Risk Assessment Framework

Seamless Border Pilot Project

Ian Bayne
CAE Inc.

Shaye K. Friesen
DRDC - Centre for Security Science

Defence Research and Development Canada

Reference Document
DRDC-RDDC-2017-D081
January 2017

IMPORTANT INFORMATIVE STATEMENTS

This work was supported by the Canadian Safety and Security Program (CSSP) (CSSP-2015-TI-2130) which is led by Defence Research and Development Canada‟s Centre for Security Science. The CSSP 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.

Template in use: (2010) SR Advanced Template_EN (051115).dotm

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2017

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2017

Abstract

This Reference Document captures reference material derived from ongoing work on risk assessment frameworks. It summarizes a concept for developing an effective framework using the Seamless Border Focus Area as a ‘test case’ for scanning risk assessment approaches that could contribute to risk-informed decision making in support of the Border and Transportation Security Portfolio investment planning and analysis cycle.

Résumé

Le présent document de référence contient de la documentation tirée des travaux en cours sur les cadres d'évaluation des risques. Il s'agit du résumé d'un concept permettant d'élaborer un cadre efficace en se servant de la question centrale que constitue la perméabilité des frontières comme 'cas type' afin d'étudier les approches en matière d'évaluation des risques pouvant contribuer à la prise de décision fondée sur le risque à l'appui du cycle de planification et d'analyse des investissements dans le portefeuille de la sécurité des frontières et des transports.

Table of contents

Abstract i
Résumé ii
Table of contents iii
List of figures iv
1 Introduction 1
2 Background 2
3 Discussion 4
4 Conclusion 6
References 8
Annex A Risk Management Framework 11
Annex B Risk Assessment Decision Tree 12
Annex C Risk Assessment Influence Diagram 13
Annex D Risk Assessment Information Flows 14
Annex E Additional Seamless Border References 15

List of figures

Figure A.1: Risk Management Framework. 11
Figure B.2: Risk Management Framework. 12
Figure C.3: Risk Assessment Influence Diagram. 13
Figure D.4: Risk Assessment Information Flows. 14

1 Introduction

Within the Canadian Safety and Security Program (CSSP), Focus Area Narratives (FANs) consider risk from multiple perspectives to ensure that costs and impacts of investments in science and technology (S&T) are aligned with national priorities and strategic outcomes. The changing nature of Canada's safety and security landscape underscores the need to have an understanding of risk at an enterprise-level. Decisions will be framed by the strategic context as well as competing S&T investment projects that are prioritized by Portfolios and Communities of Practice (CoPs) in a dynamic and resource-constrained environment. Various factors are driving the need to migrate from a fragmented and bottom-up view of risk to a more integrated and unified strategic view of risks and issues that would inform S&T program prioritization decisions and strategic planning.

Based on this review and previous work that reviewed the capability and maturity of CSSP and international national risk assessment practices, a concept for a pilot project to develop specific tools for Seamless Border is proposed, which could be adapted for other focus areas and/or for a broader participative risk assessment process, possibly including Canadian and United States (US) stakeholders.

2 Background

To better understand the potential of using a risk-informed approach for implementing a systematic process that may be used as a basis for generating S&T priorities and requirements for project funding, it is useful to describe the objective of risk assessment within the context of the CSSP decision analytic framework. The 2012 Treasury Board (TB) Submission establishes an integrated risk and capability assessment decision support model as the basis for developing investment and program priorities within the harmonized CSSP. The TB Submission introduced the notion that funding for program areas will be "…enabled by a capability and risk based investment model…",[1] further noting the need for "prioritizing and matching S&T investment responses according to the assessment of risk."[2]

Prior to this declaration and amalgamation of activities into a single harmonized CSSP, risk assessments were largely security threat/risk assessments that were based on *ad hoc* processes used by partner departments. These assessments were, and to some extent still are, constrained by specific mandates, policies and legislation. With few exceptions where CSS was in a lead role to facilitate multi-party threat assessments, responsibilities for risk assessments are decentralized to individual partners or program elements that were designed to respond to the security threats with terrorism being the dominant threat. The inclusion of public safety, critical infrastructure protection (CIP), cyber, border security and emergency management (EM) domains added new dimensions to the consideration of risk.[3]

While the prioritization of security S&T investments was based on intelligence analysis and recent events, and to a lesser extend trends, other aspects of the CSSP applied a range of risk assessment techniques based on past events, historical data, facts and evidence. The development of threat/hazard-specific scenarios and the application of the EM all hazards risk assessment concepts to support planning (i.e., design one solution that treats multiple risks that have similar characteristics and are location neutral), combined with a level of capability gap analysis, guided the CSSP investment selection process. Ultimately, this fragmented view of risk (and capability analysis) is difficult to aggregate and combine with other types of risks facing the program including more forward-focused, qualitative approaches and strategic risks.

