Summary Report of Establishing a Risk & Capability Based Framework for Assessing CSSP Investments

Ian Bayne
CAE

Prepared by:
CAE
1135 Innovation Drive
Ottawa ON, K2K 3G7

Prepared for:
Shaye Friesen, DRDC – Centre for Security Science

Contractor's Document Number: 6012-003 Version 01
PWGSC Contract Number: W7714-135838-b
Technical Authority: Shaye K. Friesen, Risk Analyst, DKTTI, DRDC – Centre for Security Science

Contract Report
DRDC-RDDC-2017-C098
April 2017

CAE Inc.

1135 Innovation Drive
Ottawa, Ont., K2K 3G7 Canada
Tel: 613-247-0342
Fax: 613-271-0963

SUMMARY REPORT OF ESTABLISHING A RISK & CAPABILITY BASED FRAMEWORK FOR ASSESSING CSSP INVESTMENTS

CONTRACT #: W7714-135838-b

FOR

SHAYE FRIESEN

Risk Analyst, DKTTI
Defence Research and Development Canada
Centre for Security Science
222 Nepean Street
Ottawa, Ontario
Canada K1A 0K2

31 March 2017

Document No. 6012-003 Version 01

REVISION HISTORY

Revision	Reason for Change	Origin Date
Version 01 DRAFT A	Initial document issued.	16 March 2017
Version 01	Final document issued.	31 March 2017

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS AND DEFINITIONS

AF	Architecture Framework
AHRA	All Hazards Risk Assessment
BTS	Borders and Transportation Security
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosives
CCSS	Canada's Cyber Security Strategy
CI	Critical Infrastructure
CIPBS	Critical Infrastructure Protection and Border Security
CMM	Capability Maturity Model
CRA	Consolidated Risk Assessment
CSSP	Canadian Safety and Security Program
CSS	Centre for Security Science
DND	Department of National Defence
DRDC	Defence Research and Development Canada
GC	Government of Canada
GUI	Graphical User Interface
IoT	Internet of Things
OAG	Office of the Auditor General
PS	Public Safety Canada
PSTP	Public Security Technical Program
QW	Qualiware
RA	Risk Assessment
RBA	Risk-Based Approach
S&T	Science and Technology
SL	Scientific Letter
SME	Subject Matter Expert
SPG	Strategic Planning Guidance
SRA	Strategic Risk Analysis
SRA	Society for Risk Analysis
STEM	Science, Technology, Engineering and Mathematics
SWOT	Strengths, Weaknesses, Opportunities and Threats
WP	Work Package

1 INTRODUCTION

This report summarizes the work on risk assessment and related projects that Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS) conducted during the 2013-17 timeframe internally and by contracting with external resources. The report establishes a reference point and body of knowledge to support future work on risk assessments in support of the Canadian Safety and Security Program (CSSP) evidence-based and risk-informed decision making on multiple levels (i.e., strategic, program, focus area, portfolio/community).

Five (5) work packages (WP), and their respective sub-projects or activities are reviewed as follows: risk scan; risk assessment framework; risk assessment in targeted domains; architecture; and software application.

1.1 Background

The majority of the work was prepared and delivered as part of a Technology Investment project, *Establishing a Risk and Capability-Based Framework for Assessing CSSP Investments* (CSSP-2015-TI-2130). The work on Task 28 ultimately aimed to establish a coordinated approach to applying capability- and risk-based assessments to inform policy, planning, science and technology (S&T) investments, and to contribute to the CSSP priority setting process.

The Department of National Defence (DND) *Defence and Security S&T Strategy* highlights the importance of systematic approaches to risk assessment as an integral part of achieving strategic and other objectives (2013).

The CSS *2014/15 Strategic Planning Guidance* (SPG) stated:

> A core element of the CSSP business model relates to the application of a **systematic approach to understanding public safety and security risks and vulnerabilities,** and to frame the range of related challenges to which governments and society may have to respond (2014).

The 2015/16 SPG describes the main decision factors as:

- impact at both the individual project level and aggregate impact (i.e., how such endeavours will contribute to achieving the CSSP's identified outcomes and S&T requirements);
- how the evidence-base is proposed to be developed to maximize value for money; and
- how the results of the investments will be transitioned to either advisory products for decision makers or sustained technologies and/or capabilities for end-users (2015, p.5).

The management environment outlined above, and the dynamic global risk environment and pressures on budget planning, formed the backdrop for the risk assessment work summarized in this report.

1.2 Objective

Objectives of this summary report include:

- highlight key findings and results of risk assessment projects;
- contribute to knowledge management; and
- identify opportunities to exploit this body of work.

1.3 Audience

The primary audience for the report is DRDC CSS risk practitioners and managers who are involved in program governance, portfolio and project management, and program administration and decision support, including policy setting, strategic planning and performance measurement. While some references focus on specific portfolios or focus areas, the material, concepts and products are intended for use by other focus areas and at the program level. The work could also support information sharing with Government of Canada (GC) partners and the United States (US) Department of Homeland Security (DHS) S&T Division under the CA-US Critical Infrastructure Protection and Border Security (CIPABS) and other initiatives.

1.4 Scope

The summary focuses on five specific work packages. It does not consider other risk work during this timeframe including: support to the three-year effort of the interdepartmental working group that implemented multiple All Hazards Risk Assessment (AHRA) scenario-based workshops; Cybersecurity Architecture Framework project in support of Canada's Cyber Security Strategy (CCSS); CSS support to the first Anti-Money Laundering and Anti-Terrorist Financing National Risk Assessment project; support to security assessments for Parliament Hill and the physical threat and risk assessment methodology; and advice to the Public Safety (PS) Canada team developing the first National Risk Profile (NRP).

1.5 Assumptions

To implement, exploit and sustain the outputs mentioned below would likely require some documentation, training and possibly, other support. However, it is assumed that these adjustments would be incremental, and in some cases may only require a shift in thinking about risk management. Opportunities related to each work package are included below for discussion purposes.

1.6 Structure

Abbreviated references are included for each section. A list of the detailed references is at Appendix A. The references and project reports are available from DRDC CSS.

