Conceptual/Contextual Framework for Critical Infrastructure Protection Supply Chain Issues

Final Report

Prepared by:

Kevin Quigley, PhD
School of Public Administration
Dalhousie University
Halifax, Nova Scotia

Ronald Pelot, PhD
Department of Industrial Engineering
Dalhousie University
Halifax, Nova Scotia

Colin Macdonald
School of Public Administration
Dalhousie University
Halifax, Nova Scotia

Scientific Authority:
Lynne Genik
DRDC Centre for Security Science
613-943-0751

Contractor Report Contract # CSSP-2013-CP-1027

Contract Report
DRDC-RDDC-2015-C193
January 2015

Supply Chain Risk Analysis and Management CSSP-2013-CP-1027 was supported by the Canadian Safety and Security Program which is led by Defence Research and Development Canada's Centre for Security Science, in partnership with Public Safety Canada. The project was led by New Brunswick Department of Public Safety in partnership with Conference Board of Canada, Deep Logic Solutions, Dalhousie University

Canadian Safety and Security Program is a federally-funded program to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.

Abstract

We use the Hood, Rothstein and Baldwin (2001) Risk Regulation Regime framework to analyze safety and security in subsectors of Canada's transportation (airports, seaports, rail, bridges and trucking) and food supply (grocer and commodities). The small sample size of interview subjects in any one sector would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We summarize observations from over 60 semi-structured interviews conducted between 2011 and 2013 with regulators, managers and owners and operators of critical infrastructure to determine the effectiveness of the control mechanisms at work in each of the subsectors; we focus on standards and behaviour, in particular. While each of the subsectors has unique concerns, coordination with key stakeholders, technical complexity, image, risk exposure, security costs and the consequences of single points of failure, for example, were common concerns. The report supports the research project in three important ways. First, decision-makers require an understanding of the strengths and weaknesses of the existing control system to determine how with limited resources one might maximize the impact of change initiatives aimed at strengthening the regime. Secondly, the research can inform the development of plausible risk scenarios that test the decision-making methods that we are developing. Thirdly, we draw on the academic literature to suggest improvements to the decision-making process based on the type of risk (complex, uncertain or ambiguous) and highlight selected tensions in conventional risk decision-making that present challenges to risk governance strategies, such as the decision to employ a precautionary approach and develop trust relationships with stakeholders.

Significance for Defence and Security

This document reports on findings from interviews with regulators, managers, owners, and operators of critical infrastructure in subsectors of Canadian transportation (airports, seaports, rail, trucking and bridges) and food supply (grocer and commodity groups). It identifies strengths and weakness in standards and behaviour change mechanisms in each of the subsectors. We subsequently draw lessons for risk decision-making in New Brunswick. The paper also summarizes key concepts and tensions in the risk governance, trust and precautionary principle literature that can assist in improving the risk decision-making process.

Résumé

Nous avons utilisé le régime de gestion des risques de Hood, Rothstein et Baldwin (2001) pour analyser la sûreté et la sécurité dans des sous-secteurs du transport (aéroports, ports, transport ferroviaire, ponts et camionnage) et de l'approvisionnement alimentaire (détaillants et produits de base) du Canada. La petite taille de l'échantillon de personnes interviewées dans l'un ou l'autre des secteurs devrait exclure l'utilisation de toute analyse rigoureuse pour appuyer les généralisations des conclusions. Nous avons résumé les observations tirées de 60 entrevues semi structurées, réalisées entre 2011 et 2013, avec des chargés de réglementation, des gestionnaires ainsi que des propriétaires et des exploitants d'infrastructures essentielles pour évaluer l'efficacité des mécanismes de contrôle appliqués dans chaque sous secteur; nous avons mis l'accent sur les normes et les comportements. Même si chaque sous secteur a ses propres préoccupations, la coordination avec les intervenants, la complexité technique, l'image, l'exposition aux risques, les coûts de la sécurité et les conséquences des points de défaillance uniques, par exemple, sont des questions qui les concernent tous. Le rapport appuie le projet de recherche de trois façons importantes. Premièrement, les décideurs doivent comprendre les forces et les faiblesses du système de contrôle en place pour déterminer comment il est possible avec des ressources limitées de maximiser l'incidence des initiatives de changement visant à renforcer le régime. Deuxièmement, la recherche peut orienter l'élaboration de scénarios de risque plausibles pour évaluer les méthodes de prise de décisions que nous sommes à mettre au point. Troisièmement, nous nous sommes inspirés d'ouvrages universitaires pour suggérer des améliorations au processus décisionnel fondées sur le type de risque (complexe, incertain ou ambigu), et nous avons soulevé certaines contraintes dans le processus classique de prise de décisions sur les risques qui font obstacle aux stratégies de gouvernance en matière de risque, comme la décision d'employer une approche de précaution et de développer des relations de confiance avec les intervenants.

Importance pour la défense et la sécurité

[Le document présente les conclusions d'entrevues réalisées avec des chargés de réglementation, des gestionnaires ainsi que des propriétaires et des exploitants d'infrastructures essentielles dans des sous secteurs du transport (aéroports, ports, transport ferroviaire, ponts et camionnage) et de l'approvisionnement alimentaire (détaillants et produits de base) du Canada. Il présente les forces et les faiblesses des normes et des mécanismes de modification des comportements dans chacun des sous-secteurs. Nous avons ensuite tiré des leçons pour la prise de décisions sur les risques au Nouveau Brunswick. Par ailleurs, le document résume les concepts clés et les principales contraintes qui sont mentionnés dans les ouvrages traitant de la gouvernance en matière de risque, de la confiance et du principe de précaution et qui pourraient aider à améliorer la prise de décisions sur les risques.

Table of contents

List of figures

List of tables

Acknowledgements

This report is the result of a research project on critical infrastructure protection that started in 2008. We have conducted research on the transportation and agricultural sectors. The authors wish to acknowledge the support of the Social Sciences and Humanities Research Council (Standard Operating Grant No. 410-2008-1357; Partnership Development Grant No. 890-2010-0123), Public Safety Canada and the Kanishka Project Contribution Program, and the Canadian Safety and Security Program (CSSP-2013-CP-1027).

Special thanks go to the 60 interview subjects from four countries who graciously gave their time in support of this research. We also wish to acknowledge the several graduate students at Dalhousie University who have assisted in this research since its inception. Many of the interviews were conducted and transcribed by Emily Pond, Ben Bissett and Bryan Mills. This document was copy-edited by Janet Lord. An early draft of the paper was reviewed by representatives from each member in the Supply Chain Risk Analysis and Management project team; their comments and suggestions were incorporated into the final version, where possible.

While we are grateful for the support from these sources, the authors alone are responsible for any errors or omissions.

1 Introduction

This paper is the task two final report *Conceptual/Contextual Framework for Critical Infrastructure Protection Supply Chain Issues* for the project Supply Chain Risk Analysis and Management (New Brunswick Department of Public Safety; CSSP-2013-CP-1027; Canadian Safety and Security Program). The overall goal of the project is to contribute to the development of tools and methodologies to assess risk in the supply chain networks of the transportation, energy and food sectors in the Province of New Brunswick.

This report draws data from two other research projects on critical infrastructure protection – 'Critical Infrastructure Protection in Comparative Perspective: Contextual Factors that Influence the Exchange of Sensitive Information' supported by a SSHRC Standard Operating Grant and 'Understanding and Responding to Terrorist Threats to Critical Infrastructure' supported by a Kanishka Project Contribution Agreement. We have conducted research on the transportation and agricultural sectors. We performed a literature review, and, between 2011 and 2013, held over 60 semi-structured interviews.

In this paper, using the Hood *et al.* [1] risk regulation regime framework, we examine the manner and extent to which critical infrastructure (CI) systems are controlled in the transportation and food sectors in Canada. We summarize interview data with CI owners, operators, managers and regulators largely from Canada. We also report on interview data from officials in the United States (US), the United Kingdom (UK) and Australia in order to provide some international perspective. The report then highlights how these data relate to this research project. We make observations and extract lessons from the data to suggest how best to develop reliable tools and methodologies that support decision-makers in emergency management.

The paper is organized in the following manner. After summarizing definitions, methods and the framework, we summarize our transportation and food interview data, which are drawn from interviews with representatives in five subsectors of the transport sector (airports, seaports, rail, trucking and bridges) and representatives from the grocer and commodity groups in the food sector. Using the Hood *et al*. framework, we summarize CI owners', operators', managers' and regulators' views of two key aspects to a cybernetic understanding of control: standards and behaviour change. Following this description of data, we make observations and extract lessons from the data that relate to risk management of potential CI events in New Brunswick. We then draw on recent research from the social science of risk literature to discuss the importance of defining types of risk as well as controversies about the precautionary principle and trust, which are critical concepts in risk management processes during CI events. Taken together, the work supports the overall goal of the project: to contribute to the development of tools and methodologies to assess risk in supply chain networks in the Province of New Brunswick.

1.1 Scope, Definitions and Limitations

1.1.1 Safety and Security

While our CIP research is focused largely on security, the concept of safety[1] also came up repeatedly in our interviews. We try to distinguish between the two, but at times interview subjects conflated the subjects. Security risks involve human aggressors who are influenced by a variety of environmental and personal factors and who may come from within or outside the target institution [2]. While their outcomes may be similar, security and safety risks demand different approaches to risk management. "[P]rotecting installations against intentional attacks," write Reniers and Pavlova, "is fundamentally different from protecting against random accidents or acts of nature" [2] (see also [3]). Human aggressors, for example, are adaptive agents; they will modify their behaviour in light of security practices that organizations adopt. Generally, safety plans tend to be more transparent, are informed by more reliable data and are regulated more clearly. Safety plans are also more clearly entrenched in the organizational culture and legal tradition of many critical sectors.

1.1.2 Critical Infrastructure Protection

Critical infrastructure protection seeks to enhance the physical and cyber security of key public and private assets and mitigate the effects of natural disasters, industrial accidents and terrorist attacks. The Government of Canada has identified ten critical sectors. Most Western governments have similar—though not identical—lists for their countries. The UK government has identified nine sectors [4] and the US government has identified 16 [5], for example.

1.1.3 Risk and Regulation

Risk is a probability, though not necessarily calculable in practice, of adverse consequences [1]. Regulation means attempts to control or mitigate risk, mainly by setting and enforcing product or behavioural standards [1]. Risk regulation is governmental intervention in market or social process to influence and control to varying degrees potentially adverse social and economic consequences.

1.1.4 Regimes

Regimes refer to the "the complex of institutional geography, rules, practice and animating ideas that are associated with the regulation of a particular risk or hazard" [1].

1.1.5 Risk Governance

Risk governance includes the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analyzed and communicated and management decisions are taken. Encompassing the combined risks, relevant information, decisions and actions of both governmental and private actors, risk governance is of particular importance in, but not restricted to, situations where there is no single authority to take a binding risk management decision but instead where the nature of the risk requires collaboration and coordination between different stakeholders. Risk governance, however, not only includes a

[1] To many people in the transport industry, safety is about lost workdays due to accident and fatalities as a result of work activities, and they pay a workers' compensation premium to address this.

multi-faceted, multi-actor risk process but also calls for the consideration of contextual factors such as institutional arrangements (e.g., the regulatory and legal framework that determines the relationship, roles and responsibilities of the actors and coordination mechanisms such as markets, incentives or self-imposed norms) and political culture including different perceptions of risk [6].

1.1.6 Limitations to this Research

The corresponding author is a public administration specialist. He uses qualitative methods, including semi-structured interviews and a broad range of social science literature, including references from psychology, political science, sociology and anthropology, to study governance and risk. We used the Hood *et al.* framework to design the interview tool and analyze the data. We use some commonly applied concepts from different academic traditions to explain the data. A mixed-method analysis was conducted on the interview data, consisting of both quantitative and qualitative methods. The quantitative analysis consists of descriptive statistics, including simple means and response percentages. The small sample size of interview subjects in any one sector would preclude the use of any rigorous statistical analysis to support generalizations of the findings. The risk regulation regime content section, in particular, relies significantly on the perspective of those working within the sector and those regulating it. Additional constraints include the scope of the sectors (from local to global), the difficulty in obtaining reliable security data, the limited amount of time to conduct the research, the limited number of interview subjects and the inevitable limitations of human perspective (researcher and interview subjects). Finally, the interviews occurred at some point over the last three years. People's views change and adapt.

1.2 The Hood, Rothstein and Baldwin Risk Regulation Regime Framework

In their analysis of risk regulation regimes in the UK, Hood, Rothstein and Baldwin define regimes as "the complex of institutional geography, rules, practice and animating ideas that are associated with the regulation of a particular risk or hazard" [1]. Hood *et al.* hypothesize that within these regimes context shapes the manner in which risk is regulated. 'Regime context' refers to the backdrop of regulation. There are three elements that Hood *et al.* use to explore context: the technical nature of the risk; the public's and media's opinions about the risk; and the way power and influence are concentrated in organized groups in the regime.

Hood *et al.* [1] employ the cybernetic theory of control to examine the management of the specific policy area, which they refer to as 'regime content'. The theory asserts that if the three dimensions of control—information gathering, standard setting and behaviour modification—are under control, the system is effectively under control.

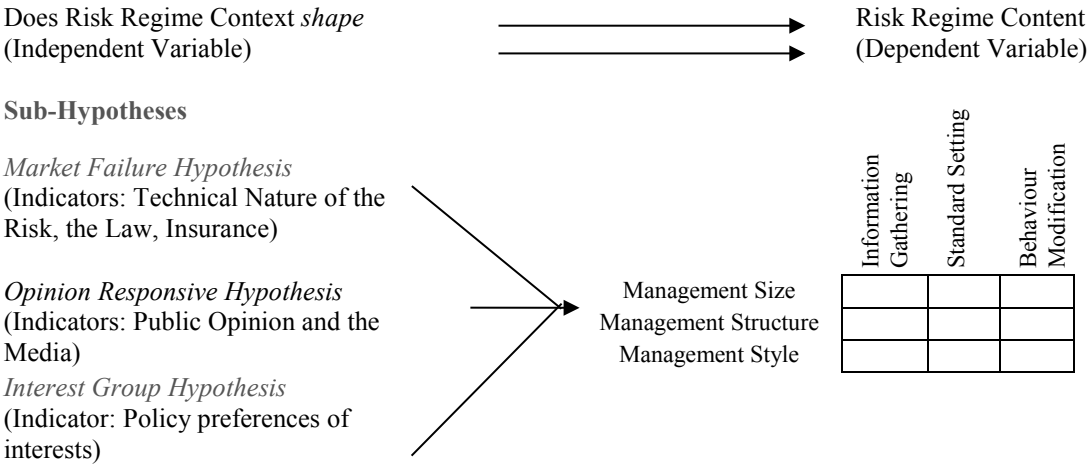

Figure 1: *Hood, Rothstein and Baldwin (2001): Understanding Risk Regulation Regimes*

For the purposes of this paper we will focus much of our discussion on two of the control mechanisms—standard setting and behaviour modification—as these are particularly important concepts in supply chain risk. (Information-gathering will be examined in more detail in subsequent reports. The influence of markets, public opinion and interests will also be examined in future reports.) Standard setting involves establishing goals, or guidelines; in government, standards often take the form of policy although *Hood et al.* [1] interpret it broadly. Finally, behaviour modification refers to the preferences, incentive structures, beliefs and attitudes that shape systems—the capacity to modify behaviour of participants is the capacity to change systems. The distinction between these dimensions is not always tidy.

Each dimension of control may be further considered according to: size—the amount and scope of regulation and the resources used to sustain it; structure—the institutional arrangements of regime content, such as public-private sector relationships; and style—the formal and informal codes and conventions that help shape regime content [1].

For more on the Hood, Rothstein and Baldwin Framework, see Annex A.

2 Methodology

In 2011 and 2012 and with the support of SSHRC funding, we conducted and transcribed 55 semi-structured interviews with CI regulators, owners, operators and managers. In 2013 and following the support of the Kanishka Project, we conducted additional interviews with regulators, owners, operators and managers from the transportation and agriculture sectors with experience relating to security. Most interviews were audio recorded and all were fully transcribed. The interview tool was designed to extract data that relates to the Hood *et al*. [1] risk regulation regime framework. The tool and process were approved by Dalhousie's Research Ethics Board. As part of our commitment to the Board and our research subjects, transcripts are confidential and exact quotations are not used without the explicit permission of the interview subjects.

Table 1: *List of transportation interview participants by subsector and type*

Subsector	**Regulator**	**Owner/Operator/Manager**	**Industry Association**	**Expert/Academic**	**Total Number of Interviews**
Aviation	1	3	3	0	7
Port	4	7	2	2	14
Bridge	0	5	0	0	5
Rail	0	3	0	0	3
Trucking	1	2	1	0	4
Other	16	0	0	1	17
Total					50

*Other includes emergency managers, and senior and management level government officials in transportation (not subsector specific).

Table 2: *List of food interview participants by subsector and type*

Subsector	**Regulator**	**Owner/Operator/Manager/Industry Representative/ Citizens' Group**	**Total Number of Interviews**
Retailer	0	2	2
Industry Association - Grocery	0	2	2
Industry Association - Commodities	0	3	3
Regulatory Agency	1	0	1
Non-Profit	0	2	2
Total	1	9	**10**

The small sample size of interview subjects in any one sub-sector would preclude the use of any rigorous statistical analysis to support generalizations of the findings.
A mixed-method analysis was conducted on the interview data, consisting of both quantitative and qualitative methods. Aside from the summary statistics generated directly from the response

data, we have found it useful when conducting semi-structured interviews to ask interview subjects to score contextual pressures that influence how they spend their time, for example. While not generalizable, the scoring allows interview subjects to distinguish more succinctly the impact of the different pressures. It also allows us to rank and compare how individuals perceive the different pressures. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a point of departure for analysis and discussion. In almost all cases, the scoring was supplemented by extensive discussion with the interview subjects. It should also be noted that we conducted a number of interviews with executive-level public officials who had an overarching responsibility for the sectors as a whole and, therefore, offered views about contextual pressures in those sectors as a whole.

We used a grounded theory-based approach to extract and organize additional themes. We used a software package, Leximancer, to identify common themes in the interviews. We then reviewed the interview scripts based on themes and according to concepts germane to the framework. We supplemented this work with a comprehensive literature review of research on the regulation in the transportation and agriculture sectors.

Research partners in this project were given an advanced copy of this report and they provided comments to the authors.

Further details on our transportation interview participants can be found in Annex C.

Further details on our food/agriculture interview participants can be found in Annex D.

The semi-structured interview tool can be found in Annex E.

3 Applying the Framework: A Summary of our Inteview Findings Focussed on Standard-Setting and Behaviour Change

This section applies the Hood *et al.* framework to risks associated with the critical infrastructure of the Canadian transportation sector and the food sector. The analysis relies on occasional references to both the professional and academic literature—but largely the interview results—to characterize the content of the risk regulatory regime for each of the transportation subsectors and food sector that we studied. The transportation sector includes Airports, Seaports, Trucking, Rail and Bridges.

3.1 Airports

Airports are not regulated with their own act. The industry was ostensibly economically deregulated in 1988 [7]. Airports within the National Airports System are not-for-profit, non-share capital corporations [8]. These airports operate commercially and are locally managed and operated by individual Canadian Airport Authorities (CAA). The land and buildings are owned by the Government of Canada and the leasehold improvements revert to the Crown at the end of the management lease. Each CAA has a management lease and most are for 60 years with a clause for renewal for a shorter period. The industry, including the airports, is responsible for complying with and paying to meet government regulations [9].