In 2014, a scan of risk assessment capability and maturity within the CSSP identified the need for greater visibility of partners' operational risk environments and risk assessment techniques to help CSS to compare partners' S&T requirements (e.g., urgency; alignment with CSSP strategic objectives; return on investment). A more unified view of risk would also help CSS to communicate how risk information informs decision making internally and externally. The scan noted there are opportunities to handle risk information more consistently, particularly by elevating risk discussions to a strategic level, which would contribute to improving CSSP

[1] Canada, Department of National Defence, Renewal and Harmonization of the Public Safety and Security Science and Technology Programs, Treasury Board Submission, February 21, 2012, .p,12 (PB).
[2] Ibid., p. 17.
[3] Annex A provides an illustrative risk management framework adapted from a U.S. National Research Council (NRC). It illustrates the full spectrum of activities that make risk management more consistent and useful to decision making, strategic planning and other management processes.

strategic outcomes, and demonstrating the value of risk information and the integrity of the evidence base.[4]

A key challenge is that stakeholders tend to assess risk and/or its individual components differently depending on the environment. This fragmented approach can obscure understanding of the bigger picture and reinforce organizational bias. Transport Canada's (TC) risk assessment matrix (RAM) , Canada Border Service Agency's (CBSA) 2013–2015 National Border Risk Assessment, the Royal Canadian Mounted Police's (RCMP) Harmonized Threat Risk Assessment (HTRA), and Public Safety Canada's (PS) All Hazard Risk Assessment (AHRA) framework are examples of risk assessments being performed in support of federal mandates.

[4] See Bayne, I., Friesen, S.K., Risk scan: a review of risk assessment capability and maturity of risk within the Canadian Safety and Security Program (U), Defence R&D Canada (DRDC) Scientific Report (SR) DRDC-2014-R36, June 2014.

3 Discussion

This proposed pilot project builds on the work of previous projects including the AHRA Framework Body of Knowledge and Risk Scan (2014). In 2015, DRDC CSS initiated a targeted investment (TI) project, Establishing a risk and capability-based framework for assessing CSSP Investments (CSSP-2015-TI-2130), to investigate options to achieve a rigorous, traceable and defensible risk-informed selection of program investments.

The results of this initial project effort (i.e., Spiral 1) were compiled in two reports: 1) Preliminary Framework for CSSP Risk Assessment, which described the conceptual framework and building blocks for an RA framework (CSS, 2015); and 2) a Comprehensive scan for the CSSP risk assessment framework, which identified lessons from a number of national risk assessments that compared risk assessments across security and safety environments. In particular, the reports identified lessons that could be applied to Seamless Border FAN, in particular the use of scenarios to describe and prioritize complex risks, and options to simplify the process to make it more dynamic, participative, sustainable and inclusive to a broader range of stakeholders including potential cooperation with US partners (e.g., Department of Homeland Security (DHS) S&T Directorate).

In order for a theoretical framework to have value, it also makes sense to test the emerging concepts on a specific problem.[5] It was determined that the Focus Area – Seamless Border would be a suitable candidate. It is assumed that the approach should be adaptable for other Focus Areas and enablers, and actually present a concept for managing risk inputs to the overall strategic planning and program management space. Key elements of the risk assessment framework for Seamless Border include:

- Asking partners to describe how they determine their S&T priorities, to describe their most significant risk scenarios, and to share recent threat, hazard, vulnerability, impact and/or risk assessments that influenced the prioritization process;
- Developing a standardized approach to describing complex risk scenarios that captures interdependencies and uncertainty. Initial data capture can be done electronically and with limited consultation;
- Unifying impact assessment framework that considers stakeholders' risk perception and tolerance, accepts qualitative and quantitative descriptions, and is understandable by specialists and generalists;
- An iterative, simplified approach to define, validate, refine and prioritize risk scenarios of greatest interest, which is not overly time-consuming and is repeatable for different

[5] A representative decision tree can be found in Annex B. This decision tree is intended to illustrate the importance of planning and scoping for general and specific risk assessments. It is relevant for assessments that engage multiple stakeholders in the risk prioritization process, and that consider the end game – a cost-effective, and collaborative treatment plan that is intended to reduce risk to a level that is as low as reasonably achievable.

environments (e.g., land, maritime and air critical control points), possibly with different participants; and

- Taking a long-term perspective, which is to establish a baseline with a limited number of stakeholders to test the concepts and value. Then, identify options to engage a broader community, to roll out the approach in other Focus Areas, and/or to transition the approach to lead security partners. [6]

The Seamless Border FAN (2016) identifies four key priority areas: efficient cross-border flow; border-free response; border strategies and information exchange;[7] and border perimeter integrity (CSS, 2016). Implicit in this description is the complexity of the area of interest given the interdependencies, number and diversity of stakeholders, and potential for competing objectives and S&T investments.

A pilot risk assessment study would include a thematic assessment, backed up by quantitative and qualitative analysis of risk trends and risk information that is available from open sources. Three tools that would be tested include: tailored risk taxonomy; set of complex risk scenarios; and a common stakeholder and impact assessment framework. These tools would be exploited to develop a reasonable set of complex risk scenarios that cover land, air and maritime environments, and provide a regional lens including for the arctic. Scenarios would be developed iteratively from existing information (held by CSS, open source material, and/or obtained by using a short questionnaire and possibly interviews), and if practicable, validated with a subset of federal stakeholders electronically or in a workshop (e.g., CBSA, TC, Immigration, Refugees and Citizenship Canada (IRCC), RCMP, PS, Canadian Security Intelligence Service (CSIS)). The risk taxonomy would be designed to support the Focus Area consultations and to act as a checklist for scenario development.

Scenario development would apply an 'all hazards' concept. For example, identification of threats/hazards and risks for one port of entry or critical asset could be extrapolated for similar ports of entry and risk environments. The scenarios would focus on specific targets and areas, and include sufficient information to characterize the context, source, stakeholder and impact categories, time and space, dependencies on critical infrastructure, and other vital decision information. Constraining the number of scenarios and avoiding duplication among regions would simplify the scenario development process. It would also provide broader coverage of worst-case scenarios. The stakeholder and impact categories and descriptions would facilitate differentiation of risk scenarios for critical assets (e.g., international airports, major land border crossings, and major waterways) from multiple perspectives. For future iterations, the scenarios could be tailored and more detail added by regional stakeholders.

[6] Annex C illustrates another view of the planning and scoping aspect of performing risk assessments within a broader decision making activity. That is, the assessments are not stand-alone activities, and their intended use influences the methodology.

[7] Annex D illustrates the diversity of risk information management space. CSS safety and security partners apply a variety of assessment techniques to identify their priorities. If these assessments are shared among partners or with CSS, it is done in an ad hoc manner.

4 Conclusion

It is reasonable to expect that over time, a common approach to describing, differentiating and prioritizing complex risks would help to achieve the objective of elevating the conversation above a comparison of discrete threats, hazards and vulnerabilities, and avoiding a focus on known capability deficiencies and issues. The resulting risk assessment framework should foster a forward-focused dialogue that would complement partners' existing assessments that are typically fact-based, community-specific, and constrained by mandates and other factors. This convergence would support collaboration across jurisdictional, knowledge, cultural and other boundaries.

Next steps include: formulating a set of complex risk scenarios to provide a reasonable level of detail and adequate coverage of Seamless Border main areas of interest, and developing and validating a stakeholder and common impact assessment framework.[8] The output would be a report and toolkit to augment Focus Area, Portfolio and CoP procedures. The report is expected to highlight issues or concerns, and evaluate whether the framework can be exploited across the program and possibly by partners.

[8] Annex E provides partial list of references intended to support future work, including a scan of risk scenario approaches that could inform the Seamless Borders Focus Area and collaboration with partners.

This page intentionally left blank.

References

- All Hazards Risk Assessment Framework Body of Knowledge. Volume I: Establishing an information baseline. DRDC:CSS TR 2013-014. Volume 2: Supporting material. DRDC:CSS TR 2013-015. September 2013.

- Beyond the Border Implementation Report to Leaders. Department of Homeland Security (DHS). US. 2014.

- Comprehensive scan for the Canadian Safety and Security Program (CSSP) risk assessment framework: establishing a method and process for assessing the distribution of investments, CAE Document No. 5843-011. CSS. 2016.

- Gamper, C., (2014), Interconnected, interdependent, risks. Background Paper prepared for the 2015 Global Assessment Report (GAR) on Disaster Risk Reduction. The United Nations Office for Disaster Risk Reduction (UNISDR). 2014.

- Evergreen Foresight Program. US Coast Guard. http://www.uscg.mil/STRATEGY/evergreen.asp. 2016.

- Kilford, C. Portfolio Management Guide. Final Public Consultation Draft. United Kingdom (UK) Office of Government Commerce (OCG). Accessed July 2016.

- National Border Risk Assessment (2013-2015). Risk Management & Foresight Division. CBSA. May 2013 (S).