2 METHODOLOGY

The approach involved reviewing selected project and sub-project reports. The author identified other references to provide context or to augment the material (e.g., SPG and Narratives). The report follows a standard structure that aims to provide a balance of general and specific information for the reader. Preparation of this report did not involve extensive consultation with DRDC CSS management, staff or users of the project outputs, although some of this interaction did occur during specific projects. DRDC CSS iterative development and hands-on review process minimized the chances of inaccuracy or bias, and potential misinterpretation of the results of the various projects.

3 FINDINGS

This section summarizes DRDC CSS and contractor work on the five work packages that were intended to improve the value of risk assessments, and the contribution of risk assessments directly to CSSP decision making, and indirectly, to collaboration with partners, and understanding the strategic and operational risk environments from their diverse perspectives. Section or paragraph numbers are included in brackets, to be able to cross-reference with the documents.

3.1 Work Package 1: Risk Scan

References:

- Risk Scan: A Review of risk assessment capability and maturity within the CSSP. 2014.
- Understanding Existing Natural Hazard Risk Assessment Methods and Tools. 2015.

3.1.1 Context

DRDC CSS had articulated the requirement to compile a compendium of risk assessment techniques with a view to building a consolidated, cross-domain capability-based perspective of the maturity of RA practices in the 2013/14 timeframe (SPG, 2013). The Risk and Capability Integration Section initiated the risk scan project to address the SPG requirement, and to lay the groundwork for improving the visibility and value of risk information to CSSP decision makers.

The *Risk Scan* was completed in the October 2013 to March 2014 timeframe, under the Public Security Technical Program (PSTP) Task 25, using one principal consultant, supported by a DRDC CSS subject matter expert (SME). The project was originally called, *Risk Compendium and Synthesis Study*.

3.1.2 Objectives

The objectives of the *Risk Scan* included: identifying existing RA processes, tools and techniques used in, or familiar to, Portfolios and Communities of Practice; demonstrating a capability and maturity model self-assessment process; and highlighting opportunities to improve the consistency and value of risk assessment practices within CSSP.

3.1.3 Approach

The approach to structure risk assessment (RA) techniques was adapted from the international standard for risk assessment that summarizes thirty-one (31) RA and other techniques (CAN/CSA 30010-2009) – inputs, process, outputs, strengths and limitations. The main element of the approach was interviews with portfolio and community managers, and subject matter experts. Important inputs to the planning process were the output of the Community of Practice Summit (2013) and the CSSP literature available on the Partners' Collaboration SharePoint site.

The scan identified eleven (11) commonly used variables that are used to perform RA's. Many of them have different definitions from multiple sources. The study considered two types of assessments: those that CSS controlled or influenced; and those conducted by external organizations (e.g., partners) either individually or in cooperation with other partners. In both cases, federal subject matter experts with operational experience normally did the assessments.

A summary of different techniques and some implications was developed (see Table 2 in Risk Scan report). Some insights gained during interviews was included, and a cross-section of CSS managers were briefed on findings, which was a reasonable validation of the study. The report included observations on program governance and risk management with the aim of to making the link between RAs within portfolio management and decision making for science and technology (S&T) investment, and partners' RAs done in the different operational risk areas.

3.1.4 Results and Outputs

The study used a capability maturity model (CMM) technique, and strengths, weaknesses, opportunities and threats (SWOT) analysis to identify opportunities for process and RA capability improvement. The study found that there was limited visibility of partners' risk assessment and other decision support systems, and that the mechanisms to communicate risk information with partners or within CSSP were relatively ad hoc.

The project produced RA capability and maturity profiles for twelve (12) operational areas.[1] Other outputs include: summary of observations; compendium of RA techniques;[2] descriptions of the methodology; CMM frameworks; affinity diagrams to group similar or interdependent portfolios and communities to help define similar RA practices; concept of operations that presented a conceptual CSSP value proposition; and lists of acronyms and terms that cross disciplines. The report included an independent CSS-wide SWOT analysis.[3]

A consolidated CMM view across the program includes the following RA capability components: threat evaluation; hazard analysis; vulnerability analysis; impact analysis; operational risk analysis; and program/project risk analysis. The CMM shows that the area that is the least mature, and that is the most challenging, is the impact analysis. A list of observations developed in collaboration with the CSS SME was also provided. One conclusion was that, with few exceptions, "the focus of risk management is primarily on project delivery, monitoring, tracking and execution, and most portfolios are insufficiently leveraging risk assessment techniques to manager the portfolio responsibilities" (2014, p.23). The report also summarizes the benefits of measuring RA processes.

[1] 'Operational area' refers to the end-user environment and therefore, the intended use of the S&T investments, as seen through the eyes of the CSS Portfolio and Community of Practice management team.
[2] The compendium for Borders and Transportation Security (BTS) and inter-related portfolios has been expended (i.e., focus area horizon). Resources are included in the SRA for Seamless Borders Environmental (2017) report.
[3] The consultant produced the analysis as a by-product, and to support the CMM assessment.

3.1.5 Opportunities

Opportunities include: update and maintain the compendium, and consolidate it with similar outputs from other projects, in particular, a strategic risk assessment or NRP; implement a process to share lessons across communities and develop a strategy to improve RA capability and maturity; review the value proposition concept of operations (CONOPS) and extend it to CSSP decision support systems in general; review the responses that were not available at the time and identify significant gaps; and standardize risk techniques and terminology for general and specific RA applications.

3.2 Work Package 2: Risk Assessment Framework

References:

- Preliminary Framework for CSSP Risk Assessment: Establishing a Method and Process for Assessing the CSSP Distribution of Investments. 2015.
- Comprehensive Scan for CSSP Risk Assessment Framework: Establishing a Method and Process for Assessing the Distribution of Investments. 2016.
- Establishing resilient programs… Briefing to Society for Risk Analysis (SRA) Conference. 2016.
- Scientific Letter. Risk Assessment Framework – Seamless Borders. Draft. March 2016.

3.2.1 Context

The absence of a common RA framework (RAF) within the CSSP means that it is difficult to validate collective decision making, and to provide evidence for how RA's influence the identification of capability gaps and the prioritization of investments. This gap is exacerbated when the RA's have a narrow scope and other constraints such as events in Canada within a sept timeframe. The expectation is that an assessment framework would help senior management and portfolio managers to identify evidence that the communities are assessing the right risks in a consistent manner for their communities (best-fit for purpose), and they are considering multiple timeframes. The RAF would contribute to optimizing the CSSP distribution of investment decisions, and justifying the program structure and future changes.

GC central agencies, designated Lead Security Agencies (LSAs) and primary departments[4] provide guidance on RA. However, GC leaves it up to departments to implement RA (and risk management) within their own environments. The team consisted of completed the one principal consultant and two architects, supported by a DRDC CSS SME. The team completed the work in the July 2016 to March 2017 timeframe under CSSP Technical Investment Task 25.

[4] The GC uses different terms to identify the lead organization(s) for interdepartmental structures and initiatives.

3.2.2 Objectives

Risk Assessment Framework and Architecture

The objective was to develop a Risk (and Capability) Assessment Framework that supported informed decision making at the community, portfolio and program levels. A secondary objective was to establish an approach and define requirements for using architecture framework (AF) techniques to demonstrate the value of risk information as one input to decision making.

Comprehensive Scan

The literature scan reviews lessons from international organizations, the European Community and Canada's allies to capture a broad set of literature that describes techniques and tools that are being used to support decision making, and for prioritizing transnational and national investments in safety and security risk and resilience management systems.[5]

3.2.3 Approach

Preliminary RAF and Architecture

The approach included interactions with some DRDC CSS managers and stakeholders for data collection, and to validate the emerging RAF using multiple semi-structured walk-throughs. The team also applied an architecture framework (AF) methodology to elicit requirements and support the RAF design. The methodology is shown in Figure 3-1.

Figure 3-1: Risk Assessment Framework Methodology

The Comprehensive Scan builds on the initial RAF work. During the project, the focus shifted from developing a theoretical framework to focusing on a practical application using the Seamless Borders Focus Area as a reference point.

[5] A SL was an internal document to outline a concept to use Seamless Borders as a test case for the RAF. DRDC CSS did not publish the SL. However, some outputs were brought forward in a draft Scientific Brief, and subsequently, in a Project Reference Document, which was published (2017).

Comprehensive Scan

The literature scan used a four-step process:

- Step 1: Sampling – gather a broad sample of international reports identified by researchers and DRDC CSS;
- Step 2: Differentiate risk domains – present a model that helps to differentiate operational risk domains based on a domain's use of similar RA concepts, terminology and techniques;
- Step 3: Prioritize references – select references that provide broad coverage within and preferably, across domains; and
- Step 4: Lessons – identify lessons for the RAF and that support decision making within and across Focus Areas.

The CSSP risk domains were segregated on a conceptual level into three thematic groups to identify similar RA practices: security and critical infrastructure; public safety, health and environment; and emergency management, resilience and disaster risk reduction.

The consultant used eight (8) themes to describe the analysis to highlight relevant lessons for the CSSP, and Canada more broadly: challenges; RA process management; expected benefits; concepts; scenarios; assessment techniques; and communications and decision support. The scan report maps findings to the RAF building blocks that are described in the Preliminary RA Framework report. Since DRDC CSS was developing its performance measurement approach at the time, the scan report also highlighted some lessons on (RA) performance measurement.

3.2.4 Results and Outputs

Preliminary RAF and Architecture

The project produced an RAF model with four building blocks:

- CSSP investment distribution concept;
- common evaluation framework;
- classification schema; and
- standardized terminology.

The building blocks are described using the following thematic structure[6]: objectives; context; inputs; techniques; outputs; and limitations.

[6] Adapted from the format used in CAN/CSA 30010:2010 Risk assessment techniques to describe discrete processes and techniques in a consistent manner.

Other outputs included: a RAF conceptual model; a model for combining risk and capability inputs; evaluation concept; a set of acronyms that could be expanded and maintained in a Wiki-style tool; some preliminary working models including a terminology landscape; a data model development concept; a concept for defining standard program risk types; safety and security RA domains; and a working paper to summarize the architecture development approach.

Comprehensive Scan

Comprehensive scan outputs included: a model for differentiating CSSP risk areas; a discussion of how risk information supports the CSSP development of S&T Requirements conceptual model - four focus areas and five enablers. The sections on concepts, scenarios and assessment techniques offer the most potential for further analysis and refinement. The report also discusses communications and decision support lessons, in particular for a multi-dimensional problem space, which is relevant to the CSSP focus area construct.

NOTE:	The concept of illustrating multi-risk events (4.7.2, Figure 4-4), the holistic RAF (Figure 6-2) and the architecture concepts were adapted for the Seamless Borders SRA project (Refer to Section 3.3.3 below).

NOTE:	The scan and description of risk variables was an input to the software application project (WP5).

The scan includes: recommendations for future scans or investigation; examples of national planning and threat / hazard scenarios; and working models that were reused for the Project Reference Letter (2017) and the Society for Risk Analysis engagement activity.

3.2.5 Opportunities

Preliminary RAF and Architecture

In terms of the RA framework, opportunities include: developing a DRDC CSS risk toolkit that addresses gaps and inconsistencies in existing processes, and that supports the alignment of multi-dimensional risk management that would span safety and security jurisdictional, cultural and other boundaries; and evaluating the RA concepts, possibly within a given Focus Area or complex portfolio.

Comprehensive Scan

Literature scanning opportunities include: exploiting the findings related to scenarios and impact assessment frameworks to support the Seamless Borders Focus Area; developing and maintaining a watch list for international resources, preferably supported by a collaborative environment, with search and edit features, and possibly, Wiki capabilities; leveraging the strategic risk assessment (SRA) framework; exploiting the section on terminology and acronyms to develop a CSSP portfolio management guidebook or an on-line, safety and security risk lexicon, which can be compared to the DHS Risk Lexicon.

Another opportunity is to consider the Comprehensive Scan findings on performance measurement to support the next iteration of the CSSP Performance Measurement Strategic Plan, and to incorporate an integrated approach to performance and risk indicators (e.g., lag and lead indicators, respectively). There should also be value in leveraging the international work on scenarios, possibly in support of the emerging PS Canada work on developing the NRP project with GC partners and DHS work on operational and/or risk scenarios. The 18-month RA framework project could be revisited, adapted and/or streamlined to take advantage of PS initiatives, such as the Regional Resilience Assessment Program (RRAP) and regional networks, possibly using modern information technology (IT) tools (e.g., crowdsourcing and on-line surveys).

3.3 Work Package 3: Risk Assessment in Targeted Domains

This section describes three activities that were implemented by DRDC CSS risk specialists and Portfolio Managers with contractor support.

3.3.1 Chemical, Biological, Radiological, Nuclear and Explosives (CBRNE)

The primary references include:

- Chemical Consolidated Risk Assessment (CRA) Workshop Results, October 2016.
- Biological CRA Workshop Results, July 2016.
- Radiological/Nuclear CRA Workshop Results, June 2016.
- Explosives CRA Workshop Results, November 2015.

3.3.1.1 Context

CBRNE CRA

The CRA process historically supports CBRNE decision making and prioritization of threats and hazards. DRDC CSS developed the CRA methodology as part of the CBRNE Research and Technology Initiative (CRTI). The CRA uses an intelligence- and science-based approach to consolidate assessments of multiple factors outlined below.

> Strategic Priority – Improve capabilities for early detection, location, and identification of chemical, biological, radiological, nuclear, and explosives (CBRNE) threat materials and support the research, development, and transition to operations of new capabilities to prevent / mitigate, prepare for, respond to, and recover from CBRNE events. (Jonkmans, 2015)

Characteristics of the CBRNE environment include: focus on malicious threats where there is little historical data; and a significant reliance on intelligence community to estimate terrorist capability and intent. Two key issues related to assessing the source of terrorism risks are that there is significant uncertainty due to the availability of classified and/or

open source data, and the objective to assess intent is challenging even for specialists. The methodology has been adapted for multiple applications including radiological / nuclear (R/N); chemical / biological (CB) and explosives, and it has considered threat scenarios that cover multiple communities (e.g., explosives to spread threat and hazard effects over different timeframes and geographic spaces).

Concerned that the risk assessments had not been done for a few years, a team committed to deliver the full suite of risk assessments across all 5 CBRNE domains in one year, which is exceptional and above and beyond normal expectations. The CRA update effort was delivered by a cross-centre team of individuals who engaged CSSP partners in an evidence-based assessment of risks and threats to operations. Partners saw this as a very high value proposition, with more than 100 personnel dedicating their time and energy to the cause at their own expense. The effort culminated in September 2016 with a final briefing of the results to stakeholders, including DHS and the Domestic Nuclear Detection Office (DNDO). The CRA epitomized the value-added of DRDC CSS and its leadership in engagement that has come to be expected by OGDs, operators, and the broader safety and security community. The workshops brought together policy, scientific and operational leaders from all levels of government, as well as members of DRDC CSS to discuss the trends and drivers, capability gaps, priorities, and emerging issues affecting the Explosives community. The workshop leveraged CSS expertise in risk analysis and explosives threats

3.3.1.2 Objectives

CBRNE CRA

Objectives of the CRA methodology include: balance practicality for decision-making with analytical rigour; incorporate Public Safety (RN, E) and health (CB, infectious disease; animal, food and agriculture) security risks; provide a methodology that is systematic, defensible and transparent; and demonstrate a process that engages diverse specialist stakeholders including international SMEs.

3.3.1.3 Approach

CBRNE CRA

The methodology combined Vulnerability with Intelligence Judgement to provide an ordered ranking of risks (synonymous with threats or hazards). Intelligence Judgement considers the amount and reliability of intelligence. It is an assessment of the terrorists' intent and capability to carry out a specific attack scenario. Participants assign confidence ratings of the assessment (i.e., process and output) and/or input information, as an integral part of the process.

The simplified methodology includes four steps:

- **Step 1:** Develop characteristic scenarios that describe CBRNE events;
- **Step 2:** Evaluate vulnerabilities of each scenario using matrices (Relative Technical Feasibility and Impact);

- **Step 3:** Assess the likelihood of each scenario by factoring in Intelligence Judgement; and
- **Step 4:** Determine the degree of risk for each scenario using a risk matrix (combines Vulnerability and Intelligence Judgement).

The scope of the engagement was as follows: adjusting and refining the CRA methodology; developing a software tool for the CRA process; providing an on-site methodology awareness briefing; reviewing and validating explosive hazard scenarios, and identifying new scenarios; data collection and assessment using the structured CRA methodology; verification of results with key stakeholders; the development of graphs to assist in visualization of results; and analysis to inform the investment priorities, S&T requirements and gaps for the CSSP in CBRNE domains.

3.3.1.4 Results and Outputs

The CRA tested several innovative concepts including the application of threat and hazard scenarios. Specific vignettes were used to describe how a threat and/or hazard could come to exploit a target vulnerability, including time and spatial factors. The project also tested scoring techniques to quantify and combine assessments for multiple factors including **vulnerability** (e.g., scored as a function of the feasibility and impact of the occurrence of a scenario vignette). The assessment of Vulnerability combined the **Relative Technical Feasibility** (i.e., combination of materials, equipment, expertise, and knowledge), and **Impact** (e.g., human loss, intensity of response, level of disruption and economic loss). A representative output is shown in Figure 3-2, below. The size of the ellipses is a graphical technique to illustrate a confidence associated with the factors being assessed.

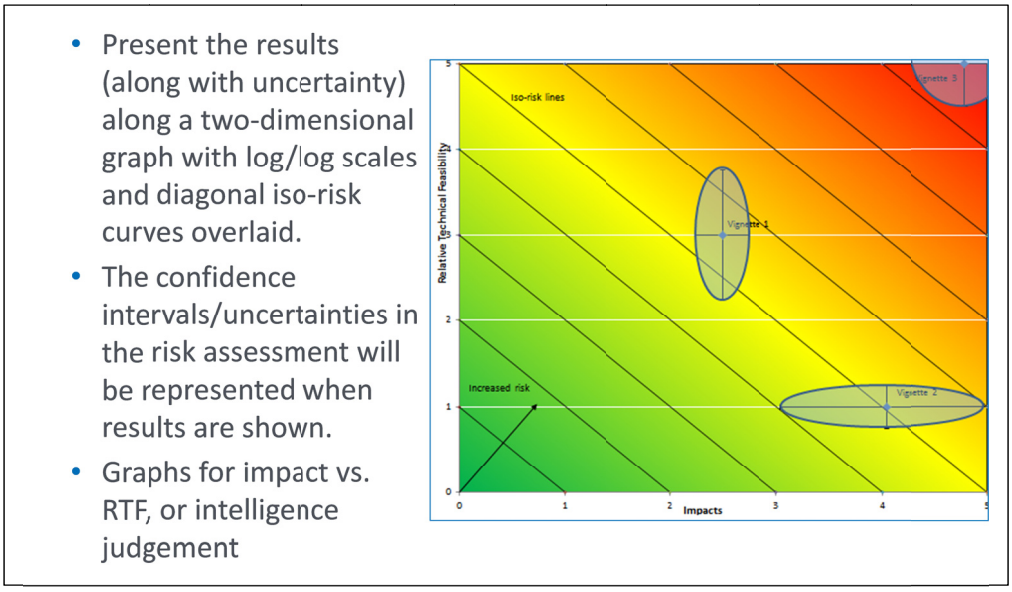

Figure 3-2: Representative CRA Output

3.3.1.5 Opportunities

DRDC CSS has applied the CRA concepts to national security and safety domains. There are opportunities to continue to apply and adapt the methodology further including in the health, and animal, food and agriculture security areas. There are opportunities to relax some of the constraints on the intelligence judgement to consider a broader set of scenarios and what-if analysis, and extend and expand the analysis to incorporate non-malicious threats and hazards.

The opportunity and challenge is to continue to develop specialized tools and expertise in order to sustain this unique knowledge area and capability (i.e., applicable to CBRNE and CRA). There is an opportunity to implement a centralized solution for collaboration and scenario management by consolidating the scenarios and vignettes that have been developed within the CBRNE and other areas. The idea of a central knowledge base to support scenario planning was presented earlier (Hales, 2010).[7]

The work on explosives shows that there are opportunities to apply the assessment technique across CSS communities to gain a richer sense of the threat environment, and how the assessments influence decision making across communities to mitigate risk or to take more risk. The workshop also demonstrates the value of having diverse stakeholder input to: define national capabilities for effective prevention, preparedness, and response to each of the scenarios; to assess existing capabilities; and to identify priorities for investment. The workshop demonstrated an evidence-based, traceable and defendable approach to identify and prioritize Canadian capability gaps.

3.3.2 Cybersecurity – Literature Scan

References:

- Cybersecurity literature scan (Fowler). 2016.
- e-Security Narrative. 2013.

3.3.2.1 Context

The e-Security[8] Portfolio's primary objective is to support the e-Security aspects of Critical Infrastructure (CI) Protection as defined by PS Canada in the Canadian Cyber Security Strategy (CCSS, 2013). The portfolio focuses mainly on the telecommunications, energy and utilities CI sectors. The portfolio narrative states,

> CSSP provides an evidence-based decision-support mechanism by gathering, analyzing, and disseminating information on security threats, vulnerabilities, and incident

[7] Hales, D., and Race, P. (2010). P*ublic Security Technical Program (PSTP) Planning Scenario: Final Report*. DRDC CSS CR 2010-10. December 2010.
[8] The terms e-security and cybersecurity are used interchangeably.

> vectors, this provides the basis to invest in projects that provide countermeasures, and best practices to help inform private sector cyber security decisions and subsequent actions (2013, p.25-26).

A co-op student completed the study during the September 2016 to January 2017 timeframe, in consultation with CSS SMEs.

3.3.2.2 Objectives

The environmental scan's objectives included: providing an overview of a complicated domain in order to inform the CSS e-security portfolio; and contribute to a future risk assessment of the cybersecurity domain.

3.3.2.3 Approach

The scan methodology considered two domain mapping techniques. One is a structured approach based on a taxonomy. The second is a less structured concept that involves selecting a representative range of particular examples to provide a broader, but possibly less cohesive understanding of the domain. The second approach was chosen mainly due to the complexity of the cybersecurity[9] domain.

The approach selected references by defining four cyber domain components - attacks, technical infrastructure, socio-cultural environments, and actors; and using specific criteria[10] to select the following significant factors:

- Ransomware;
- Internet of Things (IoT); and
- Dark Markets and Malware Authors.

3.3.2.4 Results and Outputs

The information resources fall into three main groups: open source cyber intelligence reports (not-for-profit organizations and private sector service providers); credible new media; and academic research.[11] Key findings were presented in three sections. Ransomware; IoT; and Dark Markets and Malware Authors. The report offers suggestions for mitigation and/or prevention in the first two groups.

The report summarizes technical developments in 2016 to support community work in the near-term. A key conclusion is that, given the dynamics of the environment, "This scan must be

[9] Although the Community of Practice is called e-Security, the term cybersecurity is used because this is the commonly used term within GC and broader community. It is noted that partners use other terms, for example: IT Security; Information Security; Electronic Warfare; Cyber Warfare; and Information Warfare.
[10] The criteria for selecting significant factors for the scan were: (a) significant impact in 2016, (b) likely to have large impacts in the near future, and (c) CSSP, if it chooses to allocate resources in these directions, could have influence (2016, p.2).
[11] Academic research focused mainly on university Science, Technology, Engineering and Mathematics (STEM) resources.

maintained and supplemented regularly in order for it to maintain any relevance in projects or analysis any distance in the future" (2016, p.20).[12]

3.3.2.5 Opportunities

There are opportunities to develop a watch list of relevant resources to support situational awareness of the dynamic cybersecurity risk universe, and to consider cybersecurity risk scenarios in multiple critical infrastructure sectors.[13]

3.3.3 Strategic Risk Analysis for Seamless Borders Environment

References:

- Strategic Risk Analysis for Seamless Borders Environment: Literature Scan. 31 March 2017.
- Risk Assessment Framework: Seamless Borders Pilot Project, Reference Document. 2017.

3.3.3.1 Context

This project built on the RAF project work and desire to use Seamless Borders as a use case for further develop the concepts and tools. The SPG (2015) describes the "key drivers in this area for Canada are both generic (e.g., terrorism, human smuggling, the importation of illicit drugs and firearms) and specific (e.g., evolving policy and security priorities, advances in self-service, biometrics and other technologies). Two particular challenges are noted: balance between security and privacy; and the Arctic. The *Seamless Borders Focus Area Narrative* includes a conceptual planning cycle that includes the identification and prioritization of high-level risk scenarios as tools to,

> raise the profile of risk-informed decision making, so that the seamless border focus area migrates from a fragmented view of risk, to a more unified and strategic view of the top risk scenarios and improved visibility of the link to "action-oriented" S&T investment priorities (2015, p.7-8).

3.3.3.2 Objectives

The strategic risk analysis report report summarizes findings from a scan of literature related strategic risk analysis and other techniques, as an integral part of multi-criteria decision making related to the CSSP, the Seamless Borders Focus Area, and the Border and Transportation Security, and interdependent portfolios.

[12] The draft report does not include a bibliography, which will presumably be in the final or is available from CSS.
[13] The SRA project included a few cyber risk specific scenarios related to Seamless Borders.

3.3.3.3 Approach

The literature scan was conducted during the July 2016 to February 2017 timeframe. While DRDC CSS provided some material, most of the resources were from CA and US government public web sites, and other open source literature. The focus of the study was at a strategic level. Therefore, to contain the literature search and to focus on priority risks types, the following areas received limited attention: national security and sovereignty; the Arctic; environment and climate change; natural disasters; accidents; and technological and infrastructure failures.

DRDC CSS identified several themes to guide the literature scan and analysis. Since CSSP and the Focus Area do not have a risk taxonomy or other characterization of risks, the study did a brief stakeholder analysis, and characterized the risk environment into seven (7) risk domains:

- border security;
- transportation security;
- organized crime;
- financial crime;
- health security;
- animal, food and agriculture security; and
- cybersecurity.

The Arctic, which would likely require a literature search on its own, is partially considered under the health, and animal, food and agriculture security domains. For example, the strategic risk report highlights the relationships to borders and transportation by considering the impact and cascading effects in the identification of risk scenarios. In this way, risks related to the Arctic would converge. For example, the report indicates that the following factors could be considered within a few risk scenarios - national security and sovereignty; the potential impact of climate change or major oil spills on the food chain, economy and the way of life of Indigenous Peoples, Inuit and Metis; the dependency on the existing transportation critical infrastructure (e.g., vital services including: lifeline, medical, education and legal services in remote communities); and community resiliency. This concept has implications for future collaborative approaches to RA, critical infrastructure investment, and prioritization of safety and security S&T investments.

3.3.3.4 Results and Outputs

Outputs of this study included: a baseline for developing an SRA process and a framework for shaping a set of high-level risk scenarios that can be tailored for multiple audiences and purposes; and an approach that is adaptable for other focus areas and for the CSSP planning cycle. The concept is that by using complex risk scenarios, supported by other tools, DRDC CSS could complement the existing special, mostly bottom-up threat and hazard assessment snapshots. The review of US DHS literature indicates that the DHS S&T Division faces similar

challenges. The literature review confirms that there are few examples of unifying concepts that help organizations consolidate risk information across the broad safety and security landscape. Even the DHS risk management approach is based on the historical security threat assessment model that combines threat, vulnerability and consequence, and that most risk scenario work to date is mainly focused on specific threats and hazards, which runs the risk of diffusing limited RA resources and focusing limited S&T funds on solving today's problems.

Outputs include: thematic analysis of GC and international literature, mainly US;[14] characterization of the Seamless Borders risk environment (7 risk domains); an extensive list of US and other resources; a short list of resources that should be available to CSS and/or its partner; characterization of the risk environment; a representative multi-risk scenario planning framework; and some suggestion for next steps.

3.3.3.5 Opportunities

The opportunities include: confirm the status of key partners' risk assessment approaches; validate and refine the SRA process and supporting tools; test the concepts using Seamless Borders or another focus area of complex portfolio as test case; identify opportunities for sharing information with DHS S&T Division risk counterparts, possibly building on the RRAP and/o NRP work (e.g., program evaluation; strategic risk analysis; and scenarios); and establish a watch list of key resources to maintain situational awareness of transnational and international developments, specifically focused on Seamless Borders' areas of interest.

3.4 Work Package 4: Architecture - Interoperable Modeling for Risk Assessment

References:

- Architecture contribution to evidence-based and risk-informed decision making within the Canadian Safety and Security Program (CSSP). CAE. 31 March 2017.

- Preliminary Framework for CSSP Risk Assessment: Establishing a Method and Process for Assessing the CSSP Distribution of Investments. 2015.

The architecture work builds on DRDC CSS experience and the definition work done in the RA framework project (see WP2). Initially, the RA framework work focused on a generic architecture, but in September 2015, the focus shifted to a practical application, which focused on the Seamless Borders Focus Area to demonstrate how an AF could highlight risk resources related to evidence-based assessments in support of program and portfolio objectives.

[14] The Comprehensive Scan focused on Europe and other international literature mainly focused on national risk assessments and the use of risk scenarios to enable risk prioritization.

3.4.1 Context

The team developed the architecture between October 2016 and February 2017. Constraints included: the decision to use Qualiware (QW) was made in August; the software license was obtained from DND and training was completed in September 2016; limited documentation was provided (e.g., one Focus Area Narrative); and there was limited interaction with portfolio managers and DRDC CSS SMEs. The architecture team completed the prototype in parallel with the Strategic Risk Analysis for Seamless Borders: Literature Scan project.

An AF is the structure that supports the structured collection of processes, techniques, artifact descriptions, reference models and guidance for the development and organization of a specific Enterprise Architecture (EA). For this application, the team uses the AF to highlight where RA is currently used (as-is), and to highlight how it could be used to consider to-be options, which should be integrated into the normal portfolio and program management systems.

3.4.2 Objectives

Strategic objectives are to demonstrate the potential for architecture to inform evidence-based decision making, and to show that architecture views support the visualization and evaluation of risk and capability information on multiple levels. The project provided input to the software application project. This project aimed at developing and improving the internal RA capabilities to support the CSS Annual Planning Process and to enable the CSSP to consolidate RA and improve communication of risk results across domains and Portfolios.

3.4.3 Approach

A separate report describes the methodology. The development process consisted of four phases, including: data collection; framework and validation cycles; population of the architecture; and final approval. Figure 3-3 describes the phased approach. The Section numbers refer to the architecture report (2017). Some initial thoughts on exploiting this work are also included in this report.

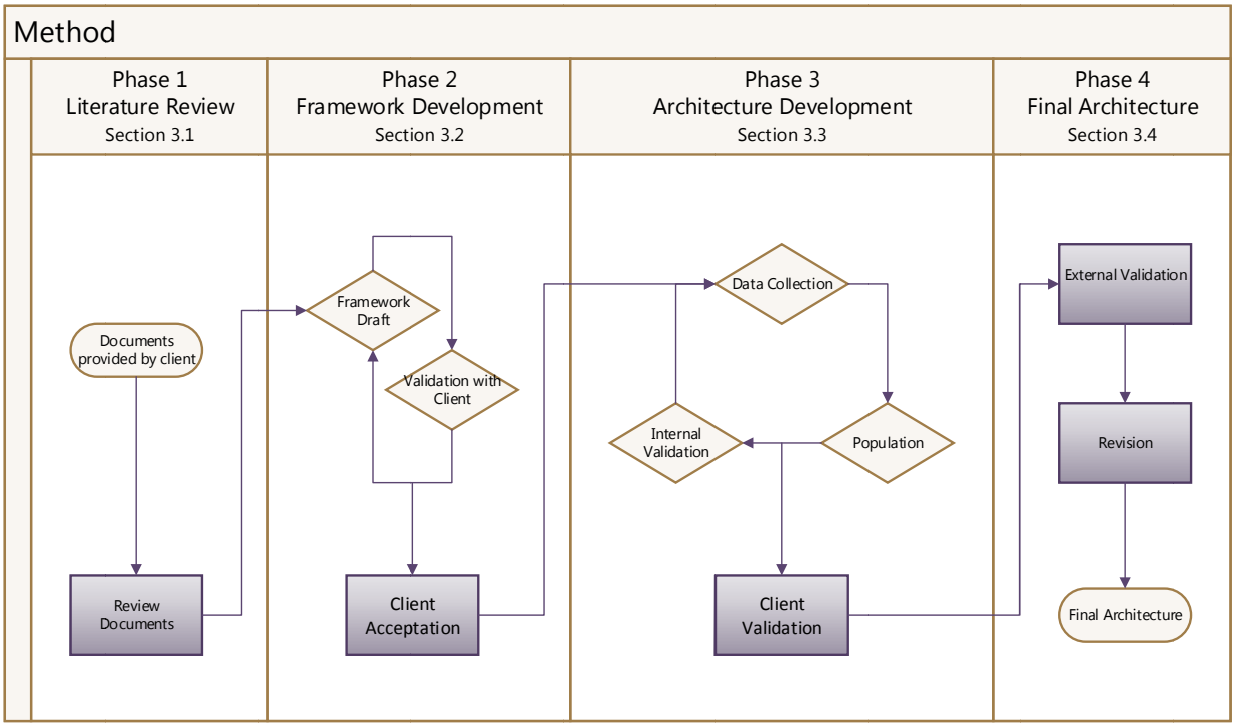

Figure 3-3: Overview of Architecture Development

3.4.4 Results and Outputs

The architecture views demonstrated that there is little mention of RA's in the CSSP Annual Planning process. With the help of SMEs, some placeholders are included in the architecture views to identify where RA should be integral to the normal management processes.

The results present a road map for adopting AF as a technique and tool to help managers to implement a more systematic approach to RA including improvement of situational awareness of trends in the strategic and operational risk environments. The AF can facilitate awareness of partners' RA approaches, which would contribute to the evidence base that partner, and CSS, consider risk along with other decision factors in their capability gap analysis and investment prioritization processes.

A working prototype architecture focuses on Seamless Borders was produced that can be shared and validated using HTML version. The framework can demonstrate the links between strategic objectives, S&T challenges, program and portfolio priorities, gaps, risks and project outcomes. It can help to link operational and risk scenarios. It can also support information sharing, data collection planning and risk analysis including strategic and operational risk environments.

Outcomes included: a detailed description of the methodology; html links in the report to artifacts and views (Section 4); separate .qrp file that includes screenshots (e.g., preliminary

taxonomies); recommendations and next steps; expected benefits of exploiting the AF; the project data collection plan; sample architectural views including Portfolio and Community of Practice snapshots; some representative RA methodologies; and some preliminary taxonomies.

A preliminary planning framework related to the use of architecture tools to align and provide evidence of RAs across the program is also included. This framework is an input to the architecture report.

3.4.5 Opportunities

CAE recommends that DRDC CSS use the architecture views to identify the gaps and modify the existing processes to include RA where applicable. Depending on what DRDC CSS decides to do with EA (and QW), there are several opportunities to build on the Seamless Borders AF work including:

- Incorporate an inventory of the different types of high-level risk scenarios and supporting threat and hazard-specific scenarios and vignettes to evaluate the architecture as a scenario management tool.

- Incorporate stakeholders' RA practices and the most current RA outputs to provide evidence that partners considered risk in their identification of gaps and investment priorities, and use the AF to complement portfolios and CoP managers' understanding of the operational risk environment.

- Incorporate an inventory of partners' impact categories and assessment approaches, and support investigation of a unifying framework to support comparison of assessments across Seamless Borders risk domains.

- Include process flow diagrams to illustrate general and specific RA processes (i.e., risk; threat / hazard, vulnerability; criticality; resilience; etc.) and link them to RA placeholders included in the architecture views. This would support the use of standardised RA methodologies; and contribute to data collection, evidence gathering, and performance measurement; and facilitate knowledge management within DRDC CSS.

3.5 Work Package 5: Risk Application -Prototype Software for Data Analytics

References:

- Risk scan: a review of risk assessment capability and maturity within the CSSP. 2014.

- Software Applications Support for All Hazards Risk Analysis within CSS. 2016.

3.5.1 Context

The expected outcomes of this effort are either to recommend options and provide advice for acquiring a commercial-off-the-shelf (COTS) tool, or to design and build a prototype graphical user interface (GUI) and searchable database. This tool would support the decision making (e.g., prioritization of investments, data collection and analysis), and comparing risks and/or risk assessments, by evaluating them against common criteria.

3.5.2 Objectives

The study examines industry software to assess its suitability for internal use by risk analysts and portfolio managers. The report provides preliminary recommendations and options from which an enterprise risk management (ERM) solution or risk analysis application could be developed to support the CSSP. The two main objectives are: to document high-level requirements for a capability- and risk-based solution; and to confirm if there are existing software tools that could be adapted to meet CSS's requirements in the near-term.

3.5.3 Approach

The analytical approach builds on previous work including: the All Hazards Risk Assessment (AHRA) framework, applied to emergency management and disaster risk reduction; the CRA, applied to CBRNE communities and counter-terrorism; and associated templates and automated (SharePoint-enabled) rating tools (e.g., Capability Assessment Management System), as well as consultations with relevant stakeholders and senior management. The concept considers the CSS continuous planning process, and design options for improving the management and visibility of dynamic threat and risk environments.

The approach consists of the following steps: needs analysis; requirements analysis; market scan and product research; comparison of requirements; data modeling; and design of a working prototype.

3.5.4 Results and Outputs

Twenty-eight (28) products were compared (on paper) using the following criteria:

- investment-focused;
- wide use in government;
- supports multiple processes;
- customizable visualization; and
- database/API access.

The study concludes that the COTS solutions are not fit-for-purpose and/or cannot be easily customized for the DRDC CSS intended purpose. Outputs include: hierarchy of portfolio, risk

and CSS priorities; example of an open source visualization library (Tree map); list of software applications that were reviewed; conceptual data model for a portfolio risk visibility tool; and a prototype web-based platform.

3.5.5 Opportunity

There is an opportunity to exploit the tool to sustain the analysis of how risk information, combined with other factors, supports investment prioritization and evaluation processes.

4 CONCLUSION

This report summarizes five projects and their sub-projects, where applicable. The work supports the advancement of risk science in DRDC CSS, and it investigates techniques, frameworks and tools that contribute to evidence-based assessments, and decision support on multiple levels, and across safety and security risk domains. The report highlights some opportunities to support discussions, and to help maintain continuity and knowledge within CSS. Each project has its own reports and recommendations. This report provides a snapshot of the WP references with cross-references to specific sections of the source documents. A planning framework related to the continued use of architecture tools to align and provide evidence of RAs across the program is included at Appendix B for discussion purposes.

APPENDIX A REFERENCES

Bayne, Ian. (2016, December 08). *Study Plan for a Seamless Borders Risk Assessment Study*. PowerPoint.

Bayne, I., and Friesen, S.K., (2017, January). *Risk Assessment Framework: Seamless Borders Pilot Project*. Project Reference. DRDC-RDDC-2017-D081.

Bayne, I., and Friesen, S.K., (2014, June). *Risk scan: a review of risk assessment capability and maturity within the CSSP*. DRDC-RDDC-2014-R36.

CBRNE Workshop Observations (I. Bayne). Version 3. September 2016.

CAE Inc. (2017, March 31). *Architecture contribution to evidence-based and risk-informed decision making within the Canadian Safety and Security Program (CSSP)*. CAE document No.113129-005-01.

CAE Inc. (2016, March 21). *Comprehensive Scan for CSSP Risk Assessment Framework: Establishing a Method and Process for Assessing the Distribution of Investments*. CAE Document No. 5843-011 Version 06.

CAE Inc. (2015, November 17). *Preliminary Framework for CSSP Risk Assessment: Establishing a Method and Process for Assessing the CSSP Distribution of Investments*. CAE Document No. 5843-011, Version 03.

CAE Inc. (2017, March 31). Scientific Letter. *Risk Assessment Framework – Seamless Borders*. CAE Document No. 5843-012 Version 02. Draft.[15]

Centre for Security Science. (2013). *Borders and Transportation Security (BTS) Portfolio Narrative. Strategic Planning Guidance (SPG)*. BTS Annex.

Centre for Security Science. (2013). *CSSP Environmental Scan*.

Centre for Security Science. (2013). *e-Security Portfolio Narrative*. Strategic Planning Guidance (SPG). E-Security Appendix.[16]

Centre for Security Science. (2015). *Seamless Borders Focus Area Narrative*.

Centre for Security Science. (2014). *Strategic Planning Guidance (SPG) 2014/15*.

Centre for Security Science. (2015, July). *Strategic Planning Guidance (SPG) 2015/16*.

[15] This document was not approved in the brief format. It was adapted to a Scientific Letter, and then to a Project Reference Document. It is included in this report to capture the outputs, to avoid them being lost.
[16] Although CSS shifted to Focus Area Narratives (2014), the portfolio / community narratives (2013) are valid for this report. It was not confirmed if managers are maintaining these lower level narratives.

Department of National Defence (DND). (2013). *Defence and Security S&T Strategy.*

Fowler, E., (2016). *The cyber domain: a 2016 environmental scan.* CSS. Draft.

Friesen, S.K., (2016, December). *Establishing resilient programs: using a risk-based approach for informing the distribution of investments in public safety and security science and technology*. Presentation at the Society for Risk Analysis (SRA) Conference.

Friesen, S.K., (2015, November 09). *Explosives CRA Workshop*. DRDC-RDDC-2015-L396. Scientific Letter.

Friesen, S.K. (not dated). *CRA Methodology Explosives*. CSS. PowerPoint.

Friesen, S.K. (not dated). *CBRNE Consolidated Risk Assessment Methodology*. DRDC.

Godsoe, M., (2015, September 23). *Understanding existing natural hazard risk assessment methods and tools*. DRDC-RDDC-2015-B025. Scientific Brief.

O'Donnell, D., (2016, August). *Software Applications Support for All Hazards Risk Analysis within the Centre for Security Science*. DRDC-RDDC-2016-C288.

Risk Management Guide for Critical Infrastructure Sectors. Version 1.0. PS. 2010.

APPENDIX B ARCHITECTURE SUMMARY

This appendix summarizes options and design questions for building on the RAF architecture work.

Way Forward	Discussion of Options
Options	
Option A – Strategic Level	**Link Seamless Borders prototype to program level (possibly in combination with B and/or C)** • Include other Focus Areas Narratives (existing model only considers Seamless Borders Narrative) – links between focus areas and enablers • Reuse products from Seamless Borders to establish common risk lexicon, acronyms and watch list of references and web sites; and review options for consolidating portfolio resources • Link to CSSP Performance Measurement Strategic Plan (i.e., CSSP indicators) • Link to CSSP dashboards or trend analysis (risk exposure; investment history; case studies; typologies) • Link to CSSP governance • Link to DRDC S&T Strategic objectives • Link to Public Safety (PS) strategies and action plans (e.g., critical infrastructure; cybersecurity) • Link to CA-US agreements (e.g., CIPABS; cybersecurity) • Link to Office of the Auditor General (OAG) reports
Option B – Program Level	**Extend Seamless Borders prototype to other Focus Areas** • Identify links between Focus Areas and Enablers, starting with Threats and Hazards Mitigation • Expand Threat and Hazard Mitigation Focus Area and link it to other Focus Area Evidence-based Assessments • