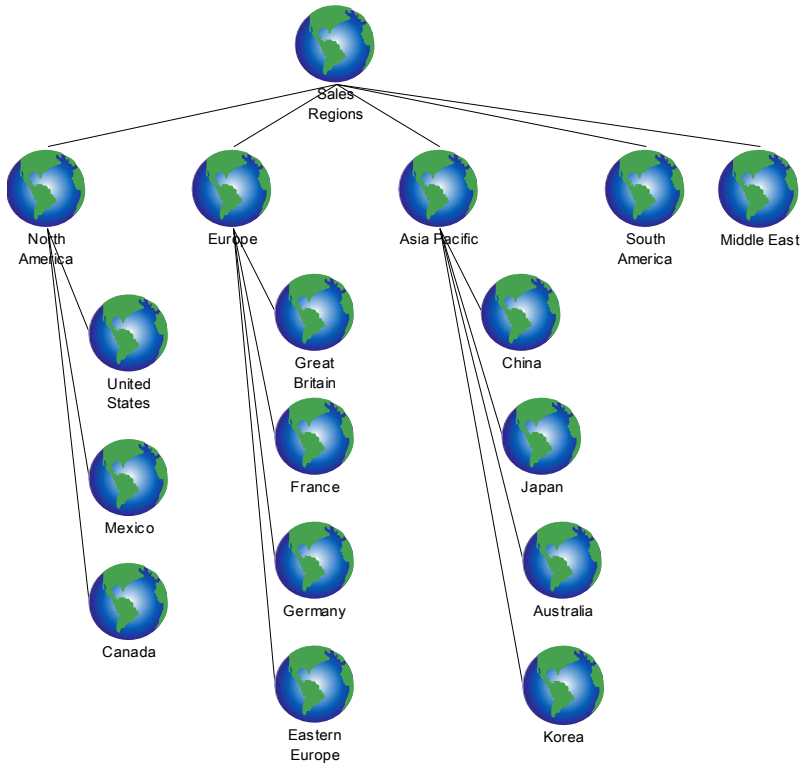


GMC USA Quality of Security Impact

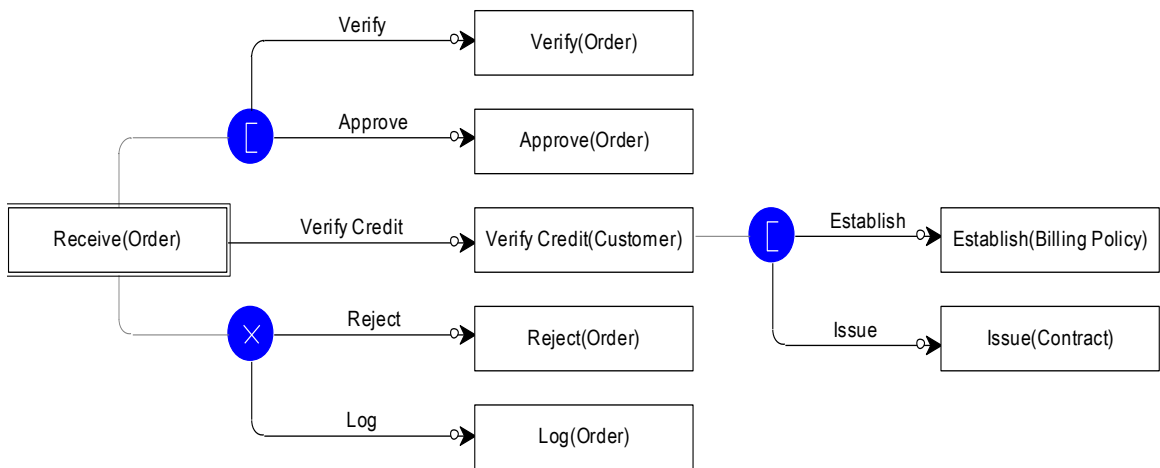


GMC USA Global Location Modeler

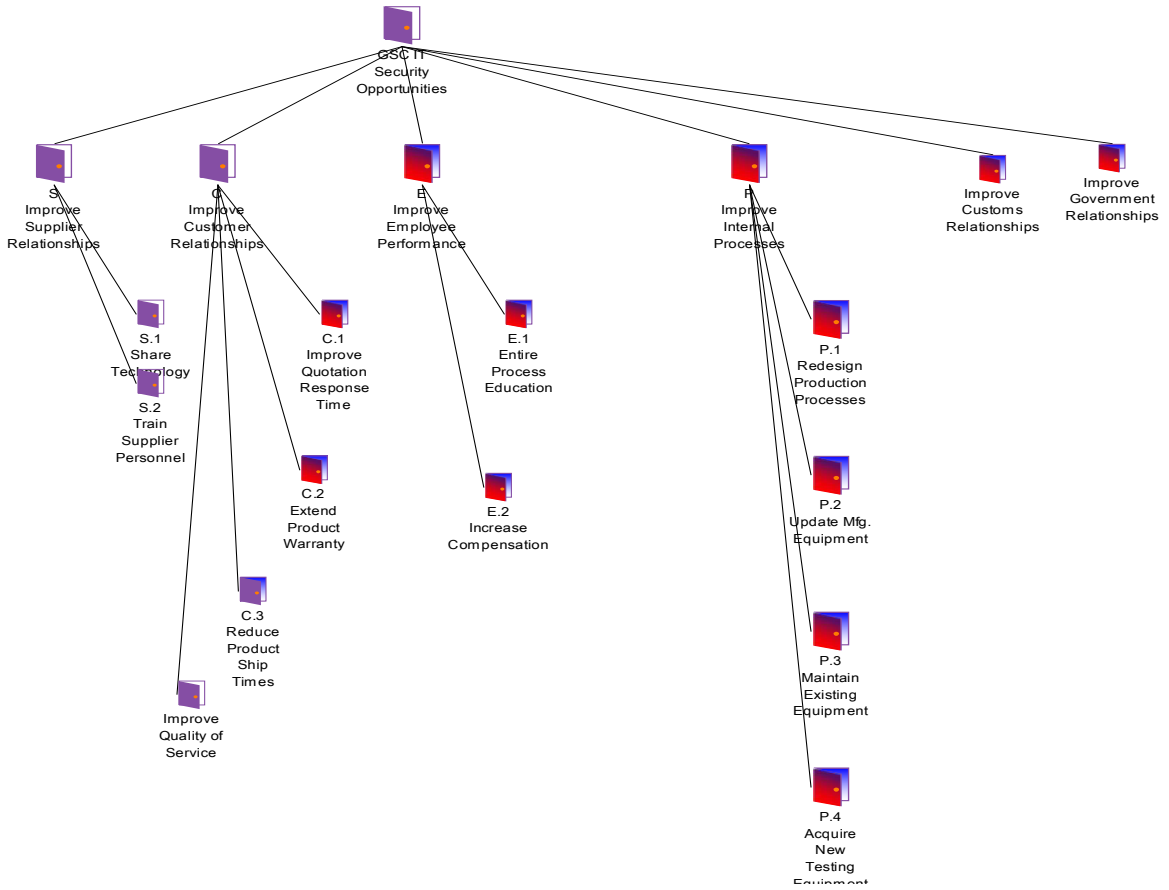
Global Supply Chain IT Security Hosted Services



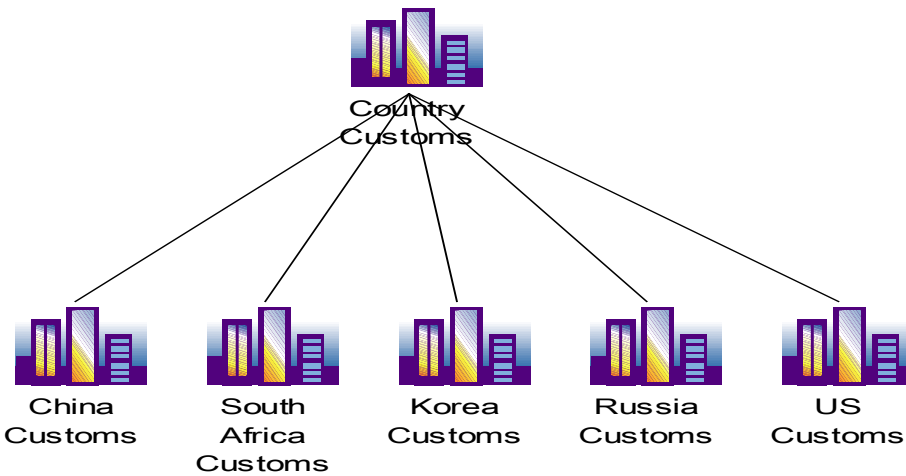
GMC USA Receive Order



GMC USA Opportunities

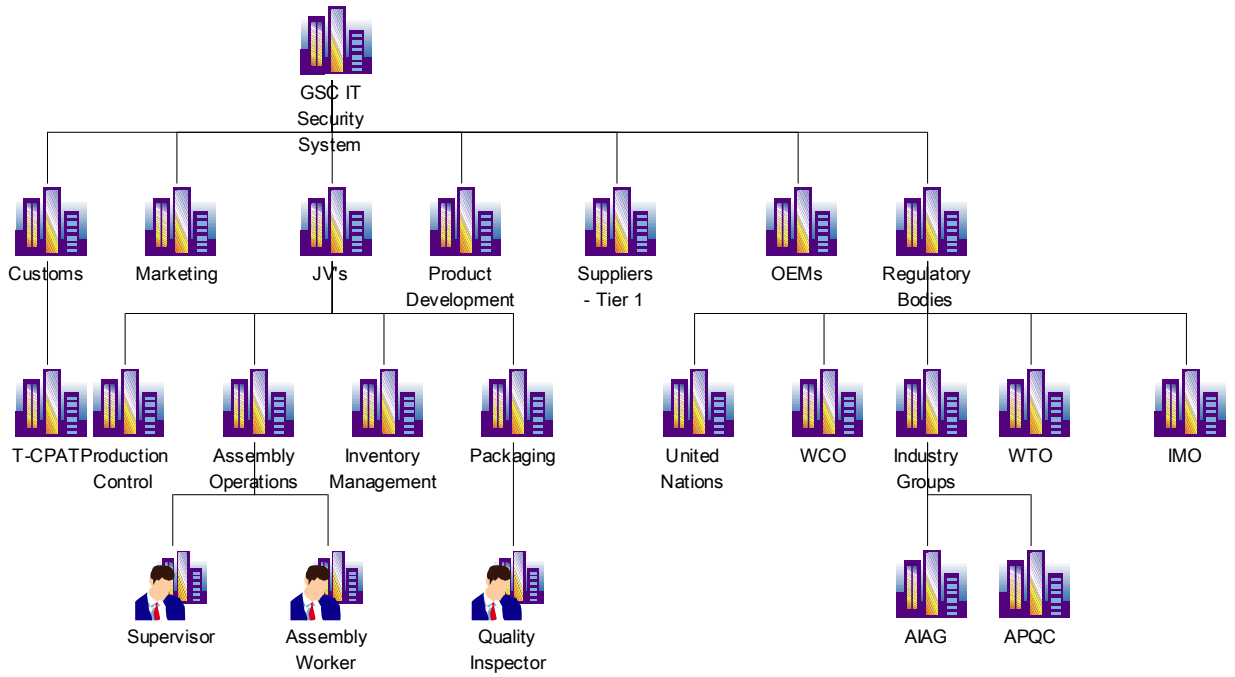


GMC USA Country Customs Organization

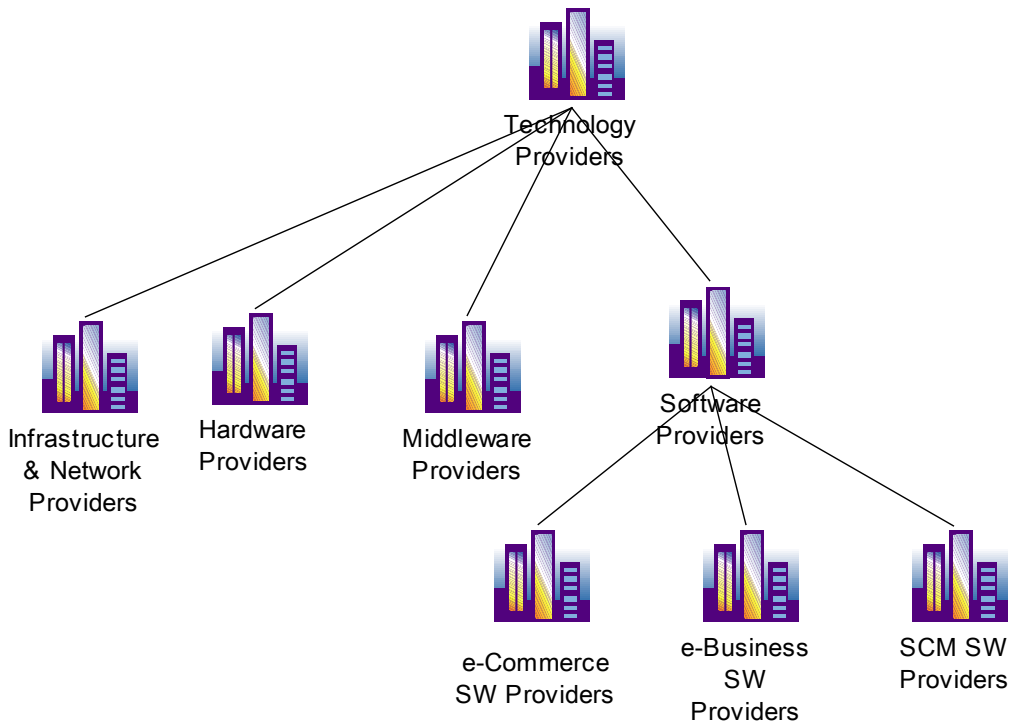


GMC USA System Organization

Global Supply Chain IT Security Hosted Services

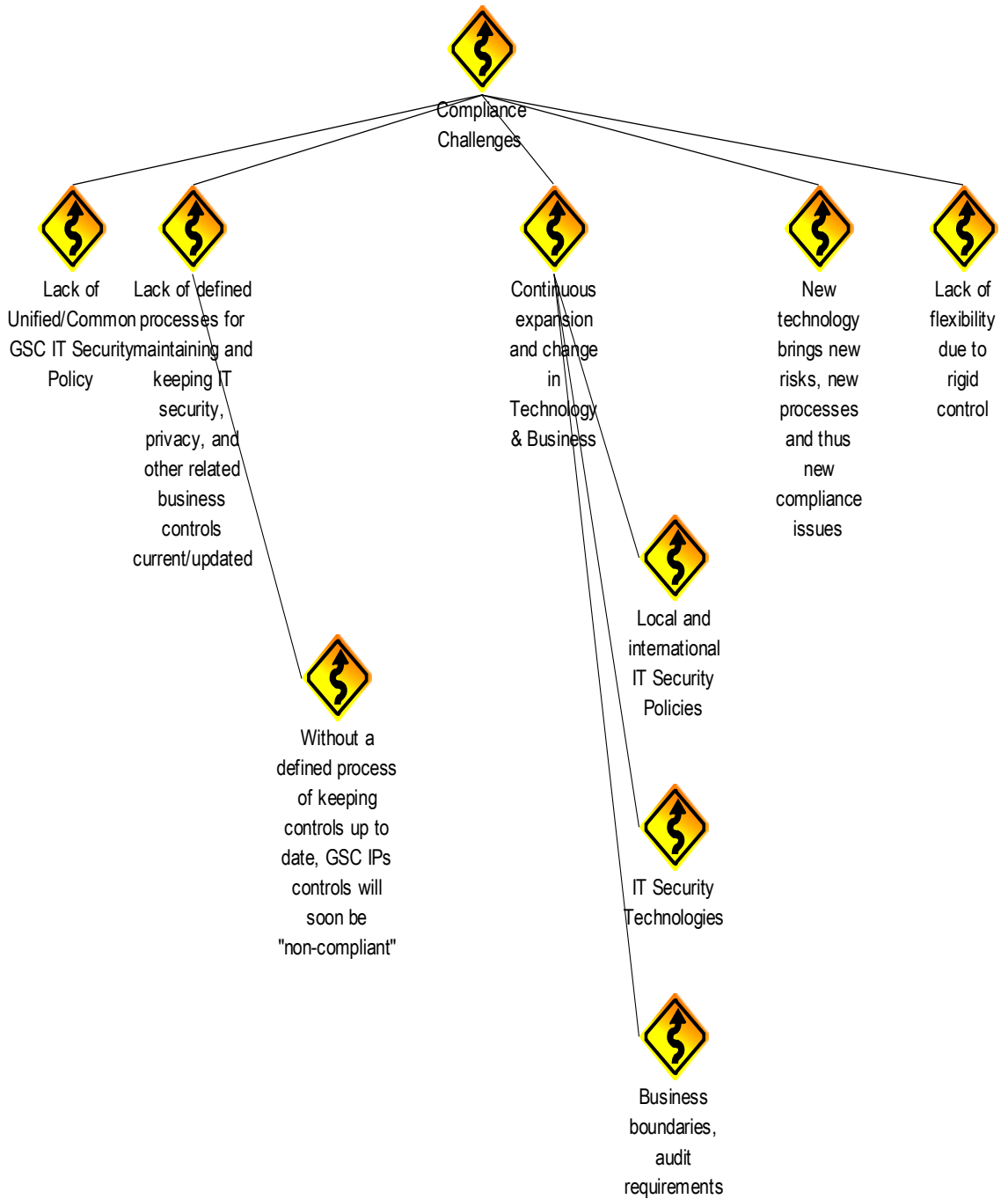


GMC USA Technology Providers Organization



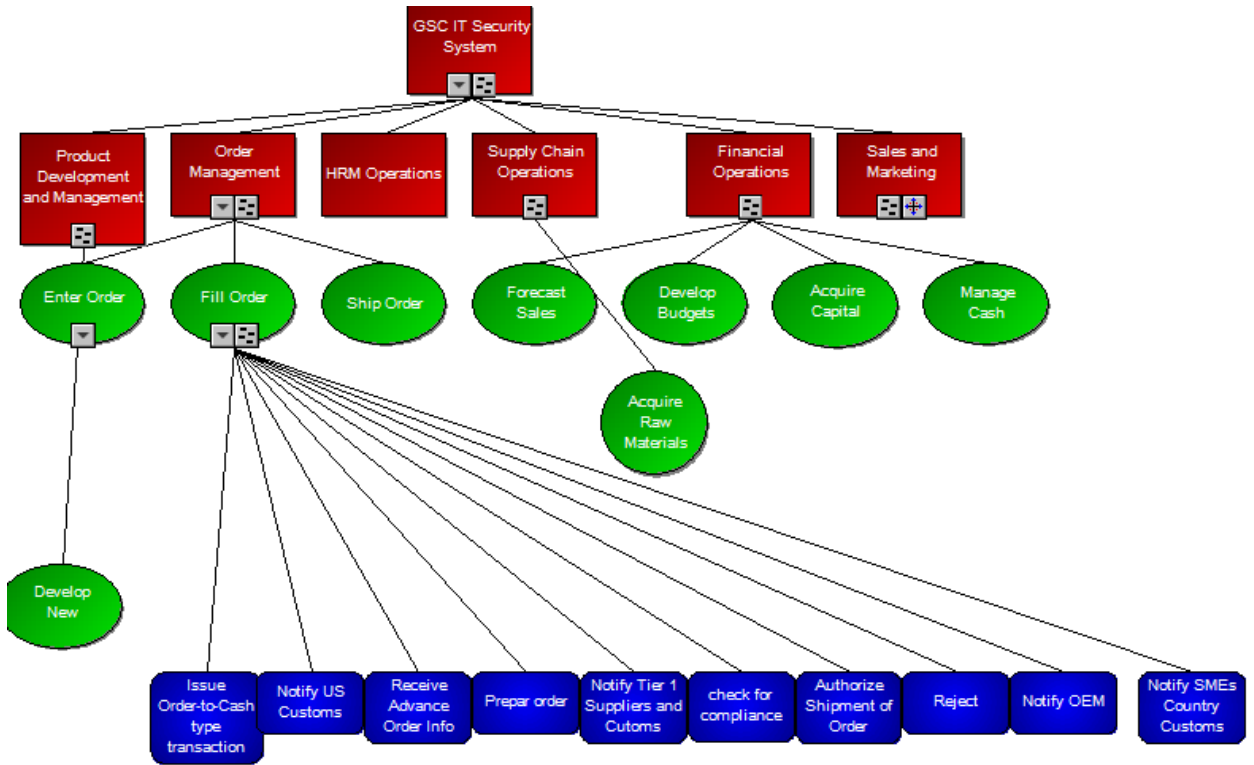
GMC USA Trade Compliance Challenges/Problems

Global Supply Chain IT Security Hosted Services

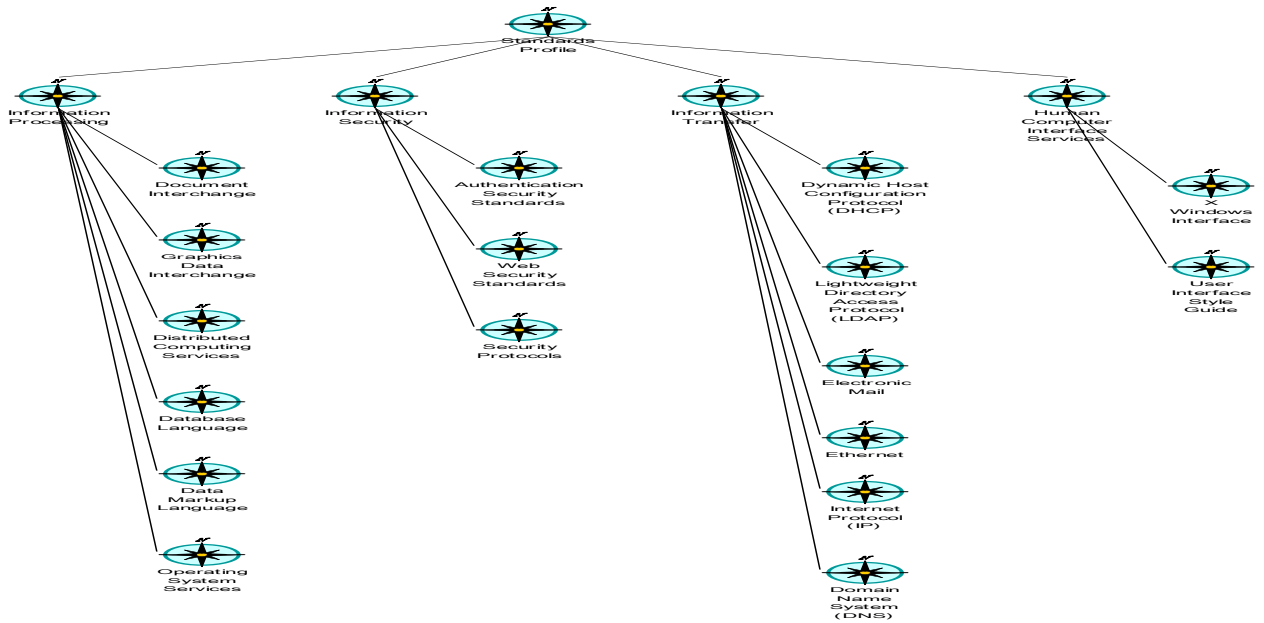


GMC USA GSC IT Security System

Global Supply Chain IT Security Hosted Services

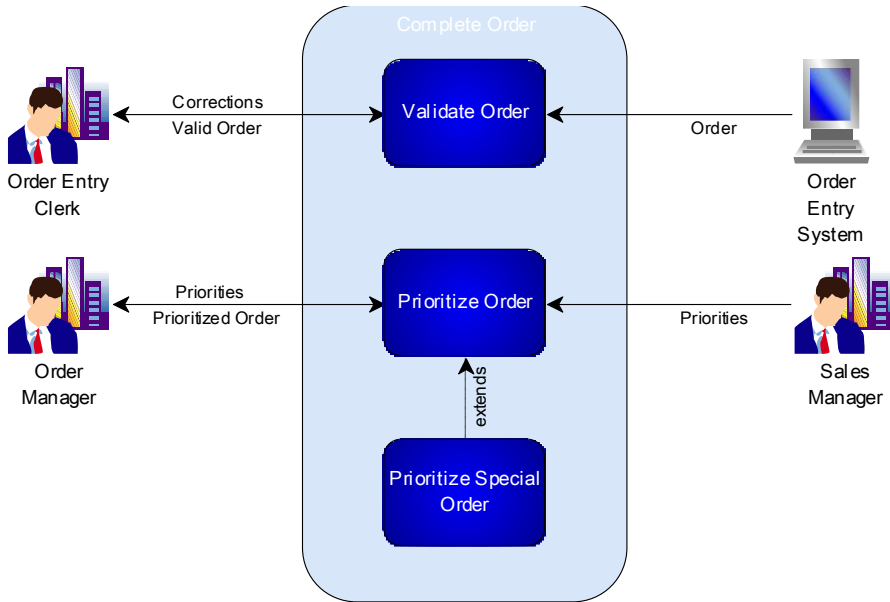


GMC USA Standards Profile

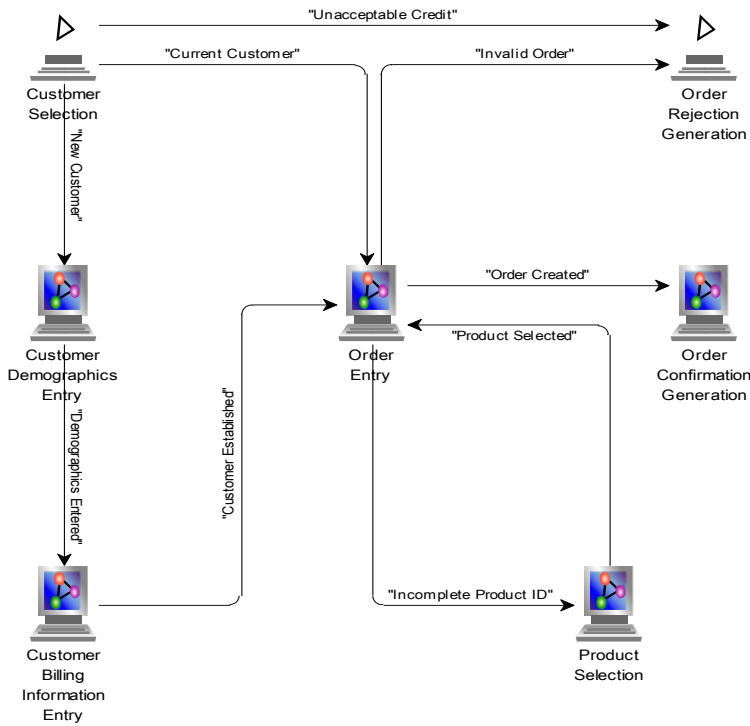


GMC USA Complete Order

Global Supply Chain IT Security Hosted Services

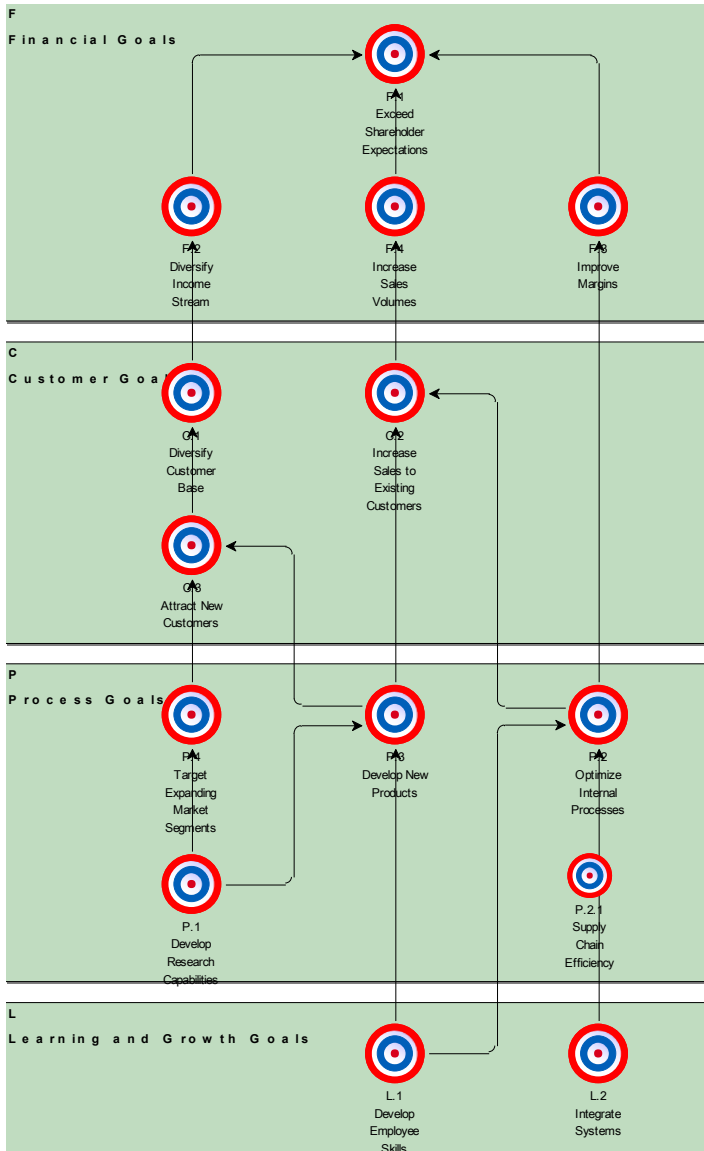


GMC USA Validate Order



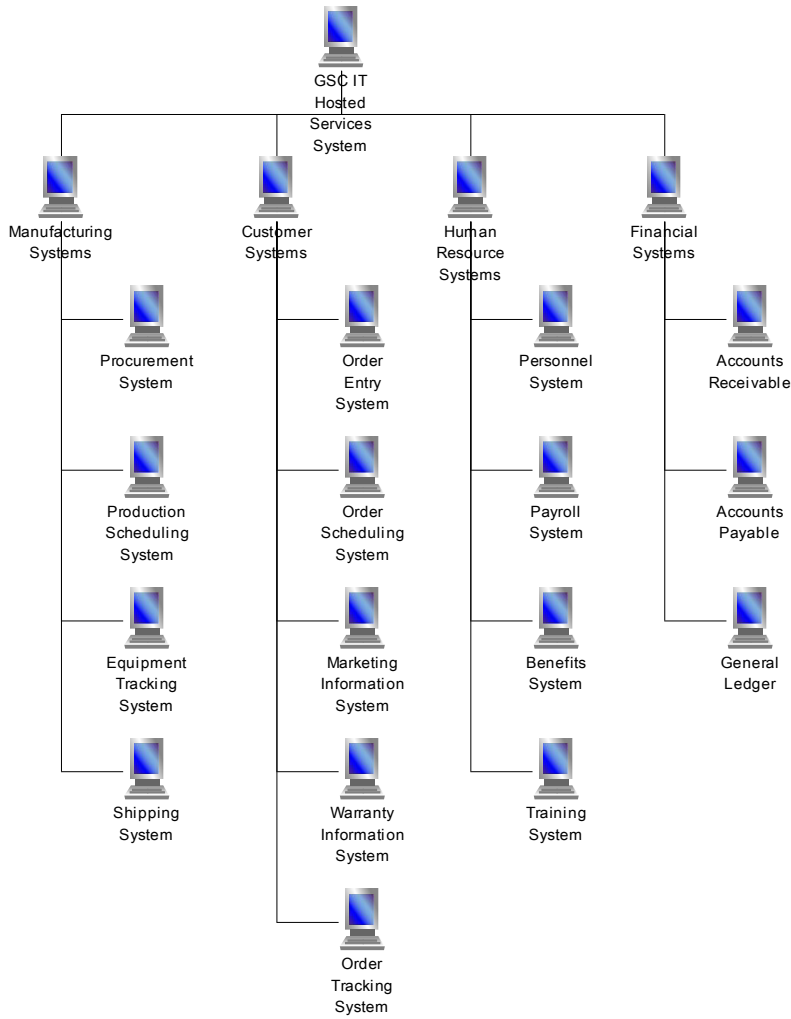
GMC USA Strategy

Global Supply Chain IT Security Hosted Services

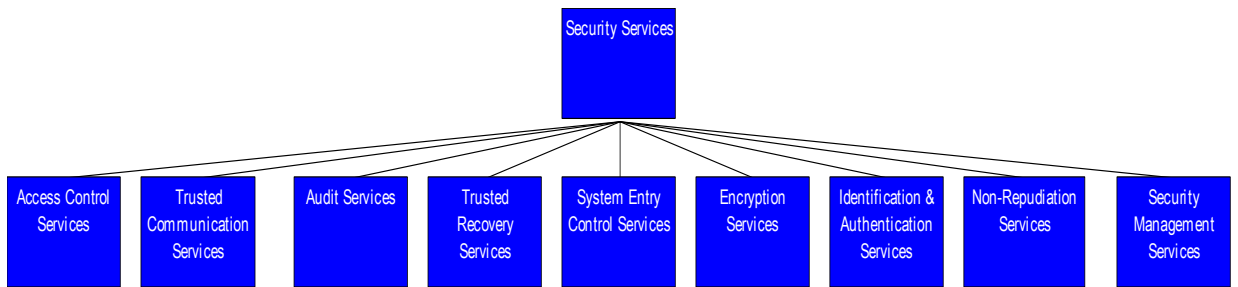


GMC USA GSC IT Hosted Security Services System Modeler

Global Supply Chain IT Security Hosted Services



GMC USA Security Services Modeler



APPENDIX C QUESTIONNAIRE RAW DATA

**IT HOSTED GLOBAL SUPPLY CHAIN SECURITY SERVICES
Improving the Global Supply Chain through Tightening Information Technology Security**

Raw Data from 11 Questionnaires

Interview #	Rankings																				
	Security			Governance			Quality			Procurement			Strategy			Integration			Compliance		
	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U	Y	N	U
1	1	4	0	5	1	1	2	5	2	0	5	0	2	6	1	4	4	2	5	0	0
2	1	4	0	6	1	0	2	4	3	1	4	0	3	4	2	5	3	2	4	1	0
3	0	3	2	7	0	0	1	6	2	0	5	0	2	6	1	6	3	1	2	0	0
4	2	2	1	2	1	0	1	8	0	1	3	1	1	8	0	6	2	2	1	1	0
5	0	4	1	4	3	0	2	6	1	1	4	0	2	7	0	7	2	1	4	1	0
6	0	5	0	6	0	1	2	5	2	0	5	0	3	5	1	5	4	1	4	1	0
7	1	4	0	6	1	0	2	6	1	1	4	1	2	6	1	7	1	2	5	0	0
8	0	5	0	5	2	0	1	6	2	0	4	1	1	7	1	6	3	1	5	0	0
9	0	4	1	3	2	2	0	6	3	2	3	0	2	6	1	5	2	3	4	1	0
10	1	3	1	5	2	0	1	7	1	2	2	1	3	4	2	5	5	0	3	2	0
11	1	4	0	3	3	1	2	6	1	1	4	0	2	7	0	4	4	2	4	1	0

Interview number corresponds to numbers in Table 1 of Dissertation (Interviewee Organizations)

Security Ranking: Number of No's. 5 is highest, 0 is lowest

Governance Ranking: Number of No's. 7 is highest, 0 is lowest

Quality ranking has possibility of 9 as a high score. 9 is highest, 0 is lowest

Procurement ranking has possibility of 5 as a high score. 5 is highest, 0 is lowest

Strategy ranking has possibility of 9 as a high score. 9 is highest, 0 is lowest

Integratio ranking has possibility of 10 as a high score. 10 is highest, 0 is lowest

Compliance Ranking: 5 questions on compliance. Positive answer is 3 to 5, and negative is 1-2.

APPENDIX D GSC STANDARDS & RECOMMENDATIONS

TOOLS AVAILABLE TO ASSIST IN IMPLEMENTING A SINGLE WINDOW

When implementing a Single Window, governments and trade are strongly encouraged to consider the use of relevant recommendations, standards and existing tools that have been developed over the past number of years by intergovernmental agencies and international organizations such as UNECE, UNCTAD, WCO, IMO, ICAO and the ICC. Some of the instruments in this category are described below, listed by the organizations in charge of their use.

UNITED NATIONS CENTRE FOR TRADE FACILITATION AND ELECTRONIC BUSINESS (UN/CEFACT), UNECE

In its capacity as the international focal point for trade facilitation standards and recommendations, UNECE, through its Centre for Trade Facilitation and Electronic Business (CEFACT), develops and maintains instruments meant to reduce, simplify, harmonize and automate procedures, information flow and paperwork in international trade. Some of the main Recommendations in this respect are as follows:

Simplification and Harmonization of Trade Procedures

Recommendation Number 18 - Facilitation Measures related to International Trade Procedures: Contains a series of recommendations regarding the simplification and harmonization of international trade procedures, including specific recommendations regarding the submission of information to governments in relation to the movement of goods. Each section describes the application area, outlines the procedures and documents covered, and describes the particular problems for which facilitation measures are provided.

Recommendation Number 4 - National Trade Facilitation Bodies: Emphasizes the need for a strong government-trade partnership in trade facilitation matters and recommends that Governments establish and support national trade facilitation bodies with balanced private and public sector participation in order to identify issues affecting the cost and efficiency of their country's international trade.

Trade Documents

Recommendation Number 1 - United Nations Layout Key for Trade Documents: Provides an international basis for the standardization of documents used in international trade and transport, including the visual representation of such documents. The UN Layout Key is intended particularly to serve as a basis for designing aligned series of forms employing a master document in a reprographic one-run method of document preparation; it can also be used to develop screen layouts for the visual display of computerized information.

UN/CEFACT has also developed a range of other Recommendations related to Trade Documents, such as Recommendation Number 6 - Aligned Invoice Layout Key, and Recommendation Number 22 - Layout Key for Standard Consignment Instructions.

Codes for International Trade

Recommendation Number 16: UN/LOCODE - Code for Ports and other Locations: Recommends a five-letter alphabetic code for abbreviating the names of locations of interest to international trade, such as ports, airports, inland freight terminals, and other locations where Customs clearance of goods can take place, and whose names need to be represented unambiguously in data interchange between participants in international trade. The UN/LOCODE's code list currently contains 60,000 codes for locations around the world.

UN/CEFACT has also developed a range of other recommendations related to codes for international trade transactions, such as Recommendation Number 19 - Codes for Modes of Transport; Recommendation Number 20 - Codes for Units of Measurement used in International Trade.

Recommendations for Information and Communications Technology (ICT)

Recommendation Number 25 - Use of the UN/EDIFACT Standard: Recommends coordinated action by Governments to promote UN/EDIFACT as the single international standard for electronic interchange of data (EDI) between public administrations and private companies of all economic sectors world-

wide. There are currently over 200 UN/EDIFACT messages available for the exchange of data between organizations.

UN/CEFACT has also developed a range of other Recommendations related to ICT for international trade including:

- Recommendation Number 14 - Authentication of Trade Documents by means other than signature;
- Recommendation Number 26 - Commercial Use of Interchange Agreements for Electronic Data Interchange;
- Recommendation Number 31 - Electronic Commerce Agreement;
- Recommendation Number 32 - Recommendation on E-Commerce Self-Regulatory Instruments.

Trade Data Element Directory (TDED, ISO 7372) contains the standard data elements, which can be used with any method for data interchange on paper documents as well as with other means of data communication. They can be selected for transmission one by one, or used within a particular system of interchange rules, e.g. the UN/EDIFACT. The Directory provides a common language for terms used in international trade and facilitates the interchange of data. UNTDE is a component of aligned, UNLK conform trade documents. The directory has been the basis for the first UN/EDIFACT releases and will be integrated in the future UN/CEFACT core component directory. The WCO data harmonization initiative is based on TDED definitions.

Other Tools for Implementation

United Nations electronic Trade Documents (UNeDocs): is a tool based on the UN Layout Key to provide standard based trade documents in paper and electronic format. Traders and administrators can use the documents either in paper or electronic format depending of their needs. UNeDocs provide precise specification of the form layout and the data requirements. The increased precision facilitates the implementation of efficient and automated procedures. The documents facilitate the transition from paper-based information processing to electronic document exchange. UNeDocs mitigates the digital divide by providing low cost solutions for the digital documents.

Modeling: UN/CEFACT Modeling Methodology (UMM): It is often useful at the development stage of a project to develop a model of the processes involved in submitting import and export information to government. This model can be very useful in understanding the processes and information flows and will assist in the further analysis and development and automation of the project.

WORLD CUSTOMS ORGANIZATION (WCO)

For many years, the WCO has been making progress on the simplification and harmonization of international Customs instruments and procedures. The WCO developed and introduced the Harmonized Commodity Description and Coding System, which is used world-wide as the basis for classifying goods and for the collection of duties and taxes. The WCO is administering the WTO Valuation Agreement and developed harmonized non-preferential rules of origin under the WTO Agreement on Rules of Origin. The WCO has also revised the International Convention on the Simplification and Harmonization of Customs Procedures (the Revised Kyoto Convention).

WCO Revised Kyoto Convention: The Revised Kyoto Convention contains a binding provision for Customs to ensure that where goods must be inspected by Customs and other competent authorities that these inspections are co-ordinated and where possible carried out at the same time. In addition, the Convention also addresses the operation of joint controls at common border crossings, the establishment of juxtaposed customs offices and the sharing of information with other bodies.

WCO Customs Data Model: The WCO Customs Data Model is a harmonized and standardized maximum framework for data requirements for Customs and other official cross-border related purposes. The Customs Data Model supports the operation of single window systems and allows the sharing of information nationally and internationally. The Customs Data Model is based on the UNTDED, applies UN/CEFACT's Modeling Methodology (UMM) and refers to a range of UN, ISO and other international code standards such as the UN/LOCODE. The Customs Data Model contains currently message implementation guidelines only for UN/EDIFACT but will offer XML specifications in future versions.

WCO Unique Consignment Reference (UCR): The WCO UCR is a concept using ISO 15459 (ISO License Plate) compliant numbering systems or equivalent industry solutions such as applied for example in the express carrier industry to uniquely identify consignments in international trade from origin to destination. The UCR establishes an information and documentation link between the supplier and the customer in an international trade transaction and requires this reference to be used throughout the entire supply chain. The UCR has to be linked with the transport references, where the UCR is not already serving also as the transport reference. The UCR can be used as the common access key for national and international data sharing.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD)

The Automated System for Customs Data (ASYCUDA)⁴

ASYCUDA is a computerized customs management system that covers most foreign trade procedures. The system handles manifests and customs declarations, accounting procedures, and transit and suspense procedures. It generates trade data that can be used for statistical economic analysis. The ASYCUDA software is developed in Geneva by UNCTAD and operates on microcomputers in a client server environment. ASYCUDA is fully compliant with international codes and standards developed by ISO (International Organization for Standardization), WCO (World Customs Organization) and the United Nations. ASYCUDA can be configured to suit the national characteristics of individual Customs regimes, national tariffs and legislation. The system also provides for electronic data interchange (EDI) between traders and Customs using EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) rules.

The most recent Web-based version of ASYCUDA will allow Customs administrators and traders to handle most of their transactions via the Internet. The new e-Customs platform, dubbed AsycudaWorld, will be particularly useful to developing countries, where poor fixed-line telecommunications are a major problem for e-government applications. It is also powerful enough to accommodate the operational and managerial needs of Customs operations in

⁴ For more information on ASYCUDA, visit the web-site: www.asycuda.org

any developed country as well. AsycudaWorld will mean even greater tax revenue collection and lower transaction costs than are already provided by the current version of the system, ASYCUDA++, making it a showcase for e-government. A secondary benefit is the provision of information to facilitate measures to combat fraud, corruption and illicit trafficking, as it gives Customs authorities in different countries a tool for working together online.

INTERNATIONAL MARITIME ORGANIZATION (IMO)

IMO addresses the issues related to facilitation of international maritime traffic, through its Facilitation Committee (FAL Committee). These issues include, e.g. simplification of formalities, documentary requirements and procedures on the arrival and departure of ships and harmonization of documents required by the public authorities (standardized IMO FAL Forms). Electronic business in the area of maritime traffic is one of the most important issues, which are currently under discussion in the FAL Committee. IMO has also recognized the pressing need for “a single window concept” and “pre-arrival information” to allow all the information required to be provided for and by a visiting ship to a port, including that required by the public authorities, through one point of entry. Proposed amendments to the Annex to the FAL Convention to specifically address the single window concept, together with other proposed amendments, are under consideration by the FAL Committee.

The Convention on Facilitation of International Maritime Traffic, 1965 (FAL Convention): The Convention on Facilitation of International Maritime Traffic is an international convention that has addressed:

- Facilitation of international maritime traffic;
- Prevention of unnecessary delays to ships, their crews, passengers and cargoes; and
- Unification and simplification of formalities, documentary requirements and procedures.

Amongst others it deals in the Annex, Section 1, C with electronic data-processing techniques for exchange of information.

The IMO Compendium on Facilitation and Electronic Business (FAL.5/Circ.15, dated 19 February 2001 and FAL.5/Circ.15/Corr.1): International guidance that

has been developed for exchange of information electronically and electronic means for the clearance of ships.

INTERNATIONAL CHAMBER OF COMMERCE (ICC)

ICC creates rules, norms, standards and tools for international trade. Though voluntary, ICC rules carry the force of law when incorporated into contracts and countries throughout the world abide by them because they have become indispensable in facilitating and harmonizing international trade procedures and contracts across borders.

ICC/UNCTAD Rules for Multimodal Transport Documents:

ICC/UNCTAD Rules set the only globally accepted standard for multimodal transport documents and frequently provide a basis for national legislation. Intended to avoid the problems that would arise for transporters from having to cope with a multiplicity of different regimes when drawing up contracts, the rules offer a uniform legal regime for private transport contracts and simplified documentation and practice.

EXHIBIT ONE WCO SAFE FRAMEWORK PILLAR 1 STANDARDS

Standard 6 – Advance Electronic Information: The Customs administration should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place.

Standard 7 – Targeting and Communication: Customs administrations should provide for joint targeting and screening, the use of standardized sets of targeting criteria, and compatible communication and/or information exchange mechanisms; these elements will assist in the future development of a system of mutual recognition of controls.

Standard 9 – Security Assessments: The Customs administration should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and to commit to resolving identified gaps expeditiously.

Standard 4 – Risk-Management Systems: The Customs administration should establish a risk-management system to identify potentially high-risk shipments and automate that system. The system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices.

Standard 5 – High-risk Cargo or Container: High-risk cargo and container shipments are those for which there is inadequate information to deem shipments as low-risk, that tactical intelligence indicates as high-risk, or that a risk-scoring assessment methodology based on security-related data elements identifies the shipment as high-risk.

Standard 11 – Outbound Security Inspections: The Customs administration should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.

EXHIBIT TWO WCO SAFE FRAMEWORK PILLAR 2 STANDARDS

Standard 1 – Partnership: Authorized Economic Operators involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments and containers until they are released from Customs control at destination.

Standard 2 – Security: Authorized Economic Operators will incorporate pre-determined security best practices into their existing business practices.

Standard 3 – Authorization: The Customs administration, together with representatives from the trade community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as Authorized Economic Operators.

Standard 4 – Technology: All parties will maintain cargo and container integrity by facilitating the use of modern technology.

Standard 5 – Communication: The Customs administration will regularly update Customs-Business partnership programs to promote minimum security standards and supply chain security best practices.

Standard 6 – Facilitation: The Customs administration will work co-operatively with Authorized Economic Operators to maximize security and facilitation of the international trade supply chain originating in or moving through its Customs territory.

EXHIBIT THREE RECOMMENDED BEST PRACTICES

The purpose of showing these best practices is to emphasize the need for consistent interpretation of the data fields across logistics documents between carriers and trading partners. This table was adopted from the AIAG MOSS project.

Processes		WCO ID	Data Keys
Supplier Ship	INVOIC/801 CUSDEC DESADV/856 EX2	Commercial Invoice Customs Invoice Ship Notice Export Documentation	Purchase Ref. Part Number
Trans/Consol	204 TENDER 214 STATUS RECADV/861 CDESADV856 IFCSUM/325 315	Request Pickup Pickup Executed Receipt Advice Consolidated Ship Notice Consol Cont. Manifest Depart Consol Center	Part No/Packaging Case Ocean Container Ocean Carrier
Export Process	IFTMBF/300 IFTMBC/301 IFTMIN/304 EX1, EX2 CURSES	Ocean Booking Ocean Booking Conf Ocean Shipping Instruct Export Customs Declar Export Customs Status	Ocean Container Ocean Carrier Voyage Number
Ocean Depart	CODECO/322 COARRI/322 IFSTA/315 CUSCAR/309/311 ?	In Gate Arrive Container Loaded OC In gate /Loaded on Ship NA Customs Manifest Vessel Departure	Ocean Container Ocean Carrier Voyage Number
Ocean Arrive	IFTMCS/310 IFTMAN/312 404 COARRI/322 CODECO/322 IFTSTA/315	BOL Instruction Arrival Notice Rail BOL Cont Discharge from Ship Cont Out Gate OC Cont Discharge/Out Gate	Ocean Container Ocean Carrier Voyage Number
Import Process	CUSCAR/309 355 CAMIR/350 CUSDEC/CATAIR/ CURSES 358 353/357 CF7533	Customs Manifest Customs Accept/Reject Customs Manifest Status Customs Entry Customs Truck/Train Mani Customs Advisory Truck Manifest (CAN-US)	Ocean Container Ocean Carrier Voyage Number Part No/Packaging Case Carrier/Trailer No.
Inland Transport	204 214(a) 214(b) 214(c)	Load Tender Status Status Status	Ocean Container Train Schedule No. Carrier/Trailer No.
Received	RECADV/861	Received at Destination	Ocean Container Carrier/Trailer No. Part No/Packaging Case

GLOSSARY

Acceptable Use Policy — A policy that outlines what the organization considers to be the appropriate use of company resources such as computer systems and networks.

Access controls — Mechanisms or methods used to determine what access permissions subjects (such as users) have for specific objects (such as files).

Algorithm — A step-by-step procedure, typically an established computation for solving a problem within a set number of steps.

Asset — Resources or information an organization needs to conduct its business.

Audit files — Files containing records that show who accessed a computer system and what operations he or she has performed during a given period of time.

Auditing — The name given to any set of actions or processes used to verify the assigned privileges and rights of a user, as well as any capabilities used to create and maintain a record showing who accessed a particular system and what actions they performed.

Authentication — The process by which a subject's (such as a user's) identity is verified.

Availability — Part of the CIA of security. Availability applies to hardware, software, and data. All of these should be present and accessible when the subject (the user) wants to access or use them.

Biometrics — An access control mechanism in which a physical characteristic, such as a fingerprint or the geometry of an individual's hand, is used to identify users uniquely.

Bluetooth — A wireless technology designed as a short range (approximately ten meters) Personal Area Network (PAN) cable replacement technology that may be built into a variety of devices such as mobile phones, PDAs, and laptop computers.

Bridge — A device used to segregate sections of a LAN based on layer 2 addresses.

Certificate — A cryptographically signed object that contains an identity and a public key associated with this identity. The certificate can be used to establish identity, analogous to a notarized written document.

Change control board — A body that oversees the change management process. Enables the management to oversee and coordinate projects.

Confidentiality — Part of the CIA of security. Refers to the security principle that states that information should not be disclosed to unauthorized individuals.

Configuration items — Assets identified during configuration identification and which need to be managed or controlled.

Control — A measure taken to detect, prevent, or mitigate the risk associated with a threat.

Cookie — Information stored on a user's computer by a Web server to maintain the state of the connection to the Web server. It is used so that preferences or previously used information can be recalled on future requests to the server.

Critical infrastructures — Those infrastructures whose loss would have a severe detrimental impact on the nation.

Cryptography — The art of secret writing that enables an individual to hide the contents of a message or file from all but the intended recipient.

Denial-of-Service (DoS) attack — An attack designed to prevent resources from being used for their intended purpose.

Digital certificate — A digital document that establishes an association between users and their public keys.

Disaster recovery plan (DRP) — A written plan that addresses how an organization will react to a natural or man-made disaster in order to ensure business continuity. Related to the concept of a business continuity plan (BCP).

Diversity of defense — The approach of creating dissimilar security layers so that an intruder who is able to breach one layer will be faced with an entirely different set of defenses at the next layer.

DMZ (demilitarized zone) — An area between the Internet and intranet, separated by firewalls.

Due diligence — The legal duty of investigating and ensuring that due care has been taken.

Encryption — The art of obscuring data by making it cryptic (as in scrambling data).

European Union (EU) — A governmental association of the states that comprise the countries of Europe.

Evidence — The documents, verbal statements, and material objects admissible in a court of law.

Extranet — An extension of a company's intranet functionality to select groups of people for specific business purposes.

Forensics — The preservation, identification, documentation, and interpretation of computer data for use in legal proceedings.

FTP — File Transfer Protocol is an application level protocol used to transfer files over a network connection.

Group — A group of users with a common, shared criteria or trait.

Guidelines — Recommendations relating to a policy. These are not mandatory steps.

Hardening — The process of securing and preparing a system for the production environment.

Hub — A device that makes connections between devices at the physical layer.

Impact — The result of a vulnerability being exploited by a threat, resulting in a loss.

Incident response — The process of responding to, containing, analyzing, and recovering from an incident.

Integrity — Part of the CIA of security, the security principle which requires that information is not modified except by authorized individuals.

Internet — The global connection of networks.

Intranet — An internal network utilizing TCP/IP protocols, but limited to direct company personnel access.

Intrusion detection system — A system to identify suspicious, malicious, or undesirable activity that indicates a breach in computer security.

Key management — The process that keeps the shared secrets from being exposed to unauthorized parties.

Layered security — An approach to security which provides multiple layers of protection so that if one layer is breached, other protective layers still exist to defeat the attacker.

Local Area Network (LAN) — A small, typical local network covering a relatively small area such as a single floor of an office building.

Malware — Also known as malicious code, malware refers to software that has been designed for some nefarious purpose.

Network — A group of two or more devices linked together to share data and resources.

Network security — Places an emphasis on controlling access to internal computers from external entities.

Packet — A small chunk of data transmitted from one device to another.

Password policy — A policy that covers all aspects of password management, such as password selection criteria, aging, lockouts, rotation, and dissemination.

Patch — A formal, usually large, software update that may address one or more software problems.

Permissions — Authorized actions a subject can perform on an object. Also, see access control.

Physical security — Consists of all mechanisms used to ensure that physical access to computer systems and networks is restricted only to authorized users.

PKI — Infrastructure for binding a public key to a known user through a trusted intermediary, typically a certificate authority.

Policies — High-level statements made by the management laying out the organization's position on some issues.

Privacy Policy — A policy that explains the guiding principles for guarding personal data that an organization has been given access to.

Procedures — Step-by-step instructions that describe exactly how employees are expected to act in a given situation or to accomplish a specific task.

Protocol — An agreed-upon format for exchanging information between systems.

Risk — The possibility of suffering harm or loss.

Risk assessment (or risk analysis) — The process of analyzing an environment to identify the threats, vulnerabilities, and mitigating actions to determine (either quantitatively or qualitatively) the impact of an event that would affect a project, program, or business.

Risk management — Overall decision-making process of identifying threats and vulnerabilities and their potential impacts, determining the costs to mitigate such events, and deciding what actions are cost-effective to control these risks.

Role — A job or set of job functions and responsibilities needed to perform specific tasks (for example, backup operator).

Router — A device used to direct traffic across a network based on layer 3 addresses.

Routing — The process of moving packets from the source to the destination across multiple networks.

Sarbanes-Oxley Act — Congressional law designed to combat issues of corporate governance and responsibility.

Security Policy — A high-level statement produced by the senior management that outlines what security means to the organization and what the organization's goals are to ensure security.

Server — A machine that provides services to multiple users on a network.

Service level agreements (SLAs) — Contractual agreements between entities describing specified levels of service that the servicing entity agrees to guarantee for the customer.

Service pack — A bundled set of software updates, fixes, and additional functions contained in a self-installing package.

SOAP (Simple Object Access Protocol) — A method of remote object access.

Social engineering — The art of deceiving another individual to obtain confidential information. This is often accomplished by posing as an individual who should be entitled to have access to the information.

Software exploitation — An attack that takes advantage of bugs or weaknesses in software.

Standards — Accepted specifications providing specific details on how a policy is to be enforced.

Switch — A device used to direct traffic in a network based on layer 2 addresses.

Threat — Any circumstance or event with the potential to cause harm to an asset.

URL (Uniform Resource Locator) — A unique Internet address for a resource.

Use case — A set of sample inputs and known correct responses to use in the testing of a section of functionality, whether module, subsystem, system, or application.

User — An individual that uses a computer or information system.

UserID — A unique alphanumeric identifier that identifies individuals when logging on or accessing a system.

Virtual Private Networks (VPN) — An encrypted network connection across another network, offering a private communication channel across a public medium.

Virus — A piece of malicious code that replicates by attaching itself to another piece of executable code.

Vulnerability — Characteristic of an asset that can be exploited by a threat to cause harm.

Web Service — A remote procedure invoked on a remote computer via common data formats and protocols.

Wide area network (WAN) — A computer network that spans a large geographic area, such as a network connecting offices in different cities.

Workstation — Typically, a client or end-user machine attached to a network.

Worm — A piece of code that attempts to propagate through penetration of networks and computer systems.

XML (Extensible Markup Language) — A protocol for describing data.

REFERENCES

- AbuKhalil, A. (2002), Bin Laden, Islam & America's New "War on Terrorism", Publishers Group West, retrieved from <http://angryarab.blogspot.com>
- ACS Publications, (2006), Direct Sampling of Chemical Weapons in Water by Photoionization Mass Spectrometry, retrieved from: <http://pubs.acs.org/cgi-in/abstract.cgi/ancham/2006/78/i09/abs/ac0518506.html>
- AIAG (2005), Automotive Industry Action Group, General Projects, retrieved from http://www.aiag.org/press/releases/GENERAL/Accomplishments_Final%20Updated_%20200906.pdf
- AIAG (2007), Automotive Industry Action Group, Materials Off-Shore Sourcing MOSS Project - Work Documents, retrieved from <http://www.aiag.org>
- AMR Research, (2005), Automotive and Heavy Equipment, Security and Costs Remain Key Challenges to Software as a Service in SMBs, retrieved from <http://www.amrresearch.com/Content/Topic.asp?ValueID=416>
- Anderson, D., Sweeney, D., Williams, T. (2003). Essentials of Statistics for Business and Economics. 3rd Edition., Thomson South-Western, pp. 483-497.
- Apurva, J., Moinzadeh, K., (2005), A Supply Chain Model with Reverse Information Exchange. Manufacturing & Service Operations Management, University of Washington Business School, Seattle, Washington.
- Benbasat, I., Goldstein, D. K. and Mead, M. (1987), The case research strategy in studies of information systems, MIS Quarterly, 11(3): 369-386.

- Benson, A. S., et al. (2005), Massachusetts Institute of Technology, Dept. of Civil and Environmental Engineering, The role of organizational culture in creating secure and resilient supply chains, 121 pages.
- Bowersox, D., Closs, D., and Cooper, M. (2007), Supply Chain Logistics Management, 2nd edition, Michigan State University, McGraw-Hill Irwin, New York, NY.
- Brebbia, C. A, Wessex Institute of Technology, & Rhodes Municipal Environmental Organization., (2004), Risk analysis IV : Fourth International Conference on Computer Simulation in Risk Analysis and Hazard Mitigation, Southampton [U.K.] ; Boston [Mass.] Billerica, MA.
- Caballero, C. G., Sloan School of Management, Massachusetts Institute of Technology Dept. of Mechanical Engineering & Leaders for Manufacturing Program, (2005), Leading a lean transformation in the wake of a disaster, Boston, Mass.
- Camarinha-Matos, L., (2004), Virtual enterprises and collaborative networks : IFIP 18th World Computer Congress, TC5/WG5.5--5th Working Conference on Virtual Enterprises, 22-27 August 2004, Toulouse, France. Boston, Ma., Kluwer Academic Publishers.
- CBS News (2006), FBI's New Data Warehouse A Powerhouse, War On Terror, retrieved from:
<http://www.cbsnews.com/stories/2006/08/30/terror/main1949643.shtml>
- Chan, C. K., & Lee, H. W. J., (2005), Successful strategies in supply chain management, Hershey, PA., Idea Group Publishers.
- Chiles, C. R., Dau, M. T. (2005), Massachusetts Institute of Technology Engineering Systems Division, An analysis of current supply chain best practices in the retail industry with case studies of Wal-Mart and Amazon.com Unpublished Thesis M. Eng. in Logistics --Massachusetts Institute of Technology Engineering Systems Division, Boston, Mass.

- Christopher, M., (2005), Logistics and supply chain management: creating value-added networks, (3rd ed.), Harlow, England; New York: Financial Times Prentice Hall.
- Churchman, C. W., (1971), The Design of Inquiring Systems: Basic Concepts of Systems and Organization, New York, Basic Books.
- Clinton, W., (1998) "Critical Infrastructure Protection", Presidential Decision Directive 63, 22 May 1998, retrieved from: <http://www.fas.or/irp/offdocs>
- Connaughton, P.,(2006), Supply Chain Management, Forrester Research, retrieved from <http://www.forrester.com>
- Cranor, L. F., & Wildman, S. S. (2003), Rethinking rights and regulations: institutional responses to new communication technologies, Cambridge, Mass., MIT Press.
- Creswell, J. W. (2003). Research Design: Qualitative, Quantitative, and Mixed Method Approaches, Thousand Oaks, California, Sage Publications.
- D'Antoni, H., (2005), Security Conforms To Regulatory Compliance, Information Week Magazine, retrieved from: <http://www.informationweek.com/story/showArticle.jhtml?articleID=170100825>
- DHS - Department of Homeland Security, (2006), Hazmat Equipment Survey, retrieved from: <http://homelandsecurity.ohio.gov/HazmatEquipmentSurvey.html>
- DHS - Department of Homeland Security, (2007), Comprehensive Security National Strategy, retrieved from: <http://homelandsecurity.ohio.gov/>
- Dolgui, A., & Zaikin, O., (2005), Supply chain optimization: product/process design, facility location and flow control. New York: Springer.

- Dresser, E. L., (2004), Massachusetts Institute of Technology, Dept. of Ocean Engineering, The effectiveness and economic impact of enhancing container security, Boston, Mass.
- ECO Environmental, (2005), RAE Systems Colorimetric Gas Detection Tubes, retrieved from:
http://www.ecoenvironmental.com.au/eco/gas/rae_gas_detection_tubes.html
- European Commission, (2005), Customs and Security: Customs related security initiatives of the EU, retrieved from:
http://ec.europa.eu/taxation_customs/customs/policy_issues/customs_security/index_en.htm#cus_relat
- Fandel, G., (2004), Modern concepts of the theory of the firm: managing enterprises of the new economy. Berlin, New York, Springer-Verlag.
- FBI - The Federal Bureau of Investigation, (2005), Management of the Trilogy Information Technology Modernization Project Audit Report No. 05-07, February 2005, Office of the Inspector General, retrieved from:
<http://www.usdoj.gov/oig/reports/FBI/a0507/app8.html>
- Fike, R. L. and Massachusetts Institute of Technology. Engineering Systems Division, (2005), Supply chain risk management: redefining the audit function within a large industrial company, 74 pages, Boston, Mass.
- Gansler, J. S. and Luby R. E., (2004), Transforming government supply chain management, Lanham, Md., Rowman & Littlefield.
- Gibson, S., (2006), "HP clones P&G Cincinnati Accounting Ops in India," E-Week.com on the Web, March 19, 2006, retrieved from:
<http://www.eweek.com>
- Gupta, A. K., & Westney, D. E., (2003), Smart globalization: designing global strategies, creating global networks, (1st ed.), San Francisco: Jossey-Bass.

- Han, T. and Massachusetts Institute of Technology Engineering Systems Division, (2005), The Radio Frequency Identification enabled logistics process for supply chain event management from China to the United States via Hong Kong: 69 pages.
- Harmon, P., (2003), Business Process Change: A Manager's Guide to Improving, Redesigning, and Automating Processes, Morgan Kaufman Publishers, San Francisco, CA.
- Hengst, M. D. and Vreede, G. J. D., (2004), Collaborative Business Engineering: A Decade of Lessons from the Field, Journal of Management Information System, 20(4).
- iConnect Corp., (2007), electronic commerce experience necessary to implement global trading communities quickly and cost effectively, retrieved from: <http://www.iconnect-corp.com/>
- IMD International, (2007), MIT Sloan School of Management: Managing The Extended Supply Chain (MESc) - Beyond Productivity and Efficiency, Retrieved from <http://www.imd.ch/programs/oep/execution/mesc/index.cfm?bhcp=1>
- InfoWorld Magazine, (2006), Next-generation tags, readers, and software help you effectively RF-enable your enterprise, retrieved from <http://www.infoworld.com/reports/16SRrfidsoft.html?src=sem&source=sem01-SPCL-RPTS-RFID>
- ITDS, (2007), International Trade Data System, retrieved from: <http://www.itds.treas.gov>
- Jordan, E., & Silcock, L., (2005), Beating IT risks, Chichester, England; Hoboken, NJ: J. Wiley.

- Kagami, M., Tsuji, M., & Giovannetti, E., (2004), Information technology policy and the digital divide: lessons for developing countries, Cheltenham, UK; North Hampton, MA: Edward Elgar.
- Kakish, K. (2007a). Data Analysis of GSC IT Security Interviews and Questionnaires. Lawrence Technological University, Southfield, MI.
- Kakish, K. (2007b). GSC Hosted IT Services Research Presentation. Lawrence Technological University, Southfield, MI.
- Kakish, K. (2007c). GSC IT Security Abstract for Interviewees. Lawrence Technological University, Southfield, MI.
- Kakish, K. (2007d). GSC IT Security Interview Overview. Lawrence Technological University, Southfield, MI.
- Kakish, K. (2007e). GSC IT Security Interviewee Presentation. Lawrence Technological University, Southfield, MI.
- Kakish, K. (2006), DMIT research proposal for GSC Hosted IT Services, Lawrence Technological University, Southfield, MI.
- Kakish Notes, (2007), A collection of hand-written and typed notes that were taken by the researcher throughout the research process for the purpose of conducting the research. Original Notes available upon request.
- Kakish, K., Steenkamp, A. L. (2005), A Global IT Security Perspective: An Analysis of the Information Security Capability in the U.S. and Europe, Proceedings of the Association for Global Business, Annual Conference, Miami, FL, November, 2005.
- Kakish, K., Steenkamp, A.L., Basal, A., Dawwas, M., Konda D., and Shulaiba, R. (2004), A Team Project on Information Technology Infrastructure Architecture, Proceedings of ICIER2004, International Academy for Information Management, Washington D.C., December 2004.

- Kantor, P. B., (2005), Intelligence and security informatics: IEEE International Conference on Intelligence and Security Informatics, ISI 2005, Atlanta, GA, USA, May 19-20, 2005: Proceedings. Berlin; New York, Springer.
- Katz, R., (2004), The human side of managing technological innovation: a collection of readings, (2nd ed.), New York: Oxford University Press.
- Laere, J. V., (2003), Coordinating Distributed Work: Exploring situated coordination with gaming-simulation, Doctoral dissertation, Delft University of Technology, Delft, The Netherlands.
- Lan, Y. C. and Unhelkar B., (2006), Global integrated supply chain systems, Hershey, PA, Idea Group Publishers.
- Lensing, R. P., & Massachusetts Institute of Technology, Engineering Systems Division, (2003), Historical events and supply chain disruption : chemical, biological, radiological and cyber events, Unpublished Thesis M. Eng. in Logistics --Massachusetts Institute of Technology Engineering Systems Division, Boston, Mass.
- Life Safety Systems, (2006), SAFESITE™ Multi-Threat Detection System (DETECR01), retrieved from:
<http://www.lifesafetysys.com/osb/itemdetails.cfm/ID/729>
- Luftman, J., (2004), Managing the Information Technology Resource: Leadership in the Information Age, Pearson Prentice Hall. Upper Saddle River, New Jersey.
- McCullagh, D. (2006), Post-9/11 Anti-terror technology: A report card. C | net New.com., retrieved from:
http://news.com.com/A+report+card+on+anti-terror+technology/2100-1028_3-6113064.html?tag=html.alert
- Meel, J. W. V., (1994), The Dynamics of Business Engineering, Delft University of Technology, Delft, The Netherlands.

Melvin, S. P. (2005), *Cyberlaw and e-commerce regulation: an entrepreneurial approach*, Mason, Ohio: Thomson/South-Western.

Narayanan, V. K. and Armstrong, D. J., (2005), *Causal mapping for research in information technology*, Hershey, PA, Idea Group Pub.

Neef, D., & NetLibrary Inc. (2004), *The supply chain imperative*, (1st ed.). New York: American Management Association.

NIST - National Institute of Standards and Technology (2007), *Manufacturing Systems Integration Division NIST MOSS Project Worksite*, retrieved from: <http://syseng.nist.gov/moss/moss-views>

O'Brien, D., Gannon, B., and Bois, R., (2005), *Security and Costs Remain Key Challenges to Software as a Service in SMBs*, AMR Research - Enterprise Strategies Service, retrieved from: <http://www.amrresearch.com/Content/View.asp?pmillid=18759>

Ongchin, S. M., Sloan School of Management Massachusetts Institute of Technology Dept. of Materials Science and Engineering & Leaders for Manufacturing Program, (2005), *Framework for developing a co-production strategy in a vertically integrated operation*, Unpublished Thesis M.B.A., Boston, Mass.

Pararas-Carayannis, J. and Massachusetts Institute of Technology, Management of Technology Program, (2002), *RFID-enabled supply chain replenishment*: 88 pages.

Perks, C., & Beveridge, T. (2003). *Guide to enterprise IT architecture*. New York: Springer-Verlag. pp 18-20; 55-57.

Pickett, C. B. and Massachusetts Institute of Technology, Engineering Systems Division, (2003), *Strategies for maximizing supply chain resilience: learning from the past to prepare for the future*, 126 pages, Unpublished Thesis M. Eng. in Logistics, Massachusetts Institute of Technology Engineering Systems Division, Boston, Mass.

- Rapiscan Systems, (2006), Advanced PFNA™ Technology: PFNA TCIS (Truck and Container Inspection System), retrieved from:
<http://www.rapiscansystems.com/pfnatcis.html>
- Ritter, L., Barrett, J.M., Wilson, R., (2007), Securing Global Transportation Networks: A Total Security Management Approach. McGraw Hill, New York, NY.
- Science Magazine (1994), NRC Urges Destruction of Chemical Weapons, retrieved from:
<http://www.sciencemag.org/cgi/content/citation/226/4679/1174?ck=nck>
- Sheffi, Y., (2005), The Resilient Enterprise: Overcoming Vulnerability for Competitive Advantage, MIT Press, Cambridge Ma.
- Simchi-Levi, D., Kaminsky, P., & Simchi-Levi, E. (2004), Managing the supply chain: the definitive guide for the business professional. New York: McGraw-Hill.
- Snack, P., and Kakish, K. (2007). Snack-Kakish DMIT Dissertation Interviewee List. Lawrence Technological University, Southfield, MI.
- Sol, H. G. and Bots, P. W. G., (1988), Recent Developments in Decision Support Systems, NATO ASI Series F: Computer and Systems Sciences 101: 22-34.
- Sol, H. G. and Keen, P. (2004), Rehearsing the Future. Building Decision Agility Through Decision Enhancement Services, retrieved from:
http://www.peterkeen.com/forthcoming/rehearse_future.htm
- Sol, H. G. (1992), Dynamics in Information Systems. Dynamic Modeling of Information Systems, R. L. Crosslin, Amsterdam, The Netherlands, Elsevier Science Publishers (North Holland).
- Sol, H. G., (1982), Simulation in Information Systems Development, Doctoral Dissertation, Groningen, University of Groningen.
-

Sol, H. G., (1988), Information systems development: a problem solving approach, Proceedings of the Symposium on Systems Analysis and Design, Atlanta, GA.

Stamp, P., Koetzle, L., Bernhardt, S. (2006), Application Development and Program Management The Forrester Wave™: Enterprise Security Information Management, retrieved from:
<http://www.forrester.com/Research/Document/0,7211,38279,00.html>

Stanford University Global Supply Chain Management Forum (2006), "Innovators in Supply Chain Security: Better Security Drives Business Value", The Manufacturing Institute, July 2006,
<http://www.nam.org/supplychainsecurity>

TCC - Trade Compliance Center (2006), The U.S. Department of Commerce's International Trade Administration, retrieved from: <http://tcc.export.gov>

Thiele, A. & Massachusetts Institute of Technology Dept. of Electrical Engineering and Computer Science, (2004), A robust optimization approach to supply chains and revenue management, 176 pages, Unpublished Thesis Ph. D. --Massachusetts Institute of Technology Dept. of Electrical Engineering and Computer Science, Boston, Mass.

Time Magazine, (2006), The Untold Story of al-Qaeda's Plot to Attack the Subway, retrieved from:
<http://www.time.com/time/magazine/article/0,9171,1205478,00.html>

TNT Logistics, (2007), Fastest Possible Shipping Service, Customized to Your Requirements - Express Services, retrieved from:
http://www.tnt.com/country/en_corporate/about/express.html

Tweddle, D. (2003), Security and Facilitation of the International Trade Supply Chain, Joint World Bank, WCO meeting retrieved from:
<http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,menuPK:282828~pagePK:149018~piPK:149093~theSitePK:282823,00.html>

United Nations, (2007). United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT). Economic Commission for Europe. Recommendation 33. retrieved from:
http://www.unece.org/cefact/recommendations/rec33/rec33_trd352e.pdf

United States Government Accountability Office, (2006), Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System.

US CBP - U.S. Customs and Boarder Protection, (2002), U.S. Customs Implements Enhanced Anti-Terror Sea Cargo Targeting at All U.S. Seaports, retrieved from:
http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/legacy/2002/92002/09032002.xml

US CBP - U.S. Customs and Boarder Protection, (2003), retrieved from
<http://www.cbp.gov/xp/cgov/home.xml>

US CBP - U.S. Customs and Boarder Protection, (2004), Commercial Enforcements C-TPA, retrieved from:
http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/ctpat_faq.xml

U.S. Office of Compliance, (2004), Advancing Safety, Health, and Workplace Rights in the Legislative Branch, retrieved from
<http://www.compliance.gov>

U.S. Pentagon, (2003), retrieved from:
http://www.pentagon.mil/news/Apr2003/n04252003_200304254.html

Vervest, P., (2005), Smart Business Networks, Berlin; New York, Springer.

Vreede, G. J. D., (1995), Facilitating Organizational Change : The Participative application of dynamic modeling. Doctoral dissertation, Delft University of Technology, Delft, The Netherlands.

Walker, W. T. (2005), Supply chain architecture: a blueprint for networking the flow of material, information, and cash, Boca Raton, Fla.: CRC Press.

WCO – World Customs Organization, (2006), Framework of Standards to Secure and Facilitate Global Trade (SAFE), retrieved from:
http://www.wcoomd.org/ie/EN/Press/Cadre%20de%20normes%20GB_Version%20Juin%202005.pdf

WCO – World Customs Organization, (2007), Facilitation Customs Procedures, retrieved from:
http://www.wcoomd.org/ie/EN/Topics_Issues/FacilitationCustomsProcedures/facil_wco_data_model.html

Wikipedia, (2007a), The Free Encyclopedia. Supply Chain Management, retrieved from:
http://en.wikipedia.org/wiki/Supply_chain_management#_ref-5

Wikipedia, (2007b), The Free Encyclopedia. Supply Chain Security, retrieved from: http://en.wikipedia.org/wiki/Supply_Chain_Security

Willis, H. H., & Ortiz, D. (2004). Evaluating the security of the global containerized supply chain. Santa Monica, Calif.: RAND Corporation.

WTO (2007), World Trade Organization. The WTO Gateway, retrieved from:
http://www.wto.org/english/thewto_e/thewto_e.htm

XML Europe, (2001), ebXML Security, retrieved from:
<http://www.gca.org/papers/xml europe2001/papers/html/s09-1.html>

Yin, R. K., (2003), Case Study Research Design and Methods, Thousand Oaks, Calif., Sage Publications.

TERMINOLOGY AND ACRONYMS

ACH	Automated Clearing House
ACI	Advance Cargo Information
ACSS	Automated Clearing Settlement System
AIAG	Automotive Industry Action Group
ATS	Automated Targeting System
CBO	Congressional Budget Office
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CSI	Container Security Initiative
CSO	Computer Security Organization
C-TPAT	Customs Trade Partnership against Terrorism
DHS	Department of Homeland Security
EDI	Electronic Data Interchange
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
EU	European Union
FIPS	Federal Information Processing Standards
GAO	General Accounting Office
GDP	Gross Domestic Product
GMC	Global Motors Corp
GPS	Global Positioning System
GRC	Governance, Risk, and Compliance
GSC	Global Supply Chain
GSCITSS	Global Supply Chain IT Security System
IA	Information Assurance
ICT	Information and Communications Technology
IDS	Intrusion Detection Systems
IDW	Investigative Data Warehouse
IMDS	International Materials Data System
IMO	International Maritime Organization
IP	Industry Participant
IPS	Intrusion Prevention Systems
ISPS Code	International Ship and Port Facility Security Code

IT	Information Technology
ITDS	International Trade Data System
ITIL	Information Technology Infrastructure Library
ITL	Information Technology Laboratory
JV	Joint Venture
LASER	Language and Speech Exploitation Resources
LCP	Life Cycle Processes
LSM	Least Square Method
MA	Major Application
MIT	Mass. Institute of Technology
MOSS	Materials Offshore Sourcing
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NRC	National Research Council
OEM	Other Equipment Manufacturer
PFNA	Pulsed Fast Neutron Analysis
POS	Point of Sale
PV	ProVision
RFID	Radio Frequency Identification Devices
SCM	Supply Chain Management
SDLC	System Development Life Cycle
SME	Small to Midsize Enterprises - similar to automotive tiers one.
SOX	Sarbanes-Oxley
SSL	Secured Socket Layer
ST&E	Security Test and Evaluation
SW	Single Window Facilitation
TCC	Trade Compliance Center
TCIS	Truck and Container Inspection System
UN	United Nations
US CBP	United States Customs and Borders Protection
VCO	Virtual Customs Office
WAP	Wireless Application Protocol
WCO	World Customs Organization
WSI	Web Services Interoperability
WTO	World Trade Organization
WWRE	WorldWide Retail Exchange
XML	Extensible Markup Language

End Notes

ⁱ Please note that the 10% cost includes other physical costs as well. For details on these costs, please visit <http://www.forrester.com/Research/Document/0,7211,38279,00.html>

ⁱⁱ Douglas Tweddle is the Chair of the WCO Task Force on Security and Facilitation of the International Trade Supply Chain.

ⁱⁱⁱ Please note that the names of the individuals who were interviewed were removed from this table for privacy purposes

^{iv} Please note that the names of the individuals who were interviewed were not listed here for privacy purposes.

^v These 4 documents can be made available to any reader upon request of the author. For the interest of limited space, these documents are not included here.