- National Risk Assessment (NRA): profiles of selected OECD countries, High Level Risk Forum (HLRF). Public Governance and Territorial Development Directorate. Public Governance Committee. GOV/PGC/HLRF(2015)8/ANN1. Organization for Economic Cooperation and Development (OECD). 2015.

- National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience. Department of Homeland Security (DHS). US. 2013.

- Northern Border Strategy. DHS. June 2012.

- Perimeter Security and Economic Competitiveness. Global Affairs Canada. 2011.

- Portfolio Management Guide. Final Public Consultation Draft. Office of Government Commerce (OGC). Cabinet Office. UK. 2008.

- Preliminary Framework for CSSP Risk Assessment: Establishing a Methodology and Process for Assessment the CSSP Distribution of Investments. CAE Document No. 5843-011. CSS. October 2015.

- Risk assessment framework: Seamless Border. CAE Document No. 5843-012-02 (not published). CAE. March 2016.

- Risk scan: a review of risk assessment capability and maturity within the Canadian Safety and Security Program (Part 1 – Review of Risk Capability and Maturity; Part 2 – Supporting Material). Tech. No. DRDC-RDDC-2014-R36. CSS. June 2014.

- Seamless Border Focus Area Narrative. CSS. 2016.

- Science and Decisions: Advancing Risk Assessment, Committee on Improving Risk Analysis Approaches; used by Environmental Protection Agency, National Research Council (NRC). National Academy of Sciences (NAS). National Academies Press (NAP). US. 2008.

- Strategic Planning Guidance (SPG) for 2016-2017. CSSP. CSS. 2015.

- Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach. NIPP 2013. DHS. 2013.

- The Strategic National Risk Assessment (SNRA) in Support of PPD 8: A Comprehensive Risk-Based Approach toward a Secure and Resilient Nation. DHS. US. December 2011.

- Transportation Systems Sector-Specific Plan. DHS and Department of Transportation. 2015.

- United States-Canada Agreement for Cooperation in Science and Technology for Critical Infrastructure Protection and Border Security. June 2004.

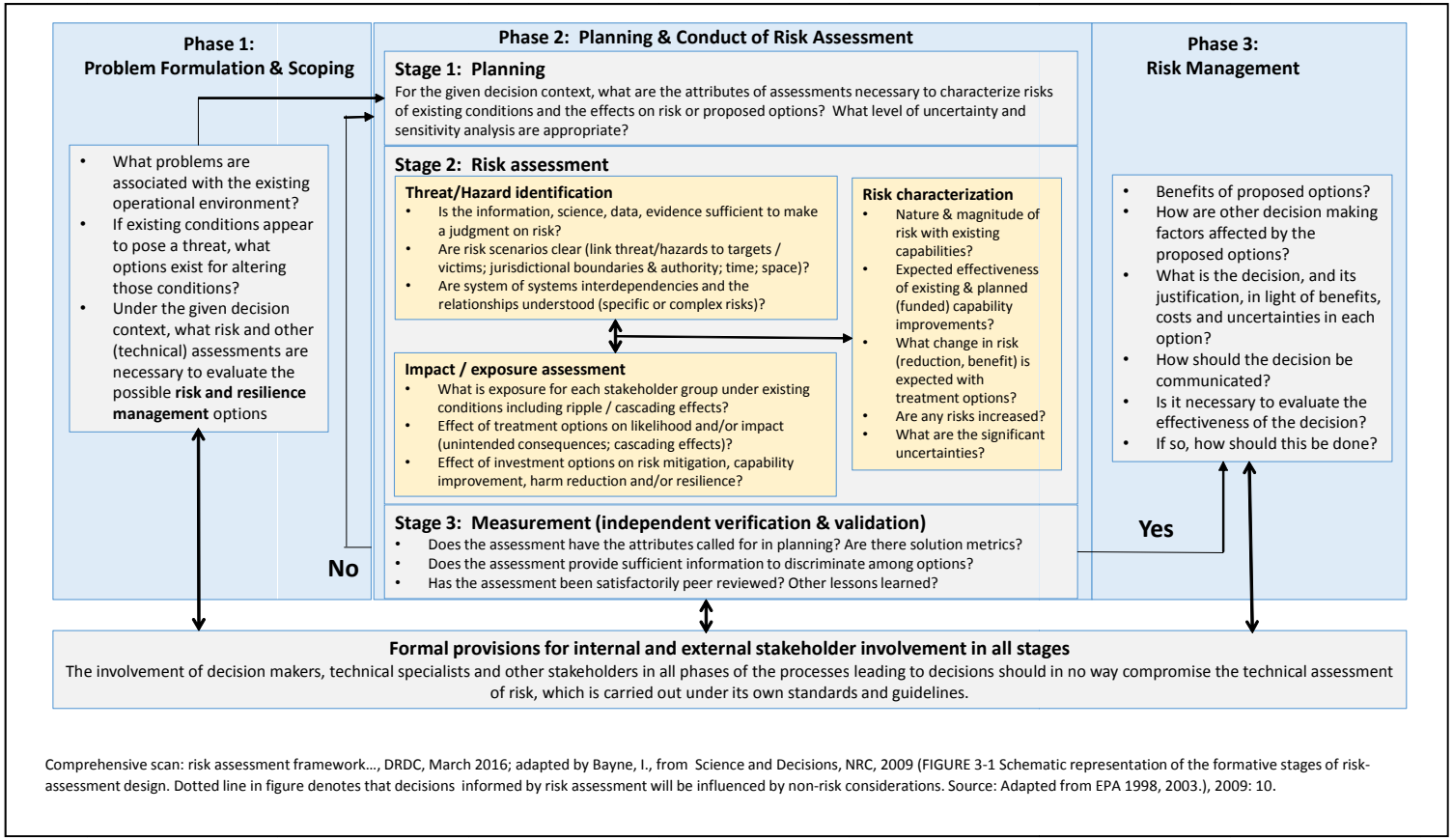
- US-CA Joint Border Threat and Risk Assessment. US Customs and Border Protection (CBP), CBSA and RCMP. July 2010. Published 2011.

- What Canadians told us: A Summary on Consultations on Perimeter Security and Economic Competitiveness. PS. https://www.publicsafety.gc.ca/cnt/brdr-strtgs/bynd-th-brdr/wht-cndns-en.aspx. Accessed 1 October 2016.

.

This page intentionally left blank.

Annex A Risk Management Framework



Comprehensive scan: risk assessment framework..., DRDC, March 2016; adapted by Bayne, I., from Science and Decisions, NRC, 2009 (FIGURE 3-1 Schematic representation of the formative stages of risk-assessment design. Dotted line in figure denotes that decisions informed by risk assessment will be influenced by non-risk considerations. Source: Adapted from EPA 1998, 2003.), 2009: 10.

Figure A.1: *Risk Management Framework.*

Annex B Risk Assessment Decision Tree

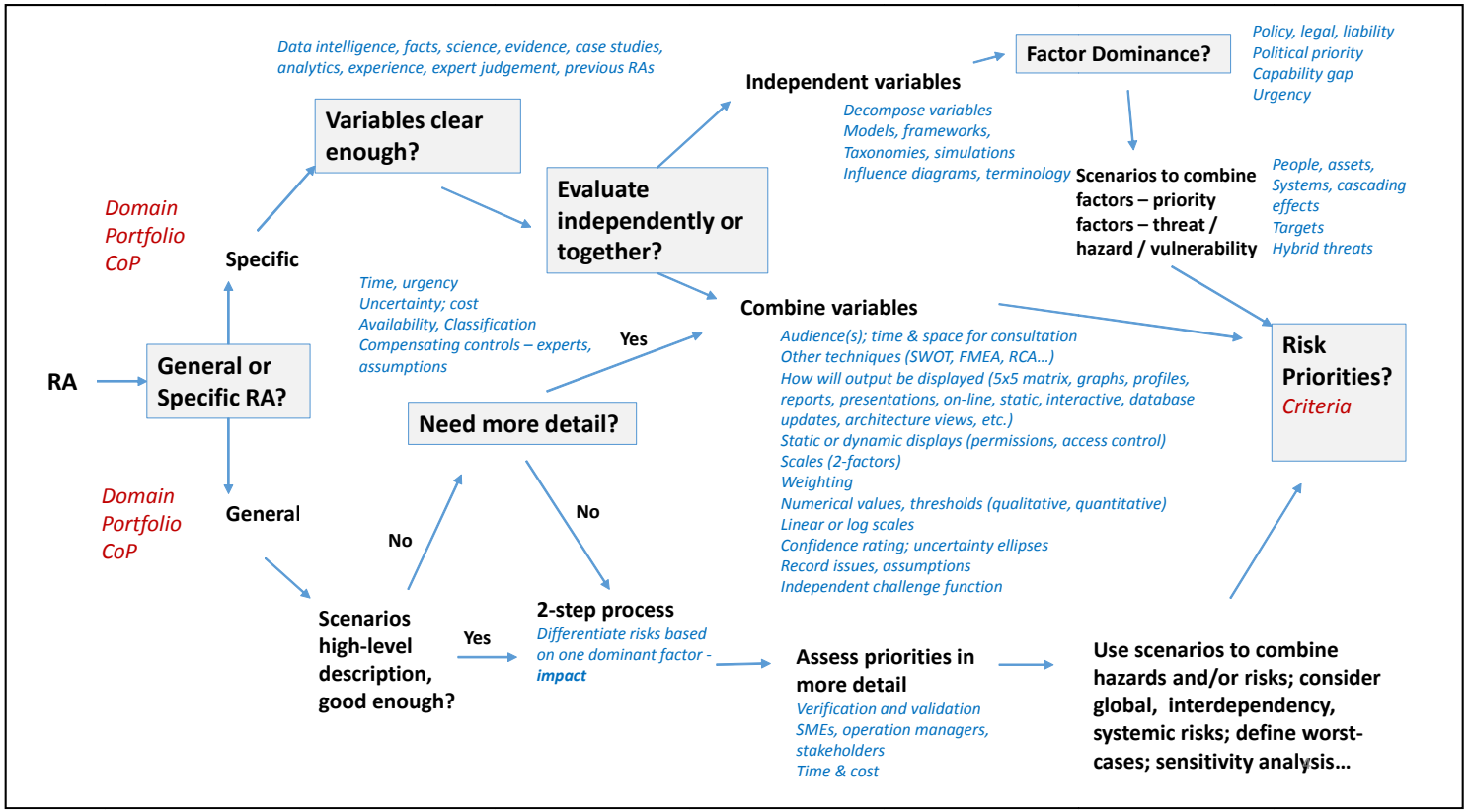


Figure B.2: *Risk Management Framework.*

Annex C Risk Assessment Influence Diagram

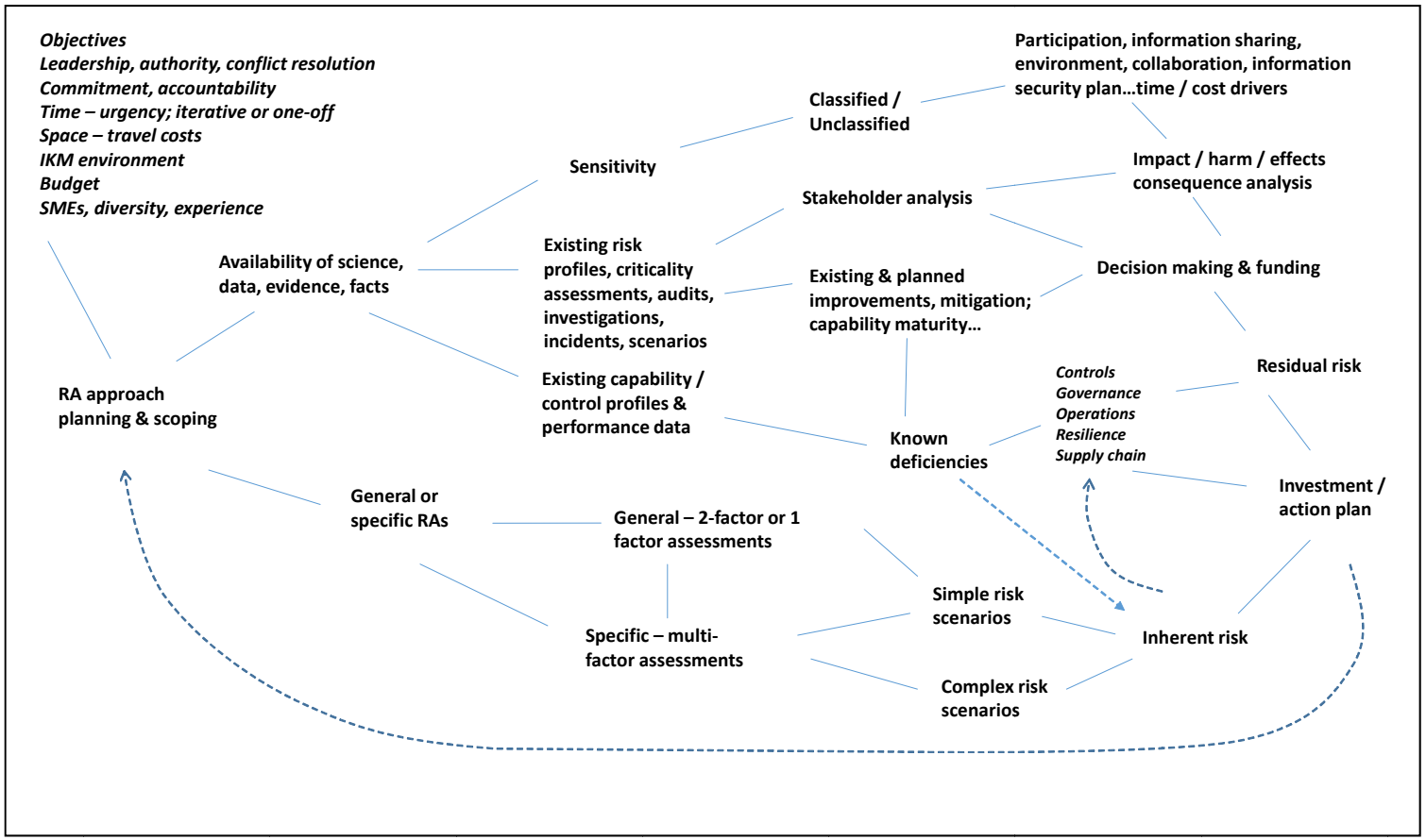


Figure C.3: *Risk Assessment Influence Diagram.*

Annex D Risk Assessment Information Flows

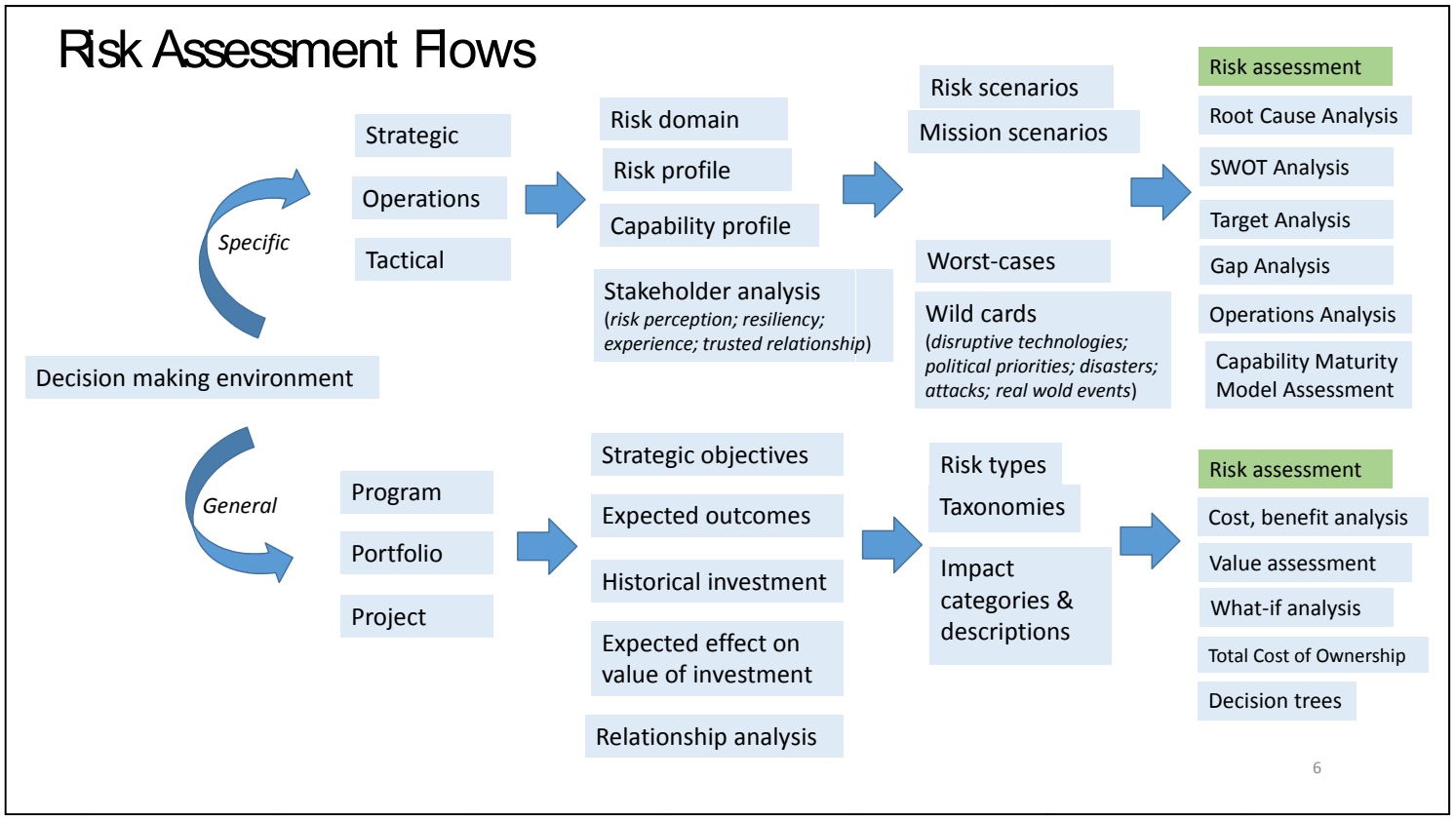


Figure D.4: *Risk Assessment Information Flows.*

Annex E Additional Seamless Border References

Assumptions used to streamline the list of references include: Seamless Borders will focus on Border Free Response and Border Perimeter Integrity (two of four objectives); other groups will address environmental and cybersecurity risks; national security and sovereignty are not in scope; health and safety are in scope; financial crime and cybercrime are in scope; transportation systems security is in scope (i.e., critical infrastructure sector); and transcontinental (and serious) organized crime is in scope, including the trend of convergence of smuggling weapons and money that support terrorism and violent extremism (link to perimeter integrity). NRCan, CNSC and DND are other potential sources, but the list is intentionally constrained.

CBSA

- Status of National Border Risk Assessment (NBRA) – last one 2013 (Secret, held by CSS).
- Integrated Border Enforcement Teams (IBET), threat assessments (with RCMP).
- Status of US-CA Joint Border Threat and Risk Assessment (last one in 2010).

Transport Canada

- Interdepartmental Maritime Sub-Working Group (IMSWG), threat or risk assessments.
- Strategic Risk Assessment Methodology.
- Multi-modal risk assessments.
- Any unclassified risk scenarios or assessments for specific border crossings or ports of entry.
- Status of Risk Assessment Matrix (RAM) Methodology Guide (Draft, copy held by CSS).

Public Safety

- RRAP and Virtual Risk Analysis Centre (VRAC).
    - Site criticality, resiliency, capability and/or risk assessment methodologies.
    - Examples of risk scenarios related to border security or specific points of entry.
    - Report from RRAP pilot projects.
- Status of Canadian National Risk Profile project – risk assessment methodology.
- Status of Canadian CI Sector Risk Profiles - Transportation.
- Status of Strategic National Risk Assessment (SNRA), DHS - last one 2011 on DHS web site).
- After-Action Review, PanAm Games (2015).

RCMP

- Domain Awareness WG (CBP and RCMP) reports on pilot projects (or specific risk products).
- Border security risk scenarios or assessments (unclassified).
- Risk assessment methodology or assessments in support of Serious and Organized Crime Strategy (RCMP, 2013, on web site).

Health Canada / PHAC and/or PS

- Health Security Working Group (CA-US Border Action Plan initiative), hazard, impact or risk assessments.
- Canadian equivalent to US National Health Security Strategy.

CFIA / AAFC

- Canadian studies or risk scenarios related to prioritizing agroterrorism countermeasures and capability improvements.

CCG

- Maritime Security Risk Analysis Model (MSRAM), USCG.
- Area Risk Assessment (ARA) Methodology.

Integrated Business & Human Resources Plan (IBHRP; previous version 2012 is on CCG web site).

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security markings for the title, abstract and indexing annotation must be entered when the document is Classified or Designated)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g., Centre sponsoring a contractor's report, or tasking agency, are entered in Section 8.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

UNCLASSIFIED

2b. CONTROLLED GOODS

(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC DECEMBER 2012

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Risk Assessment Framework : Seamless Border Pilot Project

4. AUTHORS (last name, followed by initials – ranks, titles, etc., not to be used)

Bayne, I; Friesen, S.K.

5. DATE OF PUBLICATION (Month and year of publication of document.)

January 2017

6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)

25

6b. NO. OF REFS (Total cited in document.)

25

7. DESCRIPTIVE NOTES (The category of the document, e.g., technical report, technical note or memorandum. If appropriate, enter the type of report, e.g., interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Reference Document

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

DRDC – Centre for Security Science
Defence Research and Development Canada
222 Nepean St., 11th Floor
Ottawa, Ontario K1A 0K2
Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)

9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)

DRDC-RDDC-2017-R081

10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This Reference Document captures reference material derived from ongoing work on risk assessment frameworks. It summarizes a concept for developing an effective framework using the Seamless Border Focus Area as a 'test case' for scanning risk assessment approaches that could contribute to risk-informed decision making in support of the Border and Transportation Security Portfolio investment planning and analysis cycle.

Le présent document de référence contient de la documentation tirée des travaux en cours sur les cadres d'évaluation des risques. Il s'agit du résumé d'un concept permettant d'élaborer un cadre efficace en se servant de la question centrale que constitue la perméabilité des frontières comme 'cas type' afin d'étudier les approches en matière d'évaluation des risques pouvant contribuer à la prise de décision fondée sur le risque à l'appui du cycle de planification et d'analyse des investissements dans le portefeuille de la sécurité des frontières et des transports.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g., Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Risk assessment; border security; seamless border; methodology