Transport Canada's Aviation Security Oversight Program monitors and enforces stakeholder compliance and behaviour modification regulations through inspection activities and enforcement practices such as applying fines, or revoking operating licenses or certificates [10]. One interview participant noted that Transport Canada is very active in its oversight of airports (Int 15). According to Transport Canada [10], the government takes a risk-based approach to airport security, meaning higher-probability and/or higher-consequence events receive more resources and attention. This approach includes an array of oversight activities such as focused security inspection and testing activities that are based on risk assessments, compliance results and threat information. The stated objective of Transport Canada [10] is to work collaboratively with airports and attempt to rectify any compliance issues with the least punitive measures possible. Transport Canada also ensures that the aviation security regime complies with Canada's obligations under international treaties [11].

Interview subjects had mixed feelings about Transport Canada's standards and enforcement. They felt generally that Transport Canada was engaged with industry and responsive to its concerns (Int 6; Int 7; Int 11). At the same time, the standard-setting component of the regulatory regime for airports was at times too standardized, according to interview subjects (Int 12; Int 14). The legislation and regulations governing the aviation sector are extensive; indeed, aviation is considered to be one of the most aggressively regulated industries in Canada [12]. Interview subjects stressed that government should recognize the diversity in airports when applying the Canadian Aviation Regulations [13], particularly issues such as size and use of facilities (Int 12; Int 13; Int 15). The cost of regulatory compliance was one of the most significant issues for some airports (Int 13).

Laws and legal concerns clearly weighed on the minds of airport operators, managers and regulators. Airports for the most part have business continuity plans and contingency plans in place and, in contrast to other subsectors, at times formal agreements with emergency services. When given a list of contextual issues relevant to our framework and asked which contextual issues influence the manner in which they spend their time with respect to safety and security, interview subjects in the aviation sector scored law or legal concerns higher than any other contextual issue, and scored it higher than did the other subsectors (ports or surface): 9.3 out of a possible 10. (See Figure 2.) When asked, interview subjects expressed the most concern over risks associated with terrorism.

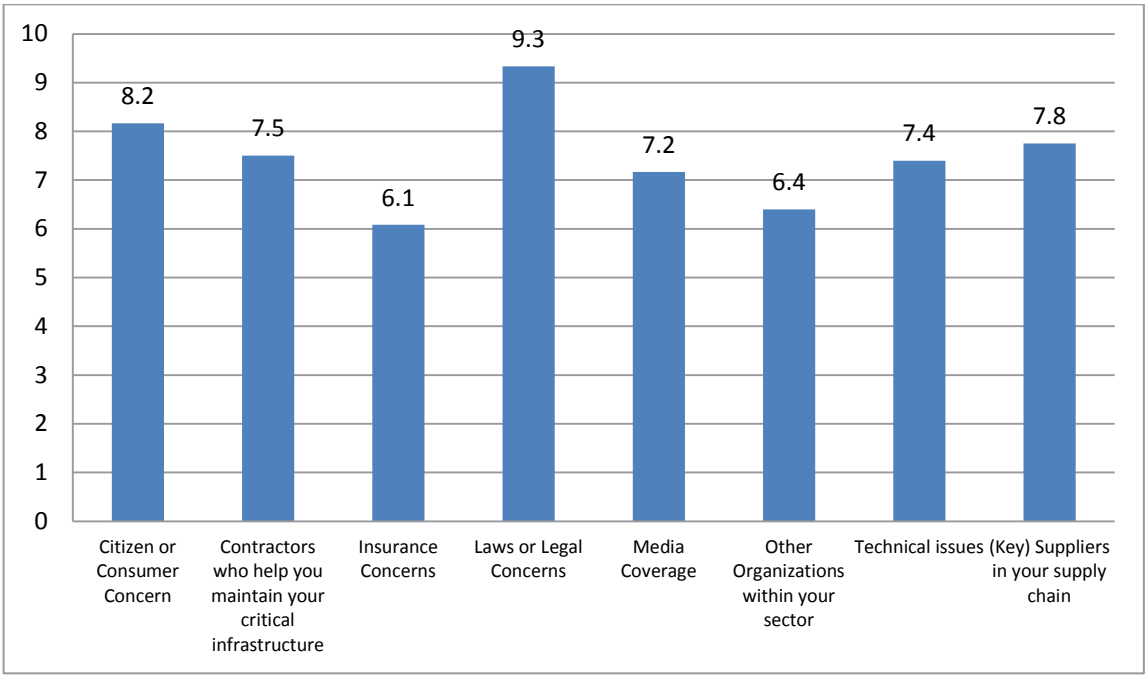

***Figure 2**: Responses from aviation interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=6; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it')*

Note: The small sample size in Figure 2 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion.

In sum, there are clear, albeit extensive standards for security, which are developed largely by Transport Canada in consultation with industry and other stakeholders. Some interview subjects noted that the regime is at times too inflexible and does not take the unique characteristics of each airport into account. Legal and policy concerns have considerable influence on airport staff. Transport Canada is active in behaviour modification, resulting in a robust, albeit at times routine- and rules-driven, control mechanism for the sector.

3.2 Seaports

The Canadian seaport system currently comprises 19 Canada Port Authorities (CPAs) that were created under the Canada Marine Act [14]. According to Brooks [15], this is akin to a not-for-profit model. CPAs are "federally incorporated, autonomous, non-share corporations that operate at arm's length from the federal government, which is the sole shareholder" [16]. Three categories of ports exist in Canada: Canadian Port Authorities (CPA), regional/local ports and remote ports. Regional/local ports are those that are deemed to be in a position in which they could be better managed by local interests [17]. Remote ports are those found in isolated communities that are reliant on marine transportation and have a government wharf [18]. In CPAs and remote ports, the government plays a strong regulatory role. Remote ports are considered to be a public good, and CPAs are considered to be essential infrastructure to the national ports system [19].

The regulations pertaining to risks within the marine sector are extensive. The primary legislation is the Marine Transportation Security Act (1994)[20]. The security framework created by these regulations includes inspections, monitoring, surveillance and enforcement. Security requires a large investment from both government and industry. The regulations are mandatory. While Transport Canada is the most significant public actor, several federal departments play a role (Int 48; Int 42). As with airports, standards are significantly influenced by the international context. The International Maritime Organization's (IMO) International Ship and Port Facility Security (ISPS) Code to a degree standardizes and shares best practices.

Operators and managers at seaports found policy direction from government to be at times inadequate (Int 31; Int 32; Int 42). While there are security standards, interview subjects felt that there were no national standards for critical infrastructure and lines of responsibility for government departments and the policy direction themselves were unclear (Int 42; Int 32). Moreover, and in contrast to the aviation interviews, interview subjects felt that government security policies were not developed in a collaborative manner (Int 32). Government regulators are aware of these issues and acknowledge they sometimes face constraints when sharing information with external parties, for example (Int 37; Int 38). As one participant noted, ports exist in an area of confusing multi-level governance (Int 48).

Many of the current standards for ports are perceived to be a government reaction to 9/11. While ship security has a long history, prior to 9/11 ports had not traditionally been as concerned with security. Some have described ports as starting with a clean slate after 9/11, and making considerable progress in a relatively short time. Interview subjects felt, however, that while some of these new standards were working well, others were not. As in aviation interviews, one participant recommended that government conduct a regulatory review examining these regulations to determine which of them should be kept and which should be discarded or redesigned (Int 31). Industry was particularly sensitive to the international context in which shipping occurs, including the international laws, competition, organized crime, terrorism and geo-political factors and felt that these pressures were not always sufficiently recognized by regulators (Int 35). There are also risks associated with passenger travel on cruise ships and ferries and inland shipping that some feel are not being adequately addressed.

This complex regulatory environment, combined with the occurrence of crime and competitive pressures ports face, creates a great deal of uncertainty and anxiety among staff (Int 29). This

point was reinforced by the fact that when asked which contextual pressures influence the manner in which they spend their time, ports identify several and cannot clearly identify selected prevailing pressures. (See Figure 3.) When asked, interview subjects expressed the most concern over risks associated with climate change and extreme natural events.

Overall, port staff are much less satisfied than airport staff with the regulatory regime. While the federal government sets standards and audits compliance, interview subjects feel there has been insufficient effort to examine the sector as a whole and evaluate interdependencies, for example.

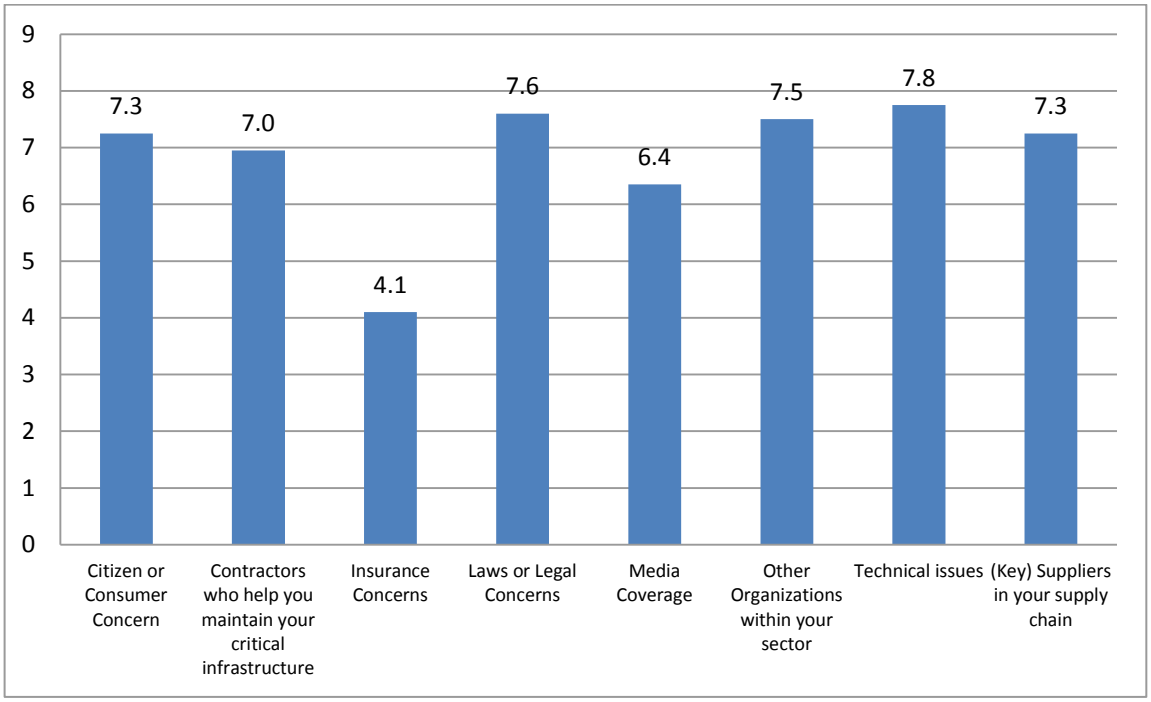

***Figure 3**: Responses from port interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=9; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it'*

Note: The small sample size in Figure 3 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion.

In sum, ports exist in an area of confusing multi-level governance; they are immovable, are expected to be competitive and serve a number of public and private sector interests. Compared to airport interviewees, port subjects feel that government/port interactions are not as collaborative or cooperative as they could be and that standards and behaviour modification are driven by getting products to market as quickly as possible, which creates uncertainty and anxiety among port staff with respect to security.

3.3 Trucking and Rail

Despite being quite different in many respects, trucking and rail are both categorized as "surface" and we therefore treat them together.

The trucking industry in Canada is made up of both corporations and small businesses. While some of these corporations are large, like TransForce with approximately 11,700 employees in 2012, by and large, the industry is constituted of smaller companies [21]. This includes for-hire carriers, private carriers, owner-operators and courier firms, for a total of approximately 56,800 firms [22].

Rail contrasts significantly with trucking. While there are 31 federally regulated rail carriers in Canada [23], the rail industry is dominated by its three Class 1 carriers, Canadian National, Canadian Pacific (Int 45) and VIA Rail. As with other subsectors, size and capacity were important themes in the rail interviews. CN and CP have their own police departments (Int 5). This allows the railways to be much more attuned to security issues and arguably more self-sufficient.

With respect to standards, trucking is much more fragmented from a regulatory perspective compared to airports or seaports [19] (Int 48). While there are some national standards, such as the National Safety Code 1987 [24] and those issued by the Commercial Vehicle Safety Alliance, regulation is primarily a provincial responsibility and as a result the regime includes a variety of different regulations across the country [25]. Interprovincial trucking is nationally regulated but is still subject to the regulations of each province it enters. The voluntary certification programs such as FAST, C-TPAT and PIP place obligations on firms to undertake a number of measures to improve their security procedures and adopt best practices, which entitles them to a lower risk classification. Gaining this status can expedite inspections and border crossings, and lead to fewer compliance audits. These programs apply not only to trucking but to rail as well.[2]

Inconsistency emerges as a recurring theme in the trucking interviews. Interview subjects cited the lack of uniformity in the credentials required for drivers to gain access to areas such as rail yards or ports as one example in a subsector with considerable inconsistencies across jurisdictions. Truck drivers undergo multiple checks, all verifying similar information to obtain access cards for the locations in which they deliver freight. One subject noted that this process has been stream-lined in the US (Int 9) although transportation specialists noted execution problems there also.

Despite regulatory responsibility for rail being shared by the federal government and the provinces and territories, the influence of the federal government is more pronounced in rail and, as such, standards across the country are more uniform (Int 43; Int 44; Int 45). Unlike aviation or seaports, there is no act focused primarily on security for the rail sector: security is based on the Railway Safety Act (1985)[26], the Transportation of Dangerous Goods Act (1985)[27] and the International Bridges and Tunnels Act (2007)[28]. Recently, new provisions were added to the Railway Safety Act (1985)[26] via the Safer Railways Act (2012)[29], which aims at enhancing safety by creating a 'culture of safety' within railways and an industry-wide safety management

[2] C-TPAT and PIP also include manufacturers and retailers. PIP is the Canadian program and C-TPAT is the US program; many Canadian and Mexican companies also belong to the US program.

system, similar to the mechanism in place in aviation [30]. There are no similar provisions concerning security.

While the recent audit by the Auditor General [23] raised concerns about safety practices in rail, interview subjects underscore that in fact safety culture is much more pronounced in rail than security culture. One interview participant noted that there simply is not a culture of security present in the rail sector as there is with safety; security typically is not a priority and as a result is not considered in the majority of strategic planning sessions (Int 45). This is particularly true for short rail lines, which rely on the local community law enforcement and the Railway Association of Canada (RAC) for security concerns. As with trucking, standards for security are based on best practices shared between operators and derived from the economic incentive to remain a trusted participant in the overall system (Int 45). The security plans that railways do develop and submit to the regulators and industry associations tend to be high level and do not conform to any specific standard (Int 5).

When asked to describe the contextual issues that influence how they spend their time, rail interviewees reflected a more corporatist environment, which prizes stability; interview subjects were more concerned with the media and, like aviation, the law. Trucking interview subjects, on the other hand, were more concerned with immediate market pressures, including insurance, the laws and citizens/consumers. When asked, trucking interview subjects expressed the most concern over risks associated with cargo theft and major collisions causing service disruption. When it comes to security, in particular, rail interview subjects expressed the most concern over risks associated with terrorism and public access points to rail infrastructure.

In sum, in trucking, standards vary across jurisdictions, and behaviour modification depends on a number of market pressures in particular, including customer demand, insurance, laws and private rewards gained from membership in sometimes voluntary organizations. Individual service providers have less capacity to influence policy decisions; the sector as a whole seems ad hoc/less coherent in its approach to security than the other sectors. Whereas trucking seems to have a pluralist dynamic, rail has a corporatist one [31]. Government and industry interactions are influenced significantly by CN and CP; laws and media attention influence their actions most. Economic and safety considerations receive attention; at the time of the interviews, security seemed to be less of a concern. For SMEs, there is a reliance on the local law enforcement community and the RAC for information and standards regarding security risks.

3.4 Bridges

Bridges are often under the jurisdiction of the provinces or local governments. Approximately 1% of the bridges in Canada are federally owned [32]. Some are also privately owned; the federal railways, for example, maintain over 4,600 rail bridges across the country [23]. Standards are primarily aimed at safety, with relatively less emphasis on security. The interviews do not refer to any concrete security standards for bridges in the Canadian or international context. The provincial safety standards vary; many include measures that relate to security, but are not expressly security standards. Bridges that fall under the federal International Bridges and Tunnels Act (2007)[28] are the exception. This Act does include security measures, but they apply only to the 25 vehicular international bridges and tunnels, and nine international railway structures that are covered under the Act [33]. Our interview participants, both Canadian and international, noted that bridge authorities tend to develop their own security measures in part by collaborating with

other bridge authorities and adapting standards used by them (Int 16, Int 18). These measures are shared best practices (Int 2) and not enforced by government oversight. For the majority of bridges, there are fewer clear security standards or protocols promulgated by government.

There are strong behaviour modification mechanisms in place with regards to safety. However, as already noted, there is an absence of clear standards for security and accordingly there is no mechanism to enforce security standards. One interview participant noted that security is mainly about communication with the security agencies; bridges are open and vulnerable and security is about sharing threat information (Int 16). When asked to weigh which contextual issues influence the manner in which they spend their day, bridge staff were more influenced by engineering risks and how the bridges are perceived by the media and local public. Compared to the other sectors, they were less concerned about the law, insurance (most are self-insured) or about expanding their contacts with other owner and operators of critical infrastructure. When asked, bridge staff expressed the most concern over risks associated with severe weather events.

In sum, major CI bridges are unique in the transportation sector in that they are effectively monopolistic. They are also immovable and open to the public and business, 24/7. They have limited built-in redundancy, or at least a failure has an immediate and significant impact in the broader community it serves. Bridge staff share information and best practices with staff from other bridges. They are mostly concerned with safety and technical/engineering risks. While there is a strong regulatory regime in place for safety, security is largely based on shared best practises and relationships with local law enforcement and other bridge staff.

3.5 Food

A key feature of the Canadian food supply chain is its complexity. In addition to consumers, the chain comprises suppliers, producers, processors, manufacturers, restaurants and retailers of varying size and sophistication, from small family-owned farms to multinational companies. A widely reported trend is the continued consolidation and industrialization of the food supply chain [34]. Today, the chain is a tightly coupled, interconnected system, with changes in one sector or location often producing extensive repercussions. At the same time, the overall food supply chain contains distinct commodity value chains (beef, pork, grains, etc.). These value chains may be further differentiated by product and location; a capital-intensive beef farm, for example, faces different pressures and risks than a fast-food hamburger restaurant [35].

All participants in the overall food supply chain are implicated to some degree in controlling food safety and security risks. With respect to food safety, the Canadian Food Inspection Agency (CFIA) is the lead agency at the federal level. Table 3, adapted from a CFIA report, illustrates the roles and responsibilities of the various actors in the supply chain in terms of addressing safety risks.

Table 3: *Safety responsibilities in the Canadian food supply chain*

International	Provincial/ municipal agencies	CFIA	Other federal departments	Industry	Consumers
Global food supply Market and trade Comparability and acceptance of food systems Meet import requirements, provide export requirements	Enforce food safety laws within their jurisdiction Inspection, public health and food safety surveillance	Delivers federal food inspection programs Investigates foods linked to illness outbreaks Initiates food recalls	Lead public health surveillance and outbreak investigations Develop health policies and standards and conduct health risk assessments	Responsible for the production of safe food in compliance with government standards	Responsible for safe food handling and preparation

Source: [36].

With respect to standards, a major theme in both our interview data and the academic literature is the heavily regulated nature of the Canadian food supply chain. This is particularly the case in the area of food safety. Standards are the product of both federal and provincial legislation and industry self-regulation programs. At the federal level, the relevant legislation includes the *Food and Drugs Act*, the *Canada Agriculture Products Act*, the *Meat Inspection Act*, the *Fish Inspection Act*, the *Consumer Packaging and Labelling* Act, as well as other statutes related to food production, distribution and processing (see [37]). As noted above, complementary legislation exists at the provincial level. CFIA is responsible for implementing the standards emanating from federal statutes. Interview respondents highlighted the stringency of these standards in areas such as food disposal (Int 53), distribution (Int 53; Int 57; Int 59), importing (Int 52) and processing (Int 56).

Importantly, the current federal regime will undergo major changes in 2015 when the *Safe Food for Canadians Act* enters into force. The Act was introduced in part in response to the 2008 listeriosis outbreak. According to federal government documentation, the Act will consolidate many of the food provisions administered by CFIA into a single statute, establish new authorities to develop regulations around traceability and ensure consistency across inspection and enforcement [38].

In Canada, federal and provincial standards are often informed by industry-developed standards. Garcia Martinez *et al.* describe this approach to standard setting as a new "paradigm in stakeholder relationships characterized by complex interactions between public and private modes of regulation" [39]. A prominent example of this approach is the Hazard Analysis and Critical Control Points (HACCP) method, which gained initial attention due to efforts by pork,

chicken and egg commodity associations to develop voluntary safety codes. HACCP was later formally recognized and, in certain cases, made mandatory by the CFIA.

Government standards are usually deemed the minimum threshold for participating in the market. That is, major commodity associations generally require members to implement standards that surpass government safety criteria. Among hog processors, for example, the CQA program, based on HACCP principles, is considered the industry standard, or requirement of sale, and many processors adhere to standards beyond the CQA (Int 56). This is similarly the case among grocers (Int 53), beef producers (Int 57) and food banks (Int 59).

The globalization of food supply chains means standards in Canada are increasingly shaped by international trends. Under WTO agreements on the liberalization of trade in food commodities, Canada must adhere to international sanitary and phytosanitary standards [40]. Perhaps more influential, however, are private standards, whose rise has coincided with the global consolidation of supermarket chains. Wielding significant buying power, the so-called 'hypermarkets' are able to impose preferred standards on suppliers [41]. In the Maritimes, supermarkets are not sufficiently concentrated to promulgate their own standards (Int 51); instead, many retailers subscribe to global systems, such as the Global Food Safety Initiative (GFSI). Table 4, adapted from a 2013 report by Grant and colleagues for the Conference Board of Canada, illustrates the prominence of private standards in Canada.

Table 4: Summary of Private Standard Systems in Canada

Collective-National Systems	**Sites Certified**
Canada Organic	3,914 farms 815 processors 380 handlers
CanadaGAP	916 (2,000 producer enrollees)
FeedAssure	170

Collective-International Systems and GFSI	**Sites Certified**
Safe Quality Food (SQF)	313
British Retail Council (BRC)	300
FSSC 22000	56
International Featured Standard (IFS-Food)	10
Global Food Safety Initiative (GFSI)	Loblaw (all private-label suppliers) Sobeys (majority) Metro (40 per cent)
GMP+ (feed)	105
Marine Stewardship Council	(6 fisheries in full assessment)

Inter-Company Systems	**Suppliers**
McDonald's Supplier Quality Management System (SQMS)	108
McCains food safety system	450
Loblaw private label suppliers (GFSI)	860

Public Schemes	**Sites Certified**
HACCP (federally registered)	1,482
Ontario Advantage HACCP/HACCP Plus	21

Source: [42].

On issues of food safety, the Canadian food supply chain is thus subject to a complex and dense web of public and private standards. The blurring of the line between public and private regulatory systems is known in the literature as co-regulation [39][40]. Overall, interview respondents described the existing standards in Canada as adequate. Although one respondent suggested that Canadian consumers face higher costs due to the expenses associated with meeting safety standards (Int 53), in general interview respondents expressed satisfaction with the existing safety regime (Int 52; Int 53; Int 56; Int 57; Int 59).

Other risk types, such as security risks and natural disasters, are less regulated than food safety (Int 60). Security remains largely the purview of individual firms (Int 52). Similarly, interview respondents reported few standards around emergency management planning (Int 57; Int 60). Business continuity planning generally occurs on a firm-by-firm basis (Int 60), and few arrangements are in place to coordinate commodity value chains in the wake of a disaster (Int 57). Among retailers, during an emergency it is the responsibility of individual supermarkets to determine whether to donate food (Int 53). Given their limited storage and distribution capacity, food banks have only a small role to play in terms of mitigating food supply risks (Int 59). Much

of the challenge in addressing these hazards stems from the centralization of distribution networks and the 'just-in-time' imperative of the overall supply chain. Indeed, the sector's thin margins incentivizes retailers to eliminate excess inventory, which means many regions in Canada would rapidly run out of food should a major distribution centre or transportation network be affected by a disaster (Int 53).

Behaviour modification is conducted through a mix of public and private mechanisms. The CFIA possesses a variety of enforcement tools, including the authority to issue warnings, suspend or cancel licences and refuse entry into Canada of food shipments [43]. None of our interview respondents spoke directly to the quality of CFIA enforcement activities. With respect to the enforcement of provincial standards, one respondent suggested that additional funding and staffing is necessary to ensure full compliance by producers in Nova Scotia, many of whom raise and slaughter livestock for personal use and are therefore difficult to monitor (Int 57).

For private standards, enforcement is conducted by third-party certification organizations that conduct inspections and verify compliance [41]. The integration of private standards into public statutes means government inspections often serve as a compliance mechanism for both types of standards. As well, compliance with private codes of practice presents an opportunity for government regulators to "distinguish between high and low risk establishments and focus inspections efforts accordingly" [39]. However, this sort of reverse capture may be problematic for small firms, which might not have the financial capacity or technical expertise to adhere to costly programs intended for larger operators [39].

When a food risk to human health is identified, a recall may be initiated. Since 2006, there have been 200 to 300 food recalls each year in Canada [44]. The CFIA is responsible for coordinating food recalls. The decision to initiate a recall, however, is made by the implicated firm. The success of a recall depends to some extent on the traceability of the affected product (Int 53). The Auditor General of Canada recently conducted a performance audit of the food recall system. The audit concludes that the first stages of the recall process—from when an issue is identified to when a recall decision is made—"are generally working well" [44]. Problems, however, were identified with the decision-making procedures used during an emergency response (i.e. a high-risk recall), which are not well understood by Agency staff. The Auditor General also identified weaknesses in CFIA's follow-up after a recall. The report describes as inadequate the monitoring and documentation used by CFIA to ensure that an affected product has been properly corrected or disposed of [44].

In addition to enforcing standards, behaviour modification in the food supply chain includes government efforts to affect consumer behaviour, for example with respect to properly cooking meat. Consumer knowledge and behaviour appears to vary according to commodity type. Pork tends to be overcooked by most consumers (Int 57), whereas fish and seafood products are often handled with less care (Int 53). Consumer concerns are a significant issue for participants in the food supply chain. Interview respondents emphasized that a food incident could have negative repercussions for public perception of an entire commodity sector (Int 56; Int 57). When given a list of contextual issues relevant to our framework and asked which contextual issues influence the manner in which they spend their time with respect to safety and security, interview respondents in the food supply chain scored citizen or consumer concern higher than any other issue. The average score assigned to citizen or consumer concern, 8.6, was also second highest

among all interview respondents, trailing only the average score for that issue among trucking respondents (9.0). (See Figure 4.)

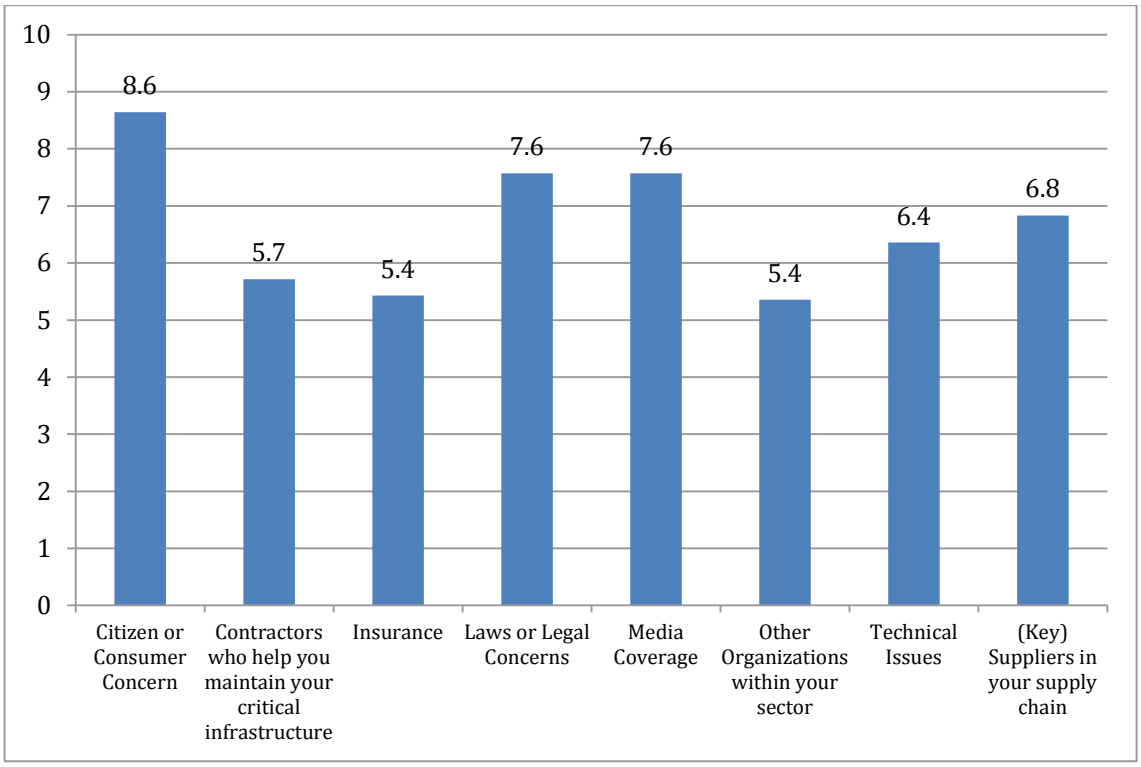

***Figure 4**: Responses from food supply interview participants to the question: "How would you rate the influence of the following subjects on how you spend your time with respect to matters of safety and security?" (n=7; results based on the mean rating given for each statement across participants on a 10-point scale in which 10 means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it')*

Note: The small sample size in Figure 4 would preclude the use of any rigorous statistical analysis to support generalizations of the findings. We present the data as indicative of the relative importance of the contextual influences as assessed by these individual interview subjects and use it as a departure point for analysis and discussion.

In sum, standards for the food supply chain are rule-oriented, extensive and aggressive, and emanate from both public statutes and private codes of practice. The line between public and private regulation is increasingly blurred, and some private programs have been integrated into government standards. International factors, such as trade liberalization under the WTO and the consolidation of retailers, serve as a key influence on private standards. Most standards address food safety issues; there are fewer standards on business continuity and emergency management. Behaviour modification is achieved through a combination of public and private tools, including product recalls and inspections. Overall, the control mechanism is characterized by systemic complexity, proactivity and a high density of formal regulatory rules, with a distinct emphasis on food safety over other risk types.

3.6 Canadian CI in Comparative Perspective

3.6.1 Transportation

3.6.1.1 United States

After the events surrounding 9/11, the US federal government shifted many of its resources to counter-terrorism activities, in particular counter-capability measures of "hardening" key points of access and critical assets [45]. While the issue of terrorism has defined much of the CI protection landscape in the US over the past 13 years and many of the interviews focused heavily on terrorism (Int 39; Int 24; Int 6; Int 19; Int 2), it was identified by some CI owner operators as being a less significant threat than it is perceived to be (Int 36; Int 4). Funding for CI protection initiatives in the US is in decline, with a federal respondent citing the lengthy period of time since the last major incident and lack of effective metrics to provide Congress with quantifiable evidence that funding has made the US safer (Int 24). Despite many improvements to the state of critical infrastructure during this period, much transportation infrastructure is ageing and deteriorating (Int 6; Int 19)—one respondent considered a major failure due to "infrastructure erosion" to be an inevitability (Int 6).

The concentration of government power will also have some influence over the way in which decisions regarding critical infrastructure can be made. In all subsectors of transportation, the Australian, Canadian and UK federal governments generally have more power, particularly on issues of security, than their local and provincial counterparts. However, barring a national security event, in the US, government power is typically more decentralized—state and local authorities have significant influence over policy, often working with local CI entities to grant regulatory exemptions.

Prioritization of critical infrastructure is a challenge, especially with respect to determining threat levels for CI; perceived threat levels change frequently (Int 39). National governments, state and local governments also often disagree on the importance of different CI entities. Federal government will prioritize CI using its preferred method of valuation to determine the level of federal funding to allocate to state and local governments for CI protection. The federal government will hold information sessions with state and local officials to ensure there is transparency with respect to method, which can become contentious. The recent solution has been for federal government to make determinations for funding based on its own risk calculations but to allow state and local governments to allocate that funding based on their own prioritization mechanisms (Int 39). The controversies concerning prioritization can also be exacerbated by the difficulty in determining what amount of risk is tolerable; politicians often do not want to acknowledge publically that a zero tolerance goal may not be achievable in an environment with finite resources (Int 24).

Information-sharing in government departments has matured dramatically over the past 10 years; which information can be shared with whom has been formalized through a growing bureaucracy (Int 39).[3] Fusion centres are "multi-agency, multi-jurisdiction groups" tasked with collecting,

[3] The interviews pre-dated WikiLeaks and Snowden. The insider threat now receives more attention in the US. As a result, US government officials may tighten regulations about sharing too much information across organizational lines and to lower organizational levels.

filtering and disseminating information on a need-to-know basis, a small portion of which is classified (Int 2). The increased emphasis on competition in the US means that firms are often less willing to share in information fora compared to firms in the UK, Australia and Canada.

Port security standards are similar in in US and Canada – both are governed by federal acts that set out standards and both are subject to periodic inspection or audits. Due to broad standards, ports in both countries have a degree of autonomy in how they meet standards.

In all areas of critical infrastructure protection, the US is placing increased emphasis on propagation, informing the citizenry of its efforts and articulating the need of those efforts (Int 39).

3.6.1.2 Australia

Post 9/11, Australia has not experienced a major terrorism event though the attacks in Bali in 2002 killed Australians on holiday, and the Australian government has detected and arrested terrorist cells working in Australia. Australia's CI community is currently "re-shifting and re-focusing" in light of the transition to a model that identifies seven critical sectors (Int 20). A part of this major refocus there is increased emphasis on building resilience into the system; resilience and information technology advisory groups have been established to cut across and consult with all sectors (Int 14, Int 26).

Trusted Information Sharing Networks (TISN) were established in 2003 (Int 26) and are organized by the Attorney General's department. Australian respondents indicated no issues with revealing secrets to the competition as a barrier to sharing information in TISNs, calling the networks "very transparent" and observing no breaches of confidentiality (Int 14). One government official did note that there was public concern about the possibility of collusion between businesses in these groups; in fact, the formation of TISNs had to be reviewed and approved by the Australian Consumer and Competition Commission (Int 26). While many respondents feel positive about the usefulness of the TISN framework (Int 26; Int 14), one noted that their TISN was struggling to be useful due to lack of industry support, citing the economic crisis moving industry's focus away from activities that are not perceived as having immediate economic value (Int 20).

In the transportation sector, one Australian respondent noted concerns of "security fatigue" as a major concern for the maritime and port sector, as well as emergency management, natural events, interruption of fuel supply, interruption of power and interruption of communication (Int 20). Amongst the transportation groups, the most common concerns were interruption of liquid fuel supply, natural events, pandemics and coordination between orders of government (Int 20). Concerns of terrorism only surfaced as a major concern for the surface transportation group, which may be a result of the presence of an alternative transport security committee whose sole focus is counter terrorism (Int 20).

As noted above, one US respondent felt that Australia in particular was more advanced in establishing security standards and suggested that groups are trying to establish international standards (Int 39).

3.6.1.3 United Kingdom

In England and Wales coordinating CI protection for government is the role of the Cabinet Office (Int 28; Int 27). One interviewee indicated that incidents such as the BSE outbreak in the 1990s have led to a common understanding amongst many that one failure in the sector can have a negative impact on the sector as a whole and has made the private sector more conducive to sharing information with competitors (Int 18). Setting of priorities occurs at both the central government, with lead departments being commissioned to develop a sector resilience plan, and at the local level where "local resilience forums prepare for emergencies" (Int 27).

The Cabinet Office does prioritize risks based on what they call "reasonable worst case scenarios" for which they freely distribute information and plans (Int 27). They are, however, limited to natural events, as information around terrorism is deemed too sensitive for distribution (Int 27).

There is a general perception in the UK that the threat level of terrorism at this particular time is low compared to the US (Int 18) and that the US has done much more work on protecting surface transport infrastructure from terrorist threats (Int 18). Increased activity in the Middle East by western countries, including the UK can change this, of course. Ageing infrastructure is also not considered to be a major issue in the UK as in the other countries (Int 17). Flooding, however, has been a substantial issue in the UK. In response, the government has established a collaborative partnership between the Environment Agency and the Met Office (agency responsible for forecasting weather and monitoring climate change) to offer a single resource for information on forecasting and managing floods (Int 28). While they have become adept at forecasting fluvial floods, surface water flood and flash flood forecasting remain a challenge (Int 28).

3.6.2 Food

Although, as noted above, standardization is occurring across the global food supply chain, both our interview data and the academic literature indicate that the Canadian regime remains unique in several respects. First, there is a sense that the Canadian food supply is among the most extensively regulated in the world (Int 53). As well, despite the growing influence of private codes of practice, public standards continue to exert a greater influence in Canada than, for example, in Europe [39][46]. In the UK, private standards are deeply integrated into the public regulatory scheme, in part due to retailer market power and the collaborative orientation of the EU regulatory environment (Int 55)[39].

A noticeable difference is also evident between Canada and the US, particularly with respect to the preference for both market-oriented and legal mechanisms. The US food sector is, according to some, more competitive (Int 55), and market solutions to risk management are preferred over traditional, top-down methods, which are seen as a last resort [39]. Given Canada's export-oriented economy, meeting international (primarily American) standards is a key objective for both governments and producers, whereas internal, domestic pressures are the primary concern for American producers [46]. Further, the institutional structure of the American system, in which the courts play a significant role in regulating firm behaviour, means the US regime relies heavily on "tort and market mechanisms, in addition to government's efforts" [47]. Canada's parliamentary system, in comparison, arguably supports a more prescriptive regulatory approach.

In Canada, Australia and the UK, there is evidence of closer collaboration between industry and government in terms of information sharing than in the US (Int 54; Int 55; Int 56). Compared to Canada, however, Australia appears to be more advanced in terms of industry-government collaboration with respect to emergency and business continuity planning, as evidenced by the degree of integration achieved through TISN (Int 54; Int 58). As well, Australian respondents expressed more concern about security risks to the food supply, including terrorism, than Canadian and British respondents, who noted that food safety, including unintentional contamination and animal health, remains their primary concern (Int 55; Int 57; Int 58; Int 60).

In sum, when we compare the interview transcripts at a national level, many of the assumptions of the literature hold. First, the US is more concerned about terrorism than the other countries though arguably the UK also expresses an elevated level of concern and not all interview subjects agreed that the focus should be on terrorism. The US also relies more on market mechanisms and less on direct government interventions to resolve issues than do other countries. That noted, no interview subjects said their industries compete on security or safety issues. All countries have public-private sector fora for sharing information about risks and all have mixed views about them although the Westminster countries seemed more optimistic about information-sharing than the US interview subjects. Getting the private sector engaged on an on-going basis seems to be one of the primary constraints for all. All countries also seem to be struggling with balancing transparency and privacy—both personal and corporate. The US has tried considerable engagement at the local level. Generally, these governments struggled with prioritization, how to develop performance metrics and the problems of overlapping responsibilities and multi-level governance. They also struggled with striking a balance between local priorities and central priorities.

4 Discussion: Identifying Salient Points from the Transcripts that Relate and Contribute to Developing Tools, Scenarios, Methods and Models that can Support the Risk and Emergency Management Decision-making Process in New Brunswick

We start with salient points that relate to each subsector in transport, and then food. We would like to stress that we are applying to the New Brunswick case what we found during our research in CI. It should not be assumed, however, that our findings are drawn from interview subjects in New Brunswick, in particular.

4.1 Airports

The interconnected nature of air travel, the high media profile, political attention and psychological impact of terror attacks (or potential attacks) by air and the shared political and corporate interest over aviation security means that New Brunswick has extensive, expensive and probably excessive security regulations and this is likely to continue. Airports are highly regulated and integrated into the security apparatus because considerable attention and resources have been committed to this sector since 9/11. Indeed, security has always been part of organization of airports and as a result, 9/11 simply built on those practices. There are very few (if any) publicly known incidents that might be classified as major security threats at New Brunswick airports; that noted, information in this domain is not always freely available.

New Brunswick airports generally are small. Very little freight is transported by air because of the expense involved. The risks that might exist for New Brunswick airports are: high cost of safety and security regulations such that they might be overlooked or marginalized (small airports in particular complain about being over-regulated and the cost of it); that staff may not know how to respond to a security event when it happens because it would seem so unlikely they would be caught off guard. (This kind lack of reaction has been noted in small Eastern European airports in recent research.) An even more likely scenario would be that a New Brunswick airport would have to accommodate flights because a major international incident overseas or an event in the US has taken place, as we saw in the Atlantic region during 9/11. In sum, airports seem low risk, relatively speaking. It would be useful, however, to identify products and services that are critical to New Brunswick and depend on air transport. Airports can also be crucial for remote regions, and even though they might not be financially viable would nevertheless receive government attention in the event of a CI failure. Despite the airports' claims that terrorism is their number one concern, bad weather seems more likely to disrupt operations. At the same time, media and political scrutiny nationally and internationally following a failure in this sector can be significant. It would also be interesting to know what excess capacity NB airports have, in the event they have to accommodate additional flights due to an international event.

4.2 Seaports

Imports and exports to and from the US via New Brunswick ports are fairly modest; from all other destinations it is significant for the province. In our research, we found staff in this sector to be the most anxious. Seaports are squeezed between intense market pressure and the need to maintain a safe and secure environment. In addition, while staff are expected to generate revenue and act like a business, they also have a quasi-government status, which increases their sensitivity to political issues and broadens their concern beyond bottom-line efficiency considerations. While the ports themselves are federal, in order for a port to be successful, it requires the coordination and support of all three orders of government, which increases complexity and transaction costs. It also means there might be public disputes between orders of government during a CI event, which generates media coverage, politicizes the issue and may have a direct impact on emergency management policy decisions. Staff frequently do not understand where safety and security fit in the order of priorities; they also feel safety and security standards generally are unclear. They do feel the pressure to remain profitable. If a port were to decide to conduct an extensive audit of goods, the goods would be delayed from their final destination, sometimes considerably because checking goods can be a lengthy process. Staff feel reluctant to delay goods, particularly for important clients.

We believe it would be helpful to examine the consequences of slowing trade at a major port, such as the Port of Saint John. It would also be helpful to test scenarios in which there were security lapses at the port. In other words, what level of tolerance do we have for slowing trade at the Port of Saint John? How quickly can it recover from an event? Ports are also concerned about extreme natural events—Saint John is on a hurricane path. They are also concerned about their social license and environmental protesters. They can also experience labour unrest—the shipping industry has strong unions. Union leaders are concerned about members working under dangerous conditions. Ports can be exposed to local and international criminal activity, including the movement of illegal drugs and weapons and people-trafficking and people-smuggling. Ports are also concerned about security related to cruise ships. Finally, the port, like airports, might examine its capacity to take extra ships during extreme events elsewhere. Halifax, for example, took in ships headed for New York during Hurricane Sandy. Finally, it would be useful to know what institutional arrangements exist that can allow for a quick and coordinated response by all three orders of government during an event.

4.3 Rail

Rail has a fairly robust safety system, especially among Class 1 carriers. It is not as fully integrated into the government security regime as airports. Class 1 rail carriers have their own police force and intelligence gathering and maintain a level of independence; they are also privately owned in a highly competitive market and therefore seem less inclined towards the rigid, integrated and at times excessive security model of airports. At the same time, Class 1 carriers dominate the market, constitute a powerful lobby and are a key service provider and employer. In this type of dynamic, making changes proactively is difficult if it is against the companies' interests. There are several risks to supply chains that include rail. First, while Class 1 carriers dominate, small and medium-sized enterprises are vulnerable because they are working on smaller margins; it is not clear that they carry adequate insurance or have business continuity plans. This creates risks. SMEs are also not as integrated into government safety and security apparatus and as a result they may not be as aware of low-probability risks or emerging threats.

In other words, distinguishing between Class 1 carriers and SMEs would be helpful because their risk profiles are almost certainly different. Secondly, ageing bridge infrastructure may also represent a threat to moving cargo. The railway goes through a number of smaller towns; this creates a risk when transporting dangerous goods because few small towns would have the resources to contend with a spill. Thirdly, the increased demand for oil might put more pressure on the system and generate more accidents; it might also generate more protests and attacks by protestors against rail companies transporting oil and their critical infrastructure. Relatedly, and unlike airports, so much of rail infrastructure is exposed without any direct supervision or security.

Unlike Nova Scotia, New Brunswick has some degree of redundancy in its railway line. Like other subsectors, the question of risk tolerance becomes crucial: What are the consequences of a rail line failure? How long can we tolerate it? What is the recovery time?

Rail stops in small towns are very important for the local community. They bring goods to and from the community and by allowing manufacturing companies to locate near these stops they create jobs crucial to the livelihood of the community. Therefore, rerouting trains or closing these stations would be controversial. At the same time, many stations can also create important redundancies. In sum, rail is an important source of transportation in the supply chain and a highly competitive market. The size of the carrier makes a difference: SMEs seem more vulnerable than Class 1 carriers. Communicating with SMEs and ensuring they have adequate safety practices in place seems like a challenge. Much of the infrastructure is exposed and this creates vulnerabilities.

4.4 Trucking

Trucking is the most adaptive of the subsectors and as result is critical to the supply chain during a major risk event. There are many service providers but they are not necessarily well organized; the industry is very customer-focused and is sensitive to costs and particularly the cost of oil. The challenge will be to coordinate it during an event; a strong relationship with the industry association will help. So too would appropriate technology for communicating with truck drivers quickly. CI owners and operators are encouraged to have strong working relationships and contingency plans with trucking service providers and industry associations. Individual trucking companies are also likely to respond to strong market signals and market incentives. There are other coordination problems: because of the jurisdictional complexity, there seems to be redundancy in administrative processes. Also, because three orders of government regulate the movement of goods by truck, there is increased chance of disputes between governments during an event; these disputes politicize the issue and change the dynamics of the decision-making process. These administrative inefficiencies may constrain the adaptive capacity of this subsector, whose flexibility during a risk event could be crucial. It will be important to look at single points of failure that could disrupt the movement of goods by truck. Flooding experiences in Australia suggest that it can be difficult to get crucial food items into major population centres if critical roads are blocked, for example.

4.5 Bridges

Bridges are monopolistic and immovable and are critical transportation hubs; if one goes down, it could be down for months, if not years. It will be important to consider redundancies and

tolerance for the failure of bridges in New Brunswick. Bridges are often built because they are crucial links but cost of construction and maintenance can make the development of redundant systems impractical. A failure of a bridge therefore can be a long-term problem. Like rail, the infrastructure is very exposed with few safety or security mechanisms in place; they are also open 24/7.

4.6 Food

Research suggests people go to grocery stores multiple times in any given week; an Australian post-floods study concluded that many people seem unable to cope without food readily available at their grocery stores; the sector is becoming increasingly concentrated due to a diminishing number of distribution centres (and slaughter houses); as a result, the consequences of single points of failure can be high. Generally, the industry works on a just-in-time model, so there is very little slack in the supply chain. As noted, Australia experienced floods that prevented critical food supplies from arriving in major cities; Brisbane was one day shy of running out of bread. New Brunswick is also susceptible to floods. Many food producers are particularly sensitive to the value of the American dollar because they ship goods to the US. An event that causes a change in the value of the American dollar (which rose after 9/11, for example) may change the behaviour of food producers and in so doing put pressure on the Canada/US border. The food industry is also sensitive to international standards and international image. The regulatory complexity and over-lapping responsibilities of three orders of government, international trading partners and regulators means there can be public disputes amplified by media coverage during an event. We saw an example of disagreement and lack of coordination by different levels of government during the 2008 listeriosis outbreak. We have very little experience with deliberate acts of contamination, so industry and public response to such an event would be unclear. Our research suggests that industry can handle safety recalls but is less well prepared for security events. The sector is bringing in new regulations and changes in the regulatory regime create risks. Finally, agriculture depends on large volumes of potable water and, while this is somewhat outside the scope of food, anything that jeopardizes the water supply can create risks to the food supply.

4.7 Observations from the Comparative Perspective

Building a model that depends on reliable data and regular use by CI owners and operators will require buy-in from key CI stakeholders and an ongoing commitment by them to it. CI owners should have regular input into the development of the model and the model should be shown to serve the interests of the CI community, not just government agencies that design it. The CI community should have regular meetings but not so often that it becomes a burden and people lose interest. While this will be a challenge it seems manageable in the NB context in which the number of CI owners and operators is not that large; the smallness of the community gives NB a considerable advantage in contacting key CI owners and operators and creates a face-to-face accountability culture that will pressure groups to participate.

A more difficult challenge in many ways will be establishing broader public accountability. Face-to-face accountability will work within a group but it is less clear how—if at all—government will report its work to the public. First, public sector/private sector groups do not articulate how the networks will report on progress to outside parties. Volunteer members, paying

their own way and with the responsibility for the community's critical assets, are unlikely to join if they believe they will be embarrassed if such membership threatens their share value or reputation. Unwanted disclosures would also undermine any trust that the governments would like to establish with these groups. Second, it is unclear how the sectors will prioritize risks, agree on standards or force behaviour change. Non-hierarchical groups are good at generating ideas, but bad at making and enforcing decisions. The US situation provides many examples of these challenges.

5 Types of Risk: Observations from the Social Science of Risk Literature that Underscore the Importance of Identifying Risk Characteristics Before Establishing a Risk Governance Decision-making Process

Renn [1] divides risks into four classes: simple, complex, uncertain and ambiguous. The classification of risk is "not related to the intrinsic characteristics of hazards or risks themselves but to the state and quality of knowledge available about both hazards and risks" [6]. Simple risks are those for which predicted events are frequent and the causal chain obvious, such as car accidents. This section examines complex, uncertain and ambiguous risks in more detail and relates them to decision-making and modelling. Different risk types require different processes to manage the risk. For more on the IRGC Framework, see Annex B.

5.1 Complex Risks

Complex Risks are those where there is difficulty "identifying and quantifying causal links between a multitude of potential causal agents and specific observed effects" [6].

This difficulty may arise from, but is not limited to:

- Interactive effects amongst potential causal agents
- Long delay periods between cause and effect
- Inter-individual variation (i.e., greater differences from case to case)
- Intervening variables.

Risk modelling is, by definition, a method applied to analyse simple risks and complex risks. Whereas simple risks are associated with phenomena that are relatively frequent with fairly well understood causal links, extending these rational quantitative methods can become increasingly unreliable as the risk situation becomes more complex. The fundamental process of decomposition during model formulation is often inadequate to capture interactive effects between system elements. Furthermore, each cause and effect relationship in the complex system is typically inferred assuming prompt linear reactions, and yet many systems are characterized by non-linear interactions and delayed feedback. This latter aspect has been shown to confound attempts to fully grasp the full extent of consequences of a hazard [46]. A classic example is mad cow disease (bovine spongiform encephalopathy, BSE, and its human variant Creutzfeldt-Jakob disease, CJD), where symptoms may emerge more than 50 years after infection in humans. Thus accurately modeling the risks of this scourge has been, and continues to be, somewhat speculative.

To compensate for deficiencies in historical data which preclude developing statistically valid cause and effect inferences, modellers turn to probability theory to estimate likelihoods based on limited data and/or expert opinion. The expected value, or expected utility, underpinning a rational risk assessment model must be viewed judiciously given these limitations in the data and relationships. Comparisons with other apparently similar scenarios are often made to help define

the system scope and cause and effect relationships; however complex systems are rarely mirrored very well in other contexts. Modelling risks for Critical Infrastructure Protection is often subject to these conceptual challenges. While the model can help inform decision-makers, prioritize problems and examine vulnerabilities and sensitivity, the actual evolution of an incident may be quite different from anticipated model outputs. Nevertheless, modelling to gain insight into potential outcomes from the failure of a complex system can be instrumental for building in redundancy to lessen the likelihood of failure propagation, and adding buffers to mitigate the impacts.

The caution here is the human tendency to overestimate our ability to understand, model, and control the complexities of a large system. A debate on this issue has ensued for many years between proponents of High Reliability Organizations (HRO) and Normal Accident Theory (NAT) [47]. In brief, HRO postulates that humans can continue to improve their monitoring and control of technological systems even as they grow larger and more complex, while NAT theorists counter that not only does this demonstrate hubris, but the potential impacts of failures are growing exponentially along with the system scope. The Fukushima disaster [49] and the Deepwater Horizon oil spill [50] are two recent examples of our limited capacity to predict complex interactions between multiple causes despite the development of many germane risk models in those industries. The food supply chain would generally fall into this category, with apparently straightforward distribution networks actually comprising disparate elements of varying reliability, and all subject to a wide variety of hazards that have somewhat unpredictable effects on the system continuity and stability.

5.2 Uncertain Risks

Uncertain risks are those where there is "a lack of clear scientific or technical basis for decision making," which "often results from an incomplete or inadequate reduction of complexity in modelling cause-effect chains." This diminishes the confidence level of traditional objective measures of risk estimation and becomes more reliant on "fuzzy" or subjective measures of risk estimation" [6].

Categories of uncertainty:

Epistemic (a result of imperfect knowledge) – characteristics include:

- Target variability
- Systematic and random error in modelling

Aleatory (a result of randomness) – characteristics include:

- Indeterminacy or genuine stochastic events
- System boundaries
- Ignorance or non-knowledge

With uncertain risks it is important to understand that formal, rational models are unlikely to capture the full scope of the challenge. Uncertain risks can frequently generate surprises or realizations that are not anticipated or explained explicitly within a risk modeling framework. Examples include rare natural disasters, terrorism and pandemics. There are simply not enough data to understand the full reach of the risk. A recent Canadian example includes the 2009

influenza A H1N1 pandemic. It was seemingly under control when suddenly a healthy 13-year-old boy died just as the vaccine became available. The probability of contracting H1N1 did not change but because of high-profile coverage of the death, there was a surge in demand for the vaccine for which health officials were seemingly unprepared [51]. Hurricane Katrina also provides a salient example. It was a rare event but one that had been theorized and anticipated for over 150 years, and it occurred during an Administration that had emergency response—though for terrorism—as its number-one priority. Yet FEMA seemed unprepared; different orders of government were not coordinated. The disaster included acts and allegations of heroism, luck, murder, racism, street violence, looting, rape, claims of assisted suicide, blame-shifting among political parties, concern over medications and pets, and the list goes on and on. With uncertain risks, we do not fully appreciate how interdependent a system is until it fails.

The absence of data that can help officials to be more specific about the magnitude of the risk requires that government employ a precautionary approach, particularly when the harm is potentially catastrophic or irreversible [52]. (A discussion of the precautionary principle and the controversies associated with it follow.) Uncertain risks also require that government avoid high vulnerability as best as it can. At the same time, it is unrealistic to think that a plan would dictate that sufficient human resources would constantly be available to respond to worst-case scenarios. Adaptive capacity and a diversity of means to accomplish mission-critical tasks are necessary. Developing surge capacity—the ability to quickly add to available resources to meet a surge in demand—will build resilience during the occurrence of uncertain events. Solutions will require risk modeling coupled with a reflective discourse by regulators, experts, industry and affected stakeholders that attempt to strike the balance between over- and under-managing the response to the event. Scenario-planning exercises can help provided they infuse an element of the unpredictable into the scenarios—not merely test for scenarios for which everyone is prepared, among friendly and convenient CI partners who are prepared to join the exercise.

5.3 Ambiguous Risks

Ambiguous risks are a result of divergent or contested perspectives on the justification, severity or wider 'meanings' associated with a given threat [6]. Examples include low-dose radiation and nuclear power. For this type of risk, broad public consultation is important and solutions are usually provisional until more reliable data become available. In the case of ambiguous risks, there is little disagreement on the data; there is disagreement, however, on what the data means. How the risk is framed is a key consideration when responding to an ambiguous risk. Fracking, for example, can be characterized as a clean, low-cost domestic energy source, which can be profitable for local economies and provide energy security for future generations. It can also be characterized as a source of energy that pollutes, jeopardizes a clean environment for future generations and exploits vulnerable populations for the purposes of making wealthy corporations wealthier. Both characterizations are fraught with controversy.

Categories of ambiguity:

Interpretative – (i.e., different interpretations of the same results)

Normative – (i.e., different concepts of what can be considered tolerable)

Examples: low-dose radiation (interpretative) and nuclear power (normative)

When modelling the risks, how the risk is framed (or characterized) is important, as is the process stakeholders establish to resolve conflicts and arrive at a stable solution. These kinds of risks can frequently pit one group against another and can include extreme reactions by ideologically-driven groups. Risk modelling alone will not solve this problem. Solutions rely on modelling coupled with political bargaining and trade-offs between different risks. The process should involve agency staff, industry, stakeholder and sometimes the general public. If there is broad-based consensus that competing groups have legitimate claims, then risk governance processes normally proceed with caution and continue to gather information until a resolution can be achieved. Provisional solutions are put in place.

Like uncertain risks, ambiguous risks can easily default into the precautionary principle. This approach is not without controversy.

5.4 The Precautionary Approach: Competing Definitions and Controversies

When evidence is contradictory or inconclusive, decision-makers often lack justifiable rules to select the best alternative. One response to dealing with such uncertainty has been the adoption of the precautionary principle, a generally more 'cautious' or 'conservative' approach to dealing with uncertainty. There are many definitions for the precautionary principle, each with slightly different emphasis. The writers noted below discuss three trends. Often advocates of the precautionary principle argue in favour of delaying implementation until there is more (scientific) certainty concerning the long-term impacts of a particular initiative. (Equally, they can argue in favour of stopping an existing program because scientists are unsure of its long-term impacts.) The concept emerged from debates over environment policy, but it is also debated in the area of science and research policy. At times, the precautionary principle has been a contentious concept.

5.4.1 Precautionary Principle: Three Definitions

The Precautionary Principle emerged as a decision-rule for regulating environmentally hazardous activities in the *Swedish Environment Protection Act* of 1969 [53]. The Act states: "the mere risk of harm, if not remote, warrants protective measures or a ban on the activity that is possibly causing harm." Since its first appearance, variations of the principle have been adopted in several national environmental laws, including those in Germany, Australia, Canada, New Zealand, Switzerland, the US and the UK. The precautionary principle is also invoked in numerous international treaties, most notably the 1992 Maastricht Treaty (EU) and the United Nations Conference on Environment and Development at Rio de Janeiro in 1992: the Convention on Biological Diversity and the UN Framework Convention on Climate Change.

The Precautionary Principle is a contentious term and various definitions exist for it. The following discussion draws significantly from the work of Khefeits, Hester and Banerjee [54] who highlight three trends in the precautionary principle, each with different emphases and degrees of severity. They summarize the trends in the following manner:

1) Where there are threats of serious irreversible damage, uncertainty should not be a reason for postponing action to prevent damage.

It could be paraphrased more positively as 'Consider taking action even if there is no conclusive evidence that harm is occurring.' This statement does not provide clear guidance for determining what action should be taken under any specific circumstances. It necessitates additional analysis based on other decision rules.

2) Where there are threats of irreversible damage, precautionary measures should be taken even if cause-and-effect relationships are not clearly established.

This much stronger statement essentially says, 'do something' in the face of threatened harm. But it does not provide any clearer guidance as to what action should be taken than the first definition. What it does do is rule out taking no action. In this sense, this version (and stronger ones) appears to call for action no matter what and hence to imply that uncertainty alone justifies action.

3) Whenever an action or substance could cause irreparable/irreversible harm, even if that harm is not certain to occur, the action should be prevented and eliminated.

This definition requires not just some action, but extreme action that totally eliminates the practice or substance that could be causing harm. It forbids consideration of other issues, such as benefits that may result from practice, as well as consideration of the degree of harm that may be caused and the degree of uncertainty about whether the harm will actually occur.

5.4.2 Precautionary Principle: Implications

Although each of the above definitions appears as a precautionary principle, there are important differences.

The strength of evidence required to justify action differs. The principle may be adopted when there is (1) 'sufficient evidence' that an action or substance is harmful; (2) when there is no conclusive scientific proof one way or the other; or (3) when the substance or action has been suggested as a possible cause.

The necessary action also differs. Definitions of the precautionary principle imply a wide range of actions that should be taken once the strength of evidence requirement has been satisfied. These actions range from (1) prevention or elimination of exposure; (2) adoption of cost-effective action; or (3) mere consideration of action.

Another important difference is who bears the burden of proof: (1) the opponents of a possibly harmful action; or (2) the proponents of a possibly harmful action. For example, if a government were considering a law that was intended to help decrease the rate of global warming, would the government look to industry to prove that its carbon emissions, for example, are not affecting global warming? Or would it look to the environmental groups to prove that the industry carbon emissions are affecting global warming?

Definitions of the precautionary principle also reflect differing degrees of risk aversion.

While not strictly synonymous, the principle is closely associated with other cautionary approaches to risk management, such as ALARA (i.e., 'as low as reasonably achievable') or ALARP (i.e., 'as low as reasonably practicable').

Despite the various approaches to the precautionary principle, the principle generally is criticized as a potentially costly approach to risk management. Critics of the approach argue that a general rule (or 'blanket' approach) for risk minimisation leads to inefficiencies and the neglect of priority setting. Even if uncertainties are high it is more prudent to guess probabilities of harmful effects rather than treat all risks as equal. Prioritizing may involve subjective judgement, but this is superior to the assumption that all risks have the same probability and magnitude.

The Precautionary Principle has also brought to light important questions about how science and scientists are potentially used in the policy process. Given the inherent uncertainty of the situations, different scientists may arrive at different conclusions about the likelihood of certain risks materializing. Some have noted that people tend to support the findings of scientists that uphold their preferred views or solutions and discard or discredit the work of those that do not.

Finally, note that the precautionary principle tends to reward some and penalize others. Political scientists, for instance, often ask themselves, 'who wins' by the adoption of a certain rule or approach? With respect to the precautionary principle, it is worth reflecting on who wins and who loses by the adoption of the principle, and what that can tell us about the power structures that are at work in the society.

When we model risks, we need to consider whether or not the risk can be classified as complex, uncertain or ambiguous. One key feature will be the reliability of the existing data. If it is an uncertain risk or ambiguous, are the consequences potentially catastrophic or irreversible? If so, should we adopt a precautionary approach? If so, which of the three definitions of the precautionary principle are we using? Who will pay and who will benefit from this approach?

5.5 Trust and Transparency

Developing trust between the public and private sectors is cited frequently in many Western governments' CIP strategies (see, for example, Australia, Attorney-General's Department 2003 [55]; for the United Kingdom, Centre for the Protection of National Infrastructure 2006 [56]; United States, Department of Homeland Security 2008 [57]). Trust increases group cohesion [58]. In this case, governments seek to develop trust relationships with and among CI stakeholders in the public and private sectors to facilitate, among other things, the exchange of sensitive information about vulnerabilities and collective action towards a common goal.

Although social scientists have given considerable attention to the problem of defining trust, a concise and universally accepted definition remains elusive. As a consequence, the term "trust" is used in a variety of distinct and not always compatible ways in organizational research [59][60]. Kramer [60] describes several ways to think about trust: *history-based trust*, which characterizes trust as something that evolves over time and is based on past experiences with individuals; *category-based trust,* based on membership; and *roles-based trust,* based on one's place or formal authority in an organization. Hardin [61] argues that the key is trustworthiness—the context that allows trust to develop—and that its value is in making social cooperation possible and even easier. Generally, there are two broad tendencies in defining trust. Some formulations highlight the strategic and calculative dimensions of trust in organizational settings; others emphasize the relational and social context for building trust.

Peters, Covello and McCallum [62] identify three dimensions that people tend to look for in others to develop trust: knowledge and expertise; care and concern; and openness and honesty (cited in [63]). These concepts can be applied equally at the organizational level [64]. The concept of open communication, in particular, appears repeatedly in research on developing organizational trust [65] and encompasses free data sharing, inclusive decision making, and collaborative work [66][58].

Calman [67] notes that trust comes on foot but leaves on horseback. It is easy to lose because negative information that can diminish people's feelings of trust is more attention-grabbing, more powerful and often more readily available than positive information [63]. CI failures are particularly susceptible to this bias because they tend to be spectacular and generate considerable media coverage. In a study of British railways post-privatization, for instance, Jeffcott and colleagues noted that fragmentation, performance regimes, proceduralization, loss of expertise and major accidents all affect the trust relationships across industry [58].

If governments assume the sociocultural approach to trust, none of the three conditions identified above (knowledge, care and openness) is readily achieved in CIP. To start, the complexity and interdependence of the networks arguably make knowledge claims suspect. With terrorist acts and pandemics, the absence of reliable data makes the magnitude of the risk problem uncertain [48], and also referred to in the section above). Even care and concern might be difficult to achieve. Sato [68] concludes that trust effects weaken as group size increases; participants feel their impact is less in larger groups, which arguably leads to a sense of helplessness or even indifference rather than one of care and concern. Finally, government also faces a trust/transparency conundrum. On the one hand, researchers note that "open communication" is a prerequisite to organizational trust. On the other hand, too much transparency might make owners and operators of CI nervous about disclosing information on vulnerabilities to government.

While most governments refer to trusted *partnerships* with industry, in many cases they may actually be referring to *dependencies*. Government takes risks when it aspires to be seen as a "trusted partner" in this context. CI and emergency events can result in clashes over public and private sector accountability structures [69][70]. Industry responds to its shareholders and is rewarded for taking successful risks. Government has a regulatory role to play on behalf of citizens to ensure appropriate adherence to standards. Strengthening these relationships can produce stability and collegiality among regulators and CI owners and operators, but may also result in compromises on transparency and prevent dramatic changes, if required [71].

Trust is important for the modelling process because in order for the model to be successful, stakeholders will have to trust the data, the process and the participants. In order to generate trust, however, the group must convey openness, knowledge and concern. Concern can be enhanced if, first, stakeholders' interests are aligned, and second, if there is strong group cohesion among stakeholders and a commitment to the community. Knowledge is more easily obtained in complex risks, which depend on experts. When responding to uncertain risks, however, we need to build up the knowledge and expertise in adaptive capacity and surge capacity because surprises occur with uncertain risks. When confronted with ambiguous risks, we need to have a good process in place that key stakeholders and the public support. Finally, the group will have to determine the degree of openness with which it is comfortable. Security work often has to strike a balance between a variety of different concepts—transparency, secrecy, privacy, discretion, competitive advantage and ministerial accountability. Ultimately, in order to generate trust, the

group should be oriented towards openness but respectful of its membership. This will likely include discussions among group members about appropriate levels of disclosure, under what conditions and with whom.

6 Conclusion

In this paper, we had three primary goals: (1) to summarize the findings of our interview transcripts with regulators, owners, operators and managers in selected subsectors in transportation and food supply; the interviews are largely with Canadian officials, however, we also conducted interviews with US, UK and Australian officials in order to provide some comparative context (see section 4); (2) to extract observations from these transcripts to help the research team identify opportunities to improve the scenarios, methods and modelling that we are working on in this project in order to improve decision-making during emergency events (see section 5); and (3) to draw on the academic literature on risk governance, trust and the precautionary principal to identify opportunities to improve risk decision-making processes and challenges that the tools and methods we develop must address (see section 6).

With respect to our first goal, we summarize the transcripts in the following manner. Airports are controlled through process-focussed formal regulations; they rank terrorism as their primary concern and have a strong security regime in place. Rail is controlled through considerable regulation but is more independent, dominated by Class 1 carriers and sensitive to market pressures; they are concerned about public points of access to critical infrastructure. Seaports have competing market and regulatory pressures that are held in perpetual and at times extreme tension; staff are concerned about many critical infrastructure (CI) risks but particularly about rare and extreme natural events. Bridges are monopolistic and controlled through regulation; they are concerned with complex technical infrastructure. Trucking is the most flexible of the subsectors—the others in the transportation sector are immovable; it is decentralized and market-sensitive. The control mechanism for the food sector is characterized by systemic complexity, proactivity and a high density of formal regulatory rules, with a distinct emphasis on food safety over other risk types. Note that the small sample size of interview subjects in any one sector would preclude the use of any rigorous statistical analysis to support generalizations of the findings.

With respect to the second goal—extracting observations for this project—we make the following observations.

- Relatively little freight is transported by air. Airports seem like comparatively low risk with respect to supply chain disruption. It would be useful, however, to identify products and services that are critical to New Brunswick and depend on air travel. Airports may also be crucial for remote regions. Bad weather is perceived as the type of event most likely to disrupt operations. At the same time, media and political scrutiny nationally and internationally following a failure in this sector can be significant, particularly in the U.S. Finally, airports may suffer from risks due to over-regulation (e.g., people over-looking the rules, or being too processed- and not outcomes-focussed); staff at smaller airports, typical of New Brunswick, tend to describe rules and regulations as excessive given the risk.
- Seaport trade is particularly important for non-U.S. trade in New Brunswick. As noted above, we found seaport staff to be the most anxious. Staff are squeezed between market and efficiency demands and meeting safety and security standards; they do not necessarily know what priority they should give security and when security concerns

should override efficiency concerns. We believe it would be helpful to examine the consequences of slowing trade at a major port, such as the Port of Saint John. What level of tolerance do we have for slowing trade at the Port of Saint John? How quickly can it recover from an event? Ports have many risks but events do not receive the same attention as they do in aviation, for example. Seaport staff are concerned about local and international criminal activity, natural disasters, environmental protesters, strikes and labour unrest and accommodating other ships due to risk events elsewhere.

- Class 1 rail carriers and small and medium-sized rail companies have different risk exposure; SMEs have less financial flexibility and as a result may build less redundancy into their systems. SMEs are more easily over-looked because they are not as integrated into the decision-making process as Class One carriers are. Moreover, small and remote towns depend on the rail line for goods, services and employment, but are ill-equipped to cope with major risk events. Rail infrastructure is also exposed with little supervision, particularly in remote areas. All of these factors should be considered when conducting a risk assessment of rail in NB.
- Trucking is the most adaptive of the transportation subsectors and as result is critical to the supply chain during a major risk event. There are many service providers but they are not necessarily well organized; the industry is very customer-focused and is sensitive to costs and administrative and regulatory demands. The challenge will be to coordinate the sector during an event, including through the use of appropriate technology which does not seem to exist at present.
- Multi-level governance increases time and transaction costs and the likelihood of disputes during events; these disputes can politicize the issue and change the dynamics of the decision-making process. Risk assessments should consider the number of governments that are involved in regulating the source of the risk; the number can vary significantly depending on the subsector; in the case of multiple regulators, regulators should ensure adequate and stable means of communicating between different stakeholders exist during risk events and on an on-going basis.
- Bridges are monopolistic and immovable; if a bridge becomes disabled, it could be down for months, if not years. It will be important to consider redundancies and tolerance for the failure of bridges in New Brunswick.
- Generally, the food industry works on a just-in-time delivery model. Recent research of natural disasters in Australia suggests many people seem unable to cope without food readily available at their local grocery stores; the number of distribution centres and slaughter houses is diminishing, making the sector increasingly concentrated at this point in the supply chain. Consequences of single points of failure—either through distribution centres or roads—can be high. Risk assessments should consider the vulnerability of the supply chain through single points of failure as well as the population's capacity to cope without regular access to food at the local grocery store. Finally, while safety processes are deeply embedded in the food sector's organizational culture, security practices are less so. The operational implications of the distinction between a safety event and a security event should be examined more closely.
- An event that causes a change in the value of the American dollar may change the behaviour of food producers that export to the US and in so doing put pressure on the Canada/U.S. border. In our interviews, food producers were aware and sensitive to the value of the US dollar; they were less aware of other risks in the supply chain.

- Building a model that depends on reliable data and use by CI owners and operators will require buy-in from key CI stakeholders and their on-going commitment to it. This is particularly difficult during tough financial times when organizations are short on staff resources. In order to maintain reliable models and methods to support decision-making during an emergency, CI owners and operators should be involved in the design of the methods and should develop routines within their organizations to update the data and train staff on the use of tools and methods.
- The relatively small size of the New Brunswick critical infrastructure community gives it a considerable advantage in contacting key CI owners and operators and also creates a face-to-face accountability culture [72], which will pressure groups to participate, and do a good job. It can also generate high group cohesion and high group trust which makes oversight and coordination less costly. There are challenges with this type of dynamic. First, public sector/private sector groups will need to articulate clearly how the networks will report on progress to its members and outside parties, such as to the public. Second, it is unclear who and how groups will prioritize critical infrastructure in the province during an event, agree on standards or motivate appropriate behaviour change, when necessary. These decisions will be sensitive and will have cost implications for owners and operators and government, and political implications. Generally, non-hierarchical groups are good at generating ideas, but bad at making and enforcing decisions. We will need to address these issues as the project progresses.

With respect to our third goal—drawing lessons from the risk governance, trust and precautionary principle literature, respectively—we make the following observations.

These observations are focussed on developing a risk management process that can lead to a more effective decision-making process during an emergency event. These observations do not necessarily focus on the 'decision moment' itself but rather how—in the context of risk events that typically involve many interested parties, accountability is frequently shared and interests are not always aligned—do we put processes in place in advance of an event to generate a context for better risk management that will generate better outcomes during an event.

Different types of risk require different approaches and different levels of engagement with stakeholders prior to making decisions. Renn [48] describes three types: complex (e.g., aging infrastructure), uncertain (e.g., terrorism) and ambiguous (e.g., conflict over aboriginal rights). The risks are distinguished largely by the quality and certainty of the information and knowledge that we have about the risk. We believe it will be important to identify the type of risk with which we are dealing in order to develop an appropriate solution. Each of the different risk types requires different levels of engagement with experts, stakeholders and the public, for example, and different degrees of adaptive capacity.

Risk of low-probability/high-consequence events frequently lead to a precautionary approach. The precautionary principle is commonly used but poorly defined and a decision to invoke it is not without controversy or ambiguity. It can be an extremely costly way to conduct risk management and arguably the concept has several contradictions inherent within it. It should be applied selectively—usually when the consequences can be catastrophic or irreversible, such as a nuclear event—and with an awareness of who pays for it (including opportunity costs) and what risks are being overlooked as a result of the decision to pursue the precautionary approach.

Precautionary approaches should be revisited regularly. When we do adopt a precautionary approach, as for fracking, for example, we need to continue to collect data to confirm the magnitude of the risk and the appropriateness of the risk management process.

Trust among members of a supply chain can increase group cohesion, which can increase adaptive capacity during emergencies. There are three dimensions that people tend to look for in others to develop trust: knowledge and expertise; care and concern; and openness and honesty. None of these is easily achieved in critical infrastructure protection or emergency management, particularly when there is a strong market/competitive context. A lack of trust can undermine the model and the process. Owners, operators and regulators will have to generate conditions that are conducive to a trusting context or else recognize that the models and methods may not be fully trusted by those using them. This in itself is not necessarily a bad thing; many good governance processes can be built with a degree of skepticism as opposed to trust. It does, however, contradict the conventional wisdom in CIP, which frequently cites trust among stakeholders as desirable.

Our second and next report will use the Hood *et al*. risk regulation regime framework in particular to identify contextual issues that influence the CI risk regulation regime for the sectors for which we have collected data. These contextual pressures will include market, public opinion and interest group pressures. We will also identify best practices for managing supply chains risks in light of the data that we have collected.

References/Bibliography

[1] Hood, C., Rothstein, H., and Baldwin, R. (2001). *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford, UK: Oxford University Press.

[2] Reniers, G., and Pavlova, Y. (2013). Introduction: Why a book on game theory for safety within the chemical industry? In G. Reniers, Y. Pavlova (Eds.), *Using Game Theory to Improve Safety within Chemical Industrial Parks* (pp. 1-11). London: Springer.

[3] Russell, D. and Simpson, J. (2010), Emergency planning and preparedness for the deliberate release of toxic industrial chemicals. *Chemical Toxicology*, 48: 171-176.

[4] The Centre for Protection of National Infrastructure. (n.d.). *The National Infrastructure.* Retreived March, 2014 from http://www.cpni.gov.uk/about/cni/

[5] Office of the Press Secretary, the White House. (2013). *Presidential Policy Directive – Critical Infrastructure Security and Resilience*. Retrieved from http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[6] Renn, O., Walker, K.D., & International Risk Governance Council (eds.) (2008). *Global risk governance: Concept and practice using the IRGC framework*. Dordrecht, the Netherlands: Springer.

[7] Madore, O., Shaw, D. J. (1993) The Canadian airline industry: its structure, performance and prospects. Retrieved from http://publications.gc.ca/Collection-R/LoPBdP/BP/bp329-e.htm.

[8] Brooks, M. R., and Prentice, B. (2001). Airport devolution: The Canadian experience. In *Seoul, Korea: World Conference on Transport Research,* July.

[9] Transport Canada. (2011a). Audit of Aviation Security Regulatory Oversight April 2011, Retrieved from http://www.tc.gc.ca/eng/corporate-services/aas-audit-870.htm.

[10] Transport Canada. (2013b). Program Activity Architecture 2011-2012, Retrieved from http://www.tc.gc.ca/eng/corporate-services/planning-paa-32.htm#s1.

[11] Transport Canada. (2013a). National Civil Aviation Security Program (CARAC), Retrieved from http://www.tc.gc.ca/media/documents/security/NCASP_FINAL_ENGLISH_%282%29.pdf

[12] Robert, W. P. J. (2008). *Toward Risk-Based Aviation Security Policy*. OECD Publishing; Éditions OCDE.

[13] Canadian Aviation Regulations (2012). Retrieved from http://www.tc.gc.ca/eng/civilaviation/regserv/cars/menu.htm

[14] Canada Marine Act. (1998). Retrieved from http://laws-lois.justice.gc.ca/eng/acts/c-6.7/

[15] Brooks, M. R. (2004). The governance structure of ports. *Review of Network Economics,* 3(2), 68-183.

[16] Transport Canada. (2013e). Canadian Port Authorities. Retrieved from http://www.tc.gc.ca/eng/policy/acf-acfi-menu-2963.htm

[17] Ircha, M. C. (2001). Port strategic planning: Canadian port reform. *Maritime Policy & Management, 28,* 2, 125-140.

[18] Brooks, M. R. (2007). Port devolution and governance in Canada. *Research in Transportation Economics,* 17*,* 237-257.

[19] Brooks, M. R. (2008). *North American Freight Transportation*. Northampton, MA: Edward Elgar Publishing Ltd.

[20] Marine Transportation Security Act (1994) Retrieved from http://laws-lois.justice.gc.ca/eng/acts/M-0.8/

[21] Canadian Trucking Alliance (2012). Snapshot of Trucking Industry. Retrieved from http://www.cantruck.ca/iMISpublic/Content/NavigationMenu2/CTAIndustry/TruckinginCanada/default.htmlois.justice.gc.ca/eng/regulations/SOR-96-433/

[22] Transport Canada. (2011b). Transportation in Canada 2011. Retrieved from http://www.tc.gc.ca/media/documents/policy/Transportation_in_Canada_2011.pdf

[23] Office of the Auditor General of Canada (2013a). Fall Report of the Auditor General of Canada. Retrieved from http://www.oagbvg.gc.ca/internet/English/parl_oag_201311_e_38780.html

[24] Transport Canada. (2013d). National safety code 1987. Retrieved from http://www.tc.gc.ca/eng/mediaroom/backgrounders-b01-r118-1350.htm

[25] Kahai, S. K., and Ford, J. M. (1997). Economics of intrastate trucking regulation: Some empirical evidence. *Transportation Research Part E: Logistics and Transportation Review*, 33(2), 139-145.

[26] Railway Safety Act (1985). Retrieved from http://www.tc.gc.ca/eng/acts-regulations/acts-1985s4-32.htm

[27] Transportation of Dangerous Goods Act. (1985). Retrieved from http://www.tc.gc.ca/eng/acts-regulations/acts-1992c34.htm

[28] International Bridges and Tunnels Act (2007) Retrieved from http://laws-lois.justice.gc.ca/eng/acts/I-17.05/

[29] Safer Railways Act (2012). Retrieved from http://www.parl.gc.ca/About/Parliament/LegislativeSummaries/bills_ls.asp?ls=s4&Parl=41&Ses=1&source=library_prb&Language=E

[30] Transport Canada (2013g). Harper government launches Rail Safety Week with new funding for railway crossing improvements. Retrieved from http://www.tc.gc.ca/eng/mediaroom/releases-2013-h050e-7149.html

[31] Schmitter, P.C. (1977). Modes of interest intermediation and modes of societal change in Western Europe. *Comparative Political Studies,* 10(1).

[32] Transport Canada. (2012b). Road Transportation. Retrieved from http://www.tc.gc.ca/eng/road-menu.htm

[33] Transport Canada. (2013f). Harper Government introduces *Administrative Monetary Penalties Regulations* to support the *International Bridges and Tunnels Act*. Retrieved from http://www.tc.gc.ca/eng/mediaroom/releases-2012-h084e-6815.htm

[34] Sparling, D., Quadri, T. & van Duren, E. (2005). *Consolidation in the Canadian Agri-Food Sector and the Impact on Farm Incomes*. Ottawa: Canadian Agricultural Policy Institute. Retrieved from: http://www.capi-icpa.ca/archives/pdfs/papid11_dsparling.pdf

[35] Standing Committee on Agriculture and Agri-Food. (2013). *Toward A Common Goal: Canada's Food Supply Chain – Part 1*. Ottawa: House of Commons. Retrieved from: http://www.parl.gc.ca/content/hoc/Committee/411/AGRI/Reports/RP6226525/agrirp10/agrirp10-e.pdf

[36] Canadian Food Inspection Agency. (2013b). *Improved Food Inspection Model: Final Model*. Ottawa. Retrieved from: http://www.inspection.gc.ca/DAM/DAM-aboutcfia-sujetacia/STAGING/text-texte/acco_modernization_modeldraft_final_1371833418843_eng.pdf

[37] Canadian Food Inspection Agency. (2014). *Acts and Regulations*. Retrieved from: http://www.inspection.gc.ca/about-the-cfia/acts-and-regulations/eng/1299846777345/1299847442232

[38] Canadian Food Inspection Agency. (2012). Safe Food for Canadians Act: *An Overview*. Retrieved from: http://www.inspection.gc.ca/about-the-cfia/acts-and-regulations/regulatory-initiatives/sfca/overview/eng/1339046165809/1339046230549

[39] Garcia Martinez, M., Fearne, A., Caswell, J.A., & Henson, S. (2007). Co-regulation as a possible model for food safety governance: Opportunities for public-private partnerships. *Food Policy, 32*(3), 299-314. doi: 10.1016/j.foodpol.2006.07.005

[40] Henson, S.J. (2008). The Role of Public and Private Standards in Regulating International Food Markets. *Journal of International Agricultural Trade and Development*, *4*(1), 63-81.

[41] Fagotto, E. (2014). Private roles in food safety provision: the law and economics of private food safety. *European Journal of Law and Economics*, *37*(1), 83-109.

[42] Grant, M., Stuckey, J., & Le Vallée, J-C. (2013). *Pathways to Partnership? Private Food Standards in Canada*. Conference Board of Canada.

[43] Canadian Food Inspection Agency. (2013a). *Compliance and Enforcement Activities*. Ottawa. Retrieved from: http://www.inspection.gc.ca/about-the-cfia/accountability/compliance-and-enforcement/eng/1299846323019/1299846384123

[44] Office of the Auditor General of Canada (2013b). *Report of the Auditor General of Canada: Chapter 4: Canada's Food Recall System*. Retrieved from: http://www.oag-bvg.gc.ca/internet/docs/parl_oag_201311_04_e.pdf

[45] Wilner, A. S. (2012). Counter-capability and counter-motivation: a counterterrorism strategy for Canada. In McDonough, D. S. (2012). *Canada's national security in the post-9/11 world: Strategy, interests, and threats*. Toronto: University of Toronto Press.

[46] Hobbs, J.E., Fearne, A., & Spriggs, J. (2002). Incentive structures for food safety and quality assurance: an international comparison. *Food Control*, *13*(2), 77-81.

[47] Brewster, N.A., & Goldsmith, P. D. (2007). Legal systems, institutional environment, and food safety. *Agricultural Economics*, *36*, 23-38.

[48] Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World.* London: Earthscan.

[49] Acton, J.M. & Hibbs, M. (2012). Why Fukushima Was Preventable. *Carnegie Endowment for International Peace*. Retrieved from: http://carnegieendowment.org/2012/03/06/why-fukushima-was-preventable/a0i7

[50] Deepwater Horizon Study Group (2011). Final Report on the Investigation of the Macondo Well Blowout. Berkeley. Retrieved from: http://ccrm.berkeley.edu/pdfs_papers/bea_pdfs/dhsgfinalreport-march2011-tag.pdf

[51] Quigley, K., Quigley, J., & Macdonald, C. (n.d.). The Uncertainty of Uncertain Risks: Selected Print Media Coverage of Government Performance in Canada during H1N1. Manuscript under review.

[52] Sunstein, C.R. (2009). *Worst-case scenarios*. Cambridge, Mass: Harvard University Press.

[53] Sweden (1972). *Environmental Protection Act, Marine Dumping Prohibition Act*. Stockholm: Norstedt.

[54] Khefeits, L., Hester, G., & Banerjee, G. (2001). The precautionary principle and EMF: implementation and evaluation. Journal of Risk Research, 4 (2), 113-125

[55] Australia. Attorney-General's Department (2003). Trusted Information Sharing Network [website].Retrieved from http://www.tisn.gov.au/Pages/default.aspx.

[56] Centre for the Protection of National Infrastructure (2006). *CPNI* [website]. Retrieved http://www.cpni.gov.uk/

[57] United States Department of Homeland Security (2008). *One Team, One Mission, Securing Our Homeland: U.S. Department of Homeland Security Strategic Plan, Fiscal Years 2009–2013*. Washington, DC: GPO.

[58] Jeffcott, S., Pidgeon, N., Weyman, A., & Walls, J. (2006). Risk, trust, and safety culture in U.K. train operating companies. *Risk Analysis, 26,* 5, 1105-1121.

[59] Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (July 01, 1998). Not so different after all: A cross-discipline view of trust. *The Academy of Management Review, 23,* 3, 393-404.

[60] Kramer, R. M. (January 01, 1999). Trust and distrust in organizations: emerging perspectives, enduring questions. *Annual Review of Psychology, 50,* 569-598.

[61] Hardin, R. (2006). *Trust*. Cambridge: Polity Press.

[62] Peters, R., Covello, V., & McCallum, D. (1997). The determinants of trust and credibility in environmental risk communication: An empirical study. *Risk Analysis, 17,* 1, 43-54.

[63] Eiser, J.R., & White, M.P., (2006). A psychological approach to understanding how trust is built and lost in the context of risk. Workging Paper 12-2006. *Social Contexts and Responses to Risk Network.* Canturbury, U.K.: School of Social Policy, Sociology and Social Research, University of Kent.

[64] Gillespie, N., & Dietz, G. (2009). Trust repair after organization-level failure. *Academy of Management Review, 34,* 1, 127-145.

[65] Clarke, M.C., & Payne, R.L. (1997). The nature and structure of workers' trust in management. *Journal of Organizational Behaviour, 18,* 3, 205-224.

[66] Firth-Cozens, J. (2004). Organizational trust: The keynote to patient safety. *Quality and Safety in Health Care,* 13, 56-61.

[67] Calman, K. (2002). Communication of risk: Choice, consent, and trust. *Lancet, 360*, 9327, 166-68.

[68] Sato, K. (1998). Trust and group size in a social dilemma. *Japanese Psychological Research, 30,* 2, 88-93.

[69] Koliba, C. J., Mills, R. M., & Zia, A. (March 01, 2011). Accountability in governance networks: An assessment of public, private, and non-profit emergency management practices following Hurricane Katrina. *Public Administration Review, 71*, 2, 210-220.

[70] Koski, C. (January 01, 2011). Committed to protection? Partnerships in critical infrastructure protection. *Journal of Homeland Security and Emergency Management, 8*, 1.

[71] Vogel, D. (1986). *National Styles of Regulation: Environmental Policy in Great Britain and the United States* (Vol. 242). Ithaca, NY: Cornell University Press.

[72] Hood, C. (1998). *The Art of the State: Culture, Rhetoric and Public Management*. Oxford: Oxford University Press.

[73] Cowen, T. (1993). Public Goods and Externalities. In *The Concise Encyclopedia of Economics*. First Edition. Retrieved from http://econlib.org/library/Enc1/PublicGoodsandExternalities.html

[74] Niskanen, W. A. (1971). *Bureaucracy and representative government*. Chicago: Aldine, Atherton.

[75] Dunleavy, P. (1991). *Democracy, bureaucracy and public choice: Economic explanations in political science*. New York: Harvester.

[76] Downs, A., & Rand Corporation. (1967). *Inside bureaucracy*. Boston: Little, Brown.

[77] Wilson, J. Q. (1980). *The Politics of Regulation*. New York: Basic Books.

[78] North, D. W. (2005). Comments on the IRGC Framework for Risk Governance. In Renn, O., Walker, K. D., & International Risk Governance Council (eds.) (2008). *Global risk governance: Concept and practice using the IRGC framework*. Dordrecht, the Netherlands: Springer.

[79] Rosa, E. A. (December, 2005). White, Black and Gray: Critical Dialogue with the International Risk Governance Council's Framework for Risk Governance. In Renn, O., Walker, K. D., & International Risk Governance Council (eds.) (2008). *Global risk governance: Concept and practice using the IRGC framework*. Dordrecht, the Netherlands: Springer.

[80] Boholm, A., Corvellec, H., & Karlsson, M. (January 01, 2012). The practice of risk governance: Lessons from the field. *Journal of Risk Research, 15,* 1, 1-20.

[81] De Vries, G., Verhoeven, I., & Boeckhout, M. (April 01, 2011). Taming uncertainty: The WRR approach to risk governance. *Journal of Risk Research, 14,* 4, 485-499.

[82] Renn, O. (2006). *Risk Governance: Towards an Integrative Approach.* International Risk Governance Council.

[83] Aven, T., & Renn, O. (2010). *Risk management and governance: Concepts, guidelines and applications*. Berlin: Springer.

This page intentionally left blank.

Annex A Risk Regulation Regime Framework (Hood, Rothstein, and Baldwin, 2001)

Key observations from this section:

This section summarizes the Hood et al Risk Regulation Regime Framework in more detail. Note that this paper focussed on one aspect in particular—standard setting and behaviour change. Our second and next report will use the Hood et al. risk regulation regime framework to expand the analysis by identifying contextual issues that influence the CI risk regulation regime for the sectors for which we have collected data. These contextual pressures will include market, public opinion and interest group pressures. We will also identify best practices for managing supply chains risks in light of the data that we have collected. This section summarizes and highlights potential analysis for our next report; it is not meant to be an exhaustive account of the framework or our future reports.

Controlling information is only one part of a control system. A cybernetic understanding points to three components to a control system: information gathering, standard setting, and behaviour modification. Modern CI plans often assume that, by sharing information, standards and behaviour modification will occur. In the absence of more transparency, this is a potentially faulty assumption.

Depending on the subsector and indeed the organization, several factors can influence the extent to which organizations may be willing to share sensitive information, including competition, incentives, penalties, confidence, willingness, perceived importance of the information, concern over leaks, authority, liability and insurance concerns, organizational culture, market sensitivities, ownership and capacity, for example.

Public opinion can be volatile; the literature on the psychology of risk provides many insights into the potentially irrational and erratic reaction people have to risk events and CI failures. Governments, emergency services and the CI community have to respond to these reactions, which can be difficult to anticipate but can have a significant impact on the success of a post-CI event recovery operation.

Low-probability/high-consequence events generate high-volume media coverage for a concentrated period of time. Different types of events—natural disasters, industrial failures, terrorist plots, cyber events, for example—generate different types of coverage, not just in volume but in tone and in their search for accountability. Different sectors also generate different types of coverage. The volume of media coverage does not necessarily relate to the consequence (as measured in dollars) or probability of a disaster.

The concentration of power and authority in a sector can provide insight into whose interests are represented in supply chain regulation and whose are overlooked. It can also help us to anticipate which organizations will favour which changes to regulation regimes.

Security competes with a number of market and cultural/institutional pressures. Standing at the

ready for low-probability/high-consequence events can rarely be justified in market terms. When subsectors experience less competition and regulatory complexity and stronger incentives and organizational commitment to enact security, security practices are often more robust.

Despite in some cases being privately owned or at least privately operated, CI is crucial for our collective well-being and as a result governments are unlikely to let the service, if not the organizations that run them, fail outright, particularly monopolies and oligopolies. This arguably creates a moral hazard. After disasters and to varying degrees, governments often have to assume their role of insurer of last resort and assist in recovery efforts. This lessens the incentives for firms to assume robust risk management plans against low-probability events.

In their analysis of risk regulation regimes in the UK, Hood, Rothstein and Baldwin define regimes as "the complex of institutional geography, rules, practice and animating ideas that are associated with the regulation of a particular risk or hazard" [3]. Hood *et al.* hypothesize that within these regimes context shapes the manner in which risk is regulated. 'Regime context' refers to the backdrop of regulation. There are three elements that Hood *et al.* use to explore context: the technical nature of the risk; the public's and media's opinions about the risk; and the way power and influence are concentrated in organized groups in the regime.

Hood *et al.* [1] employ the cybernetic theory of control to examine the management of the specific policy area; they refer to this as 'regime content'. The theory asserts that if the three dimensions of control—information gathering, standard setting and behaviour modification—are under control, the system is effectively under control.

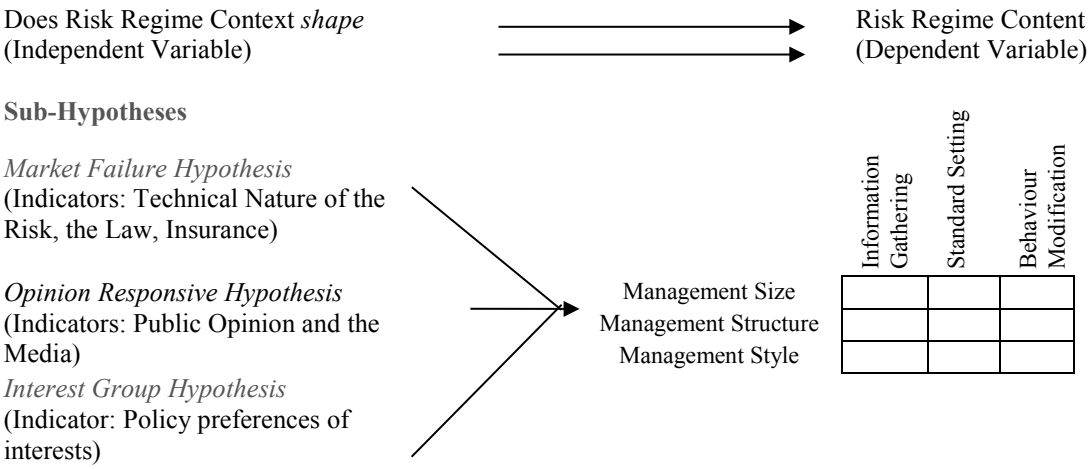

Figure: *Hood, Rothstein and Baldwin (2001): Understanding risk regulation regimes*

Content

We will discuss each of the three control components in turn. Information gathering is the capacity to obtain data that can be used to shape regime content. Information may be gathered actively or passively, both beyond the system and within it [1]. Standard setting involves establishing goals, or guidelines; in government, standards often take the form of policy. Finally, behaviour modification refers to the preferences, incentive structures, beliefs and attitudes that shape systems—the capacity to modify behaviour of participants is the capacity to change

systems. The distinction between these dimensions is not always tidy; Hood *et al.* [1] note, for instance, that information gathering may influence behaviour if people know they are being watched.
Each dimension of control may be further considered according to: size—the amount and scope of regulation and the resources used to sustain it; structure—the institutional arrangements of regime content, such as public-private sector relationships; and style—the formal and informal codes and conventions that help shape regime content [1]. Table 5 summarizes the relationship between the dimensions of control and regime content.

Table 5: *Influences of size, structure and style of dimensions of control*

	Information Gathering	Standard Setting	Behaviour Modification
Size	• The size of a regime's information gathering component is defined by the level of aggression and the level of resources going into IG from all sources, both private and public.	• Regulatory size in relation to SS can be conceived as the tolerance for risk, the degree of policy ambition and the level of time, skill and attention invested in standard development and revision.	• The size of the behaviour modification component can be understood from the funding and time committed by government and industry to enforcing the standards.
Structure	• The structure of a regime's information gathering component is characterized by the levels of third-party or private-sector contributions, as well as by a high degree of jurisdictional and system complexity	• One way of thinking about the structure of standard setting is to consider the extent to which standard development and revision involves a mix of public and private sector actors.	• The mix of private enterprise self-enforcement and government enforcement and the degree of overlap and complexity of said arrangements.
Style	• Conventions, attitudes, and processes of information gathering which determine whether IG is active (i.e., policing), passive (reactive) or interactive (e.g., auditing society).	• Style of SS can be defined by the overall extent to which regulation is governed by rules; regime style can be conceived by considering the cultural traits, or the attitudes and beliefs of standard-setters.	• A key feature of BM style is the mixture of compliance (e.g., diplomacy, persuasion, education) and enforcement (e.g., penalties, punishment) on risk regulation.

Context

Market Failure Hypothesis

The first hypothesis, the *Market Failure Hypothesis*, examines the government's intervention as a necessary one given the technical nature of the risk and the inability of the market to manage the risk effectively without such intervention. Most economic arguments for government intervention are based on the idea that the marketplace cannot provide public goods or respond appropriately to externalities. Public health and welfare programs, education, roads, research and development, national and domestic security, and a clean environment all have been labeled public goods [73].

The market failure hypothesis (MFH) posits that the content of a regime will reflect the extent to which markets fail to operate as regulators of socially unacceptable risk [1].

If the market failure approach to risk regulation is followed, regulatory size will be substantial only for risks where opt-out costs and information costs are high, and only for the specific control component that is affected by high costs. Conversely, if both information and opt-out costs were low, the market failure approach would lead us to expect regulatory size to be small. If information costs were high but opt-out costs were low, market failure logic suggests regulatory size would be high for information-gathering but low for behaviour modification. If information costs were low but opt-out costs were substantial, regulatory size would be low for information-gathering but high for behaviour modification. Figure 5 summarizes Hood *et al*.'s expectations of an approach to regulation dictated by the logic of market failure.

		Cost of obtaining information on exposure to risk	
		Low	**High**
Costs of opting-out of exposure to risk by market or contractual means	**Low**	Minimal regulation	Regime content high on regulatory size for information gathering, with behaviour modification through information dissemination
	High	Regime content high on regulatory size for behaviour modification	Maximal regulation

Figure 5: *Market failure explanation of regime size*

Source: Hood *et al.* [1]

Opinion-Responsive Hypothesis

The opinion-responsive hypothesis (ORH) means that a risk regulation regime is a certain way because that is how those affected by the risks want it to be [1]. In short, regime content reflects public preferences and attitudes. The availability of newspaper and media archives on the Internet enables us to draw on empirical data for our analysis. Here, we borrow from Hood *et al.*, who similarly use media coverage to gauge not public opinion per se but rather the flavour of public debate not least because leaders in civil society read these news sources. Figure 6 summarizes Hood *et al*.'s expectations of an approach to regulation dictated by the opinion-responsive hypothesis.

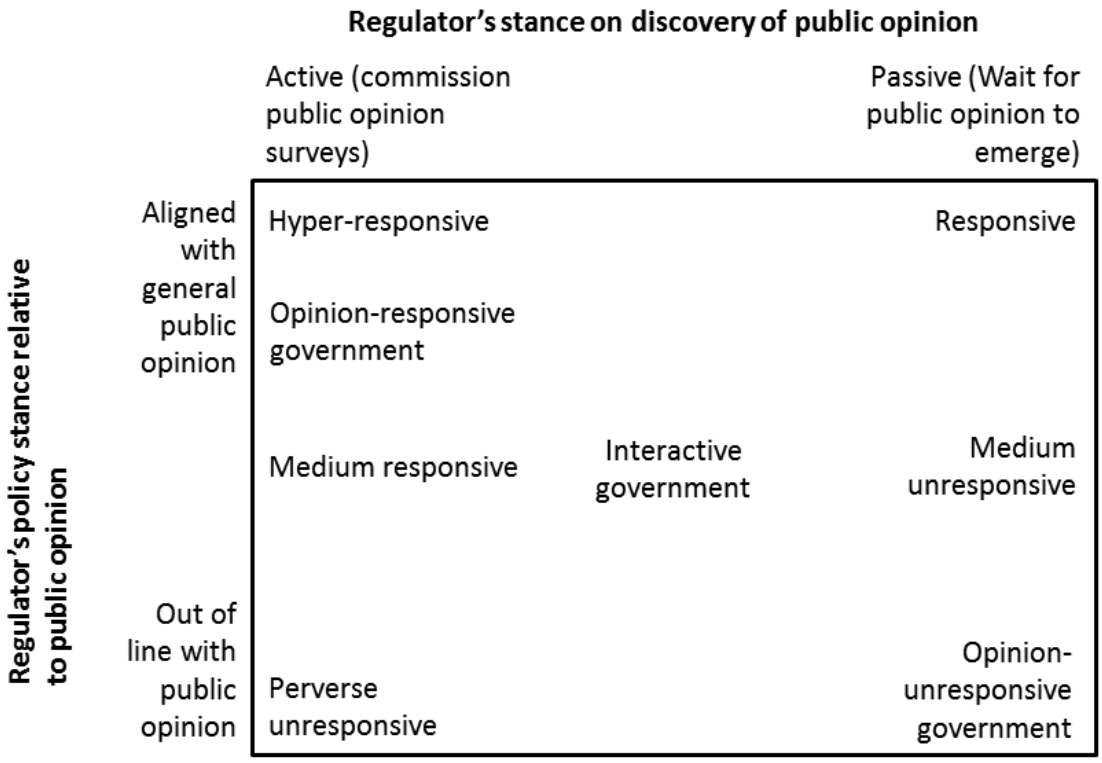

***Figure 6**: Observed regime content and opinion responsiveness, amended*

Interest Group Hypothesis

Hood *et al.* note that "various components and elements of regimes can be shaped by different organized interests" [1]. Political pressure of this sort can be difficult to study, given that public campaigns to influence policy are often complemented by informal, subtle or otherwise discrete lobbying efforts. The interest group hypothesis (IGH) thus necessitates an inferential approach, in which the preferences of relevant interest groups are assumed to be revealed by their function and observable behaviour. In the context of regulatory analysis, IGH directs our attention to the degree of alignment between these preferences and regime content, and where clear alignment *is* detected interest group pressure can be said to explain the regime. This is particularly true where regulatory policy is contested by multiple organized interests; here, alignment between content and preferences suggests that one group was 'victorious' and therefore better organized and more powerful than others.

One way to conceptualize interests is to study the benefits and costs of regulation. Put differently, IGH suggests that the concentration or diffusion of costs and benefits will affect the desire by an interest group to influence policy. According to the Stiglerian, or Chicago school perspective, business interests are often "the best-organized group in the policy domain" because their

"fortunes could be affected by price control or restrictions on entry to their markets" [1]. Regulatory capture occurs when these interests are successful in shaping the behaviour and decisions of regulators. Yet other (i.e. non-business) groups also attempt to influence government. Environmental organizations, for example, lobby governments to strengthen pollution standards. As well, Hood *et al.* contend that regulators themselves may be understood as an organized interest group. Although financial profit is not at issue, the economics and public administration literature highlights several other benefits that regulators may seek to maximize, such as their departmental budget [74], job satisfaction [75] or fulfillment from seeing personal preferences reflected in policy [76]. In any case, the IGH approach posits that the presence of well-organized interest groups in a policy area may be understood by examining how regulation affects the benefits and costs accrued by those groups.

Drawing on James Wilson's seminal book, *The Politics of Regulation* [77], Hood *et al.* illustrate the IGH using a two dimensional matrix, reproduced here.

Distribution of **benefits**

Distribution of **costs**	Diffuse	Concentrated
Diffuse	Majoritarian politics	Client politics
Concentrated	Entrepreneurial politics	Interest group politics

Source: Hood *et al.* [1].

Figure 7: *Interest group explanation of regime content*

Each quadrant in the matrix corresponds to a specific case, or type of regulatory politics. When both benefits and costs are diffuse, the matrix predicts the presence of what Wilson [77] calls majoritarian politics. The wide distribution of both benefits and costs means no group stands to gain from regulation and no group stands to lose. IGH overlaps with ORH in this situation, since the absence of organized interests means legislators craft regulatory content in light of prevailing public opinion.

The opposite situation, where both benefits and costs are highly concentrated, produces interest group politics. Ultimately, the key feature of interest group politics is that "whatever risk

regulators do is liable to advance some business interests at the expense of others" [1]. The concentration of benefits and costs means some groups must win and others lose.
The top right quadrant in Wilson's matrix, client politics, occurs in the presence of regulatory capture. This situation differs from interest group politics because the diffusion of costs means no group perceives itself as losing. "[T]he costs of the [regulation] are distributed at a low per capita rate over a large number of people," writes Wilson, "and hence they have little incentive to organize in opposition—if, indeed, they even hear of the policy" [77].

The final type, entrepreneurial politics, exists when a widely-dispersed and loosely-organized group (the public, usually) benefits from regulation that incurs a significant cost on a much smaller set of interests, such as a specific industry sector. Hood *et al.* call this the 'defeated Goliath' pattern [1]. This reflects our earlier point regarding ORH as a latent force, emerging out of major crises to disrupt 'normal' patterns of control and thereby creating the conditions for regulatory change.

Annex B The International Risk Governance Council (IRGC) Framework

Key Observation from this section:

The International Risk Governance Council's (IRGC) framework is a tool for developing a holistic approach to risk governance. Risk governance can be defined as the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analyzed and communicated, and management decisions are taken.

The framework includes four stages: pre-assessment, risk appraisal, tolerance and acceptability and risk management. It is an interdisciplinary tool and combines technical assessments with social concerns.

The framework will allow us to distinguish between different types of risk, including simple, complex, uncertain and ambiguous ones; the availability of reliable information is a key consideration in characterizing risk.

Different types of risks will generate different types of risk solutions. Expert advice, modelling, adaptive capacity and stakeholder and public engagement vary depending on the type of risk.

The framework emphasizes that risk management is an ongoing process that requires a commitment to institutional learning and perpetual refreshing of data.

The model also focusses on more controversial and challenging aspects of risk management, such as articulating a tolerance for risk, resilience, problem framing and prioritization.

The International Risk Governance Council's (IRGC) framework is a tool for developing a holistic approach to risk governance [1]. It was developed by German sociologist Ortwin Renn. Risk governance can be defined as the totality of actors, rules, conventions, processes and mechanisms concerned with how relevant risk information is collected, analyzed and communicated, and management decisions are taken. The framework takes into account different schools of thought on risk for an interdisciplinary approach. On a more macro level, the framework divides the components of risk governance into two broad categories: risk assessment and risk management. Assessment is focused on the generation of knowledge surrounding a risk, and management is concerned with deciding on and implementing actions to deal with that risk. On a more micro level, the framework breaks this process into four phases: pre-assessment, risk appraisal, tolerability & acceptability judgment, and risk management. Each phase is further sub-divided into the components that should be considered in each stage. While the framework is divided into these separate phases and presented in a sequential manner, it is necessary to understand that risk governance does not necessarily occur in this sequence. At times, each of these phases can occur simultaneously, and communication flows back and forth, further informing or shaping the overall risk governance response.

Figure 9 illustrates the basic interconnections of the phases within the framework and will act as a graphical reference for the remainder of this section.

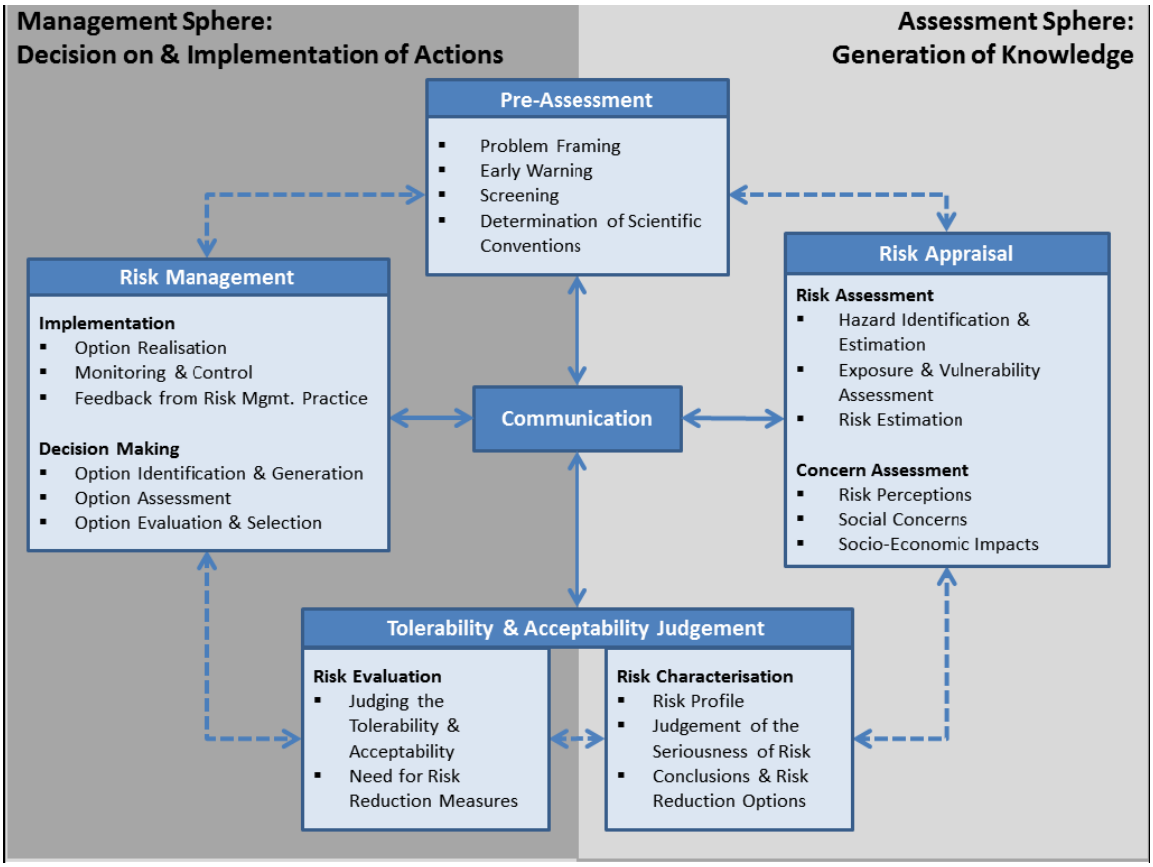

***Figure 8**: The International Risk Governance Council (IRGC) Framework*

Limitations of the IRGC framework

The IRGC framework attempts to balance the specificity required to act as a useful tool and the ambiguity required to apply to a variety of situations. The framework is viewed as a significant step forward in promoting a culture that takes a more holistic approach to handling risk and suggests that it is best used as a guideline toward better risk governance.

Many acknowledge that the framework is a step forward in addressing a gap in the approach to risk, given the increased levels of complexity and uncertainty in today's society [78][79]. It is considered a useful tool that helps those unfamiliar with recent academic research understand different approaches to risk management, and acts as a guide to identify the types of issues that risk managers should be taking into consideration, [78][79]. While the framework is regarded as useful for thinking about risk [80], some critics note the lack of a clear definition of risk [78][80]. Some argue that the framework is too complex or too simple to be useful as a practical tool [80], if the framework is applied rigidly [78][81]. Other minor criticisms include a bias towards systemic risks and that its emphasis on stakeholder engagement opens the door for lobbying [80].

The framework is reliant on taxonomies that force risks into categories; due to the systemic nature of risks it can be challenging to interpret them through a formal model [81]. By looking at larger

systems as a whole, the framework may lose sight of the importance of the micro end of decision-making [80]. Also, in attempting to decontextualize the risk system by looking at it from as many aspects as possible, it does not consider the context of how the risk has been managed and the process and definitions of risk that shaped the current situation [80].

Phases of Risk Governance

The pre-assessment phase

The pre-assessment phase inhabits a hybrid space in the assessment and management spheres. The purpose of the pre-assessment is to capture both the variety of issues that stakeholders and society might associate with a certain risk as well as existing indicators, routines, and conventions that may prematurely narrow down, or act as a filter for, what is going to be addressed as risk [82]. This phase has four components: problem framing, early warning, screening, and the determination of scientific conventions.

The purpose of *problem framing* is to attempt to see the risks from the point-of-view of all parties affected by the threats: the official agencies (government), the risk and opportunity producers (private enterprises), those affected by the risks and opportunities (producer employees, spinoff businesses, importers, and those who live nearby) and interested bystanders (media, and environmental groups). *Early warning and monitoring* refers to the ability of the market and government systems to identify the warning signs of impending failure in the system. It is described in the framework as a "systematic search for detecting hazards and threats, in particular new emerging risk events" [83]. It consists of any institutional effort to collect and interpret signs of risk and the systems of communication in place between those looking for signs and those acting upon them. *Screening* refers to "establishing a procedure for screening hazards/threats and risks, and determining an assessment and management route" and is meant to gain efficiencies in risk management [83]. Similar risks treated by similar means and the same people/departments would yield better results through specialization; an effective screening process ensures the risk is quickly diverted to those best equipped to handle it. Finally, the *determination of scientific conventions* is about understanding the "assumptions and parameters of scientific modelling and evaluating methods and procedures for assessing risks and concerns" [82].

Risk appraisal

The purpose of the risk appraisal phase is to determine whether the endeavour that creates the risk is worth pursuing, and if so, what steps can be taken to mitigate or contain said risk [82]. The risk appraisal phase consists of two major components: a scientific assessment of the risk, or *risk assessment*, and an assessment around societal concerns about the risk, or *concern assessment*.

The *risk assessment* component of risk appraisal aims to identify potential hazards, assess the level of exposure and vulnerability, and estimate the end risk using best scientific models available. It consists of scientific modelling of risks and the traditional determination of probabilities. It generally uses existing data along with scenario modelling to determine various scenarios for risk and then estimating the probability of their occurrence. *Concern assessment* is comprised of gaining an understanding of some of the underlying issues of the risk, such as how the risk affects different socio-economic groups and how the risk is perceived by society, including an analysis of any cognitive biases that may exist around the risk. By combining these

two major components, risk managers are able to gain insight into the values and evidence required to assess the public's tolerance for risk exposure.

Tolerability & acceptability judgement

The third phase of the IRGC framework, the *tolerance & acceptability judgement* phase, is essentially about determining the "appetite" for risk given the likelihood and the consequence of its occurrence. Tolerance with regard to risk looks at whether the endeavour that creates the risk is worth pursuing given the potential consequences of disaster. Acceptability refers to the level of residual risk allowable after measures are put in place to mitigate or minimize exposure [82]. Something that is intolerable should be avoided, something that is tolerable requires risk reduction measures until it becomes acceptable, and something that is acceptable should require no action. This phase is often viewed as the most difficult; the lines between intolerable, tolerable and acceptable are rarely clear, because making a decision about tolerability and acceptability involves the weighing of values and evidence. It is for this reason the phase is divided into two categories: *risk characterization* and *risk evaluation*.

Risk characterization is the collection and summarization of "all relevant evidence necessary for making an informed choice on tolerability or acceptability of the risk in question and suggesting potential options for dealing with the risk from a scientific perspective" [82]. This component is generally completed by experts in the field. The *risk evaluation* component filters the risks through societal values and norms to make a judgement on the tolerability and acceptability of the risks and, subsequently, judging the need for further risk reduction.

It is when a risk is deemed to be tolerable and in need of methods to reduce exposure to the consequences of the risk, that risk governance enters the risk management phase.

Risk management

The *risk management* phase of the IRGC framework takes the information gleaned from the other phases of the framework and uses it to make decisions about the actions required to manage the risk. The ultimate goal should be to make the tolerable risk acceptable over time. The categories within this phase endeavour to create learning organizations, both amongst the risk producers and in the government organizations in charge of regulation. They do this by instituting a risk management regime with feedback loops where risk managers identify, assess, evaluate, select and implement options for moving toward risk 'acceptability.' Finally, the chosen options should be monitored and measure for "intended and unintended consequences" [82]. The information taken from monitoring should then be fed back into the beginning process of identifying policy options, and the cycle should repeat.

Risk classification

The IRGC framework divides risks into four classes: simple, complex, uncertain, and ambiguous. Different risk classifications will guide management strategies and the level of stakeholder involvement optimal for risk governance. The classification of risk is "not related to the intrinsic characteristics of hazards or risks themselves but to *the state and quality of knowledge available* about both hazards and risks" [6].

Table 6: *Risk classification*

Simple	Risks for which "the number of predicted events are frequent and the causal chain obvious" [6]. The management of simple risks is relatively straightforward and can often be left to the market albeit with some regulations. **Example: car accidents**
Complex	Risks where there is difficulty "identifying and quantifying causal links between a multitude of potential causal agents and specific observed effects" [6]. This difficulty may arise from, but is not limited to: • Interactive effects amongst potential causal agents • Long delay periods between cause and effect • Inter-individual variation (i.e., greater differences from case to case) • Intervening variables **Example: failure risk in large interconnected infrastructure**
Uncertain	Risks where there is "a lack of clear scientific or technical basis for decision making," which "often results from an incomplete or inadequate reduction of complexity in modelling cause-effect chains." This diminishes the confidence level of traditional objective measures of risk estimation and becomes more reliant on "fuzzy" or subjective measures of risk estimation [6]. Categories of uncertainty: *Epistemic (a result imperfect knowledge)* – characteristics include: • Target variability • Systematic and random error in modelling *Aleatory (a result of randomness)* – characteristics include: • Indeterminacy or genuine stochastic events • System boundaries • Ignorance or non-knowledge **Example: acts of violence such as terrorism and sabotage**
Ambiguous	Risks are a "result of divergent or contested perspectives on the justification, severity or wider 'meanings' associated with a given threat [6]. Categories of ambiguity: *Interpretative* – (i.e., different interpretations of the same results) *Normative* – (i.e., different concepts of what can be considered tolerable) **Examples: low-dose radiation (interpretative) and nuclear power (normative)**

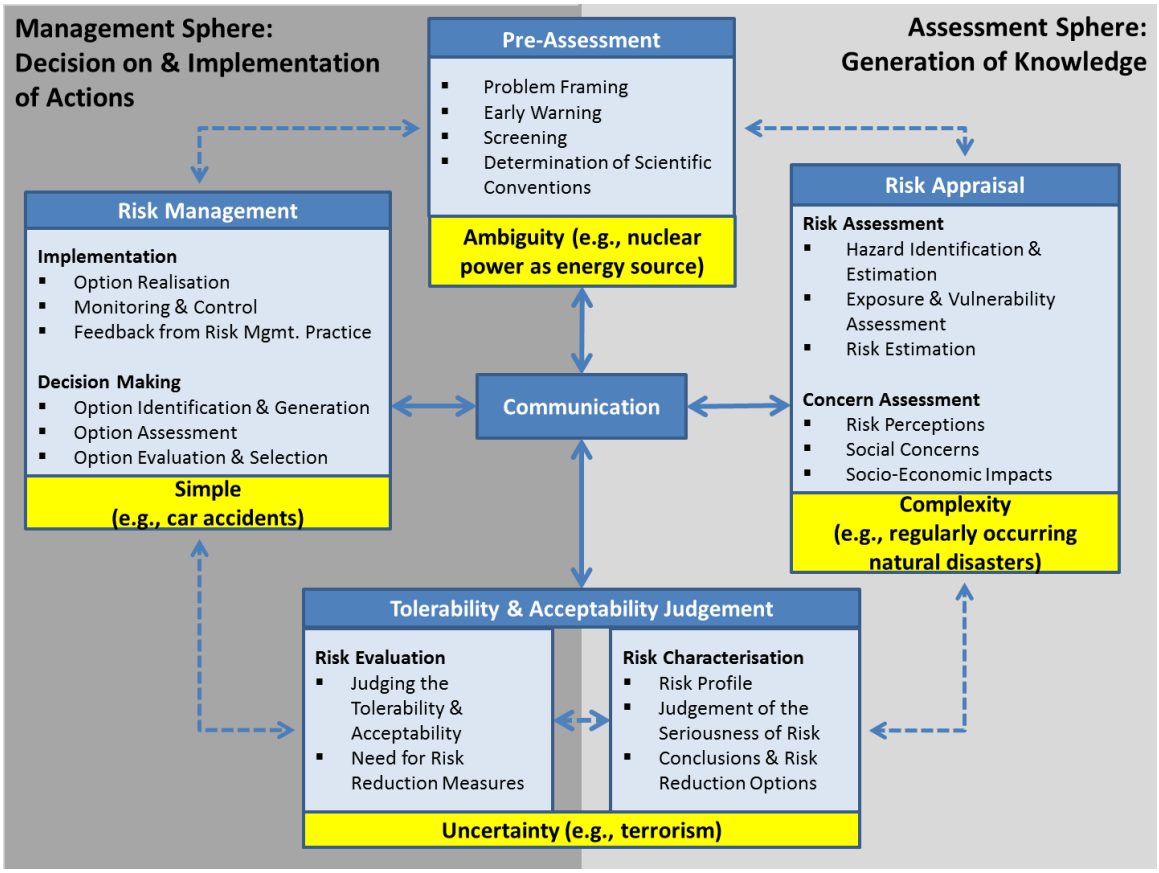

***Figure 9**: IRGC Framework - Risk classification and framework alignment*

Renn suggests that the risk classification will determine which phase of the IRGC framework should be the primary focus of governance of that risk (see Figure 9), which management strategy should be employed, and which stakeholders to involve (see Figure 10).

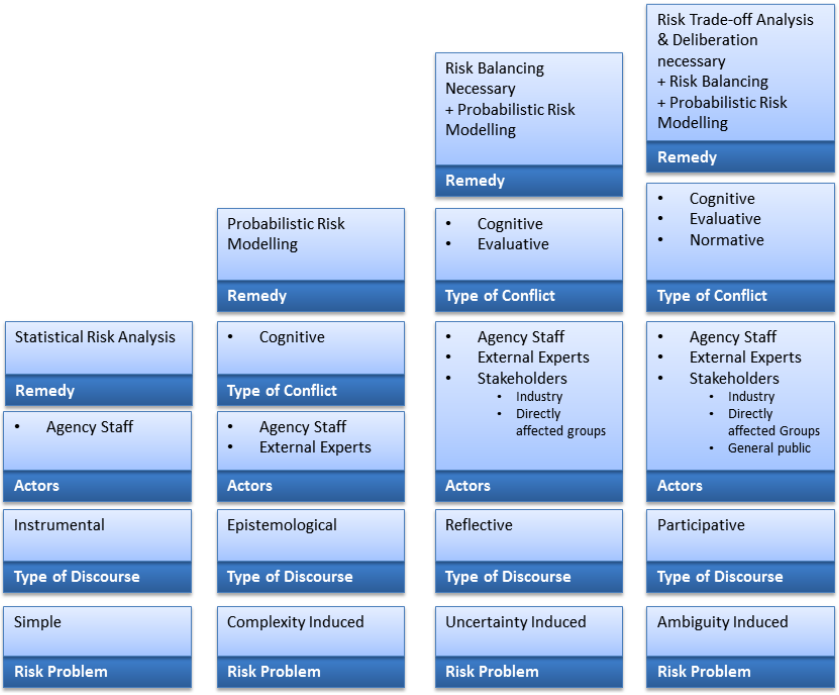

Figure 10: Risk management escalator and stakeholder involvement

Annex C Transportation Interview Participants

We conducted 50 semi-structured interviews between 2011 and 2013 with regulators, owners, operators, managers and representatives of critical transportation infrastructure. We interviewed representatives of airports, rail, seaports, trucking and bridges. Most interview subjects work for Canadian organizations, although we also interviewed specialists from Australia, the UK and the US to provide some comparative perspective. The table below summarizes information about the interviews and interview subjects.

Table 7: *Coded list of transportation interview participants*

Code	Role	Sector	Date
Int 1	Industry Association	Aviation	Dec-2011
Int 2	Owner/Operator/Manager	Bridge	Sep-2011
Int 3	Government Regulator/Official	Other	
Int 4	Government Regulator/Official	Ports	Dec-2011
Int 5	Owner/Operator/Manager	Rail	Jul-2011
Int 6	Owner/Operator/Manager	Rail	Nov-2011
Int 7	Owner/Operator/Manager	Surface Transport	Jul-2011
Int 8	Industry Association	Surface Transport	Jun-2011
Int 9	Owner/Operator/Manager	Surface Transport	Jul-2011
Int 10	Industry Association	Aviation	Feb-2012
Int 11	Government Regulator/Official	Aviation	Sep-2011
Int 12	Owner/Operator/Manager	Aviation	Oct-2011
Int 13	Owner/Operator/Manager	Aviation	Oct-2011
Int 14	Owner/Operator/Manager	Aviation	Feb-2012
Int 15	Industry Association	Aviation	Aug-2013
Int 16	Owner/Operator/Manager	Bridge	Jun-2011
Int 17	Owner/Operator/Manager	Bridge	Nov-2011
Int 18	Owner/Operator/Manager	Bridge	Sep-2011
Int 19	Owner/Operator/Manager	Bridge	Aug-2011
Int 20	Government Regulator/Official	Other	Jan-2012
Int 21	Government Regulator/Official	Other	Aug-2011
Int 22	Government Regulator/Official	Other	Dec-2011
Int 23	Government Regulator/Official	Other	
Int 24	Government Regulator/Official	Other	Oct-2011
Int 25	Government Regulator/Official	Other	Aug-2011
Int 26	Government Regulator/Official	Other	Oct-2011
Int 27	Government Regulator/Official	Other	Mar-2012
Int 28	Government Regulator/Official	Other	Nov-2011
Int 29	Transportation Specialist	Other	Jul-2013
Int 30	Owner/Operator/Manager	Ports	Jun-2011
Int 31	Owner/Operator/Manager	Ports	Aug-2011
Int 32	Owner/Operator/Manager	Ports	Jul-2011
Int 33	Owner/Operator/Manager	Ports	Dec-2011

Int 34	Owner/Operator/Manager	Ports	Sep-2011
Int 35	Industry Association	Ports	Jul-2011
Int 36	Industry Association	Ports	Sep-2011
Int 37	Government Regulator/Official	Ports	Jul-2011
Int 38	Government Regulator/Official	Ports	Jul-2011
Int 39	Government Regulator/Official	Other	Sep-2011
Int 40	Government Regulator/Official	Ports	Aug-2011
Int 41	Owner/Operator/Manager	Ports	Jul-2013
Int 42	Owner/Operator/Manager	Ports	Jul-2013
Int 43	Government Regulator/Official	Other	Aug-2013
Int 44	Government Regulator/Official	Other	Sep-2013
Int 45	Owner/Operator/Manager	Rail	Sep-2013
Int 46	Government Regulator/Official	Other	Aug-2013
Int 47	Government Regulator/Official	Other	Aug-2013
Int 48	Transportation Specialist	Ports	Jul-2013
Int 49	Government Regulator/Official	Surface Transport	Jul-2013
Int 50	Government Regulator/Official	Other	Aug-2013

*Other includes emergency managers, and senior and management level government officials in transportation (not subsector specific).

Table: *List of transportation interview participants by subsector and type*

Subsector	**Regulator**	**Owner/Operator/Manager**	**Industry Association**	**Expert/Academic**	**Total Number of Interviews**
Aviation	1	3	3	0	7
Port	4	7	2	2	14
Bridge	0	5	0	0	5
Rail	0	3	0	0	3
Trucking	1	2	1	0	4
Other	16	0	0	1	17
Total					50

*Other includes emergency managers, and senior and management level government officials in transportation (not subsector specific).

Annex D Food Interview Participants

The research draws on an analysis of 10 interviews with critical infrastructure (CI) regulators, owners, operators and managers from the agricultural sector. We interviewed retailers, industry associations, not-for-profits and regulators. Most interview subjects work for Canadian organizations, although we also interviewed specialists from countries such as Australia, the UK and the US to provide some comparative perspective. The table below summarizes information about the interviews and interview subjects.

Table 8: *Coded list of food interview participants*

Code	Role	Sector	Date
Int 51	Manager/Operator	Retailer	June 2011
Int 52	Manager/Operator	Retailer	July 2011
Int 53	Official	Industry Association – Grocery	July 2011
Int 54	Official	Industry Association – Grocery	February 2012
Int 55	Official	Industry Association – Commodities	November 2012
Int 56	Official	Industry Association – Commodities	July 2011
Int 57	Official	Industry Association – Commodities	August 2011
Int 58	Government Regulator/Official	Regulatory Agency	January 2012
Int 59	Official	Non-Profit	July 2011
Int 60	Official	Non-Profit	July 2011

Table: *List of food interview participants by subsector and type*

Subsector	**Regulator/Official**	**Owner/Operator/Manager/Industry Representative/ Citizens' Group**	**Total Number of Interviews**
Retailer	0	2	2
Industry Association - Grocery	0	2	2
Industry Association - Commodities	0	3	3
Regulatory Agency	1	0	1
Non-Profit	0	2	2
Total	1	9	**10**

Annex E Interview Questions

Note: Questions for industry and government representatives were largely the same. There will have been some slight modifications based on the interviewees response. Questions to regulators focused on their regulatory role. They were therefore likely to receive fewer questions than industry representatives, for instance. This document represents the complete list of questions.

Note also that interview subjects received the questions in advance and were asked to reflect on them before their interviews.

How do you gather information about the security of your critical infrastructure?

In your opinion, what are the significant risks currently faced by your organization?

Are you party to multi-organizational forums (either industry-sponsored or government-sponsored)?

Do you find these forums useful? In which ways?

Are there particular rules about information exchange in these forums? If so, what are they?

Are you confident in the information you receive and give in these forums?

In the context of your organization, what kinds of information about vulnerabilities are appropriate for sharing with individuals outside of the organization? How and with whom would your organization share this information?

How—if at all—could security-related information-sharing in your organization be improved?

What standards do you adhere to in protecting your critical infrastructure? Who generates these standards?

Are you satisfied with the standards? What—if anything—could be improved in terms of establishing safety and security standards?

How much would you estimate you spend on safety and security at your organization annually?

Who is responsible for security at your organization?

Describe briefly the typical interactions you have within the organization with respect to security?

We are often told that we live in a highly interdependent world and that a failure in one sector can cascade into another. On which of these sectors do you rely the most to ensure successful operation of your business? Select up to three. Generally speaking, how would you interact with these sectors on issues of business continuity?

- Banking

- Emergency Services (e.g. policing, firefighters)
- Energy and Utilities
- Food Supply
- Government Operations
- Health Care
- Manufacturing
- Telecommunications, including IT and internet
- Transportation
- Water Supply

Pressures or Influences

On a scale of 1 to 10 in which '10' means 'very influential' or 'very demanding' and 1 means 'not at all' or 'I spend little time thinking about it', rate the following:

1. Citizen or Consumer Concern
2. Contractors who help you maintain your critical infrastructure
3. Insurance Concerns
4. Laws or Legal Concerns
5. Media Coverage
6. Other Organizations within your sector
7. Technical issues
8. (Key) Suppliers in your supply chain
9. Other (specify):

Imagine you had one extra day per month and you had to spend it on the security and/or safety of your critical infrastructure. How would you spend it?

What do you think the chances are of a significant operational failure in your sector in the next three years? Let's assume by significant operational failure, we mean that a key organization within your sector (that provides a similar service as you do) is unable to carry out its core function for at least three days.

Uncertain risks

When we refer to "uncertain risks" we mean events that occur rarely and for which we do not have a lot of reliable data that can help us to predict them. Examples of uncertain risks include *rare* natural disasters (not seasonal; more like once in a decade or even less frequent), a pandemic or terrorist attack. We would like to ask a few questions about uncertain risks. We will use these three as examples for our discussion.

In the following questions we will ask you to score your answers from one to ten but if you would like to provide additional reflections or comments please feel free to do so.

On a scale of one to ten in which ten means very confident and one means no confidence at all, how confident are you that you would receive reliable and timely information that would help you prepare:

- For a pandemic
- For a rare natural disaster

- For a terrorist attack

If we asked your peers in your sector, do you think they would answer the same way?
That you would know who to contact for reliable information:

- For a pandemic
- For a rare natural disaster
- For a terrorist attack

If we asked your peers in your sector, do you think they would answer the same way?
That you have a reliable business continuity plan that would allow you to maintain your service:

- During a pandemic
- During a rare natural disaster
- During a terrorist attack

If we asked your peers in your sector, do you think they would answer the same way?

In which areas do you think your sector has made the most progress in the last decade with respect to preparing for or anticipating uncertain risks?

In which areas do you think your sector needs to make more progress with respect to preparing for or anticipating uncertain risks?

If we were to reconvene in three years' time, where would you like to be on this issue?

Do you have any final comments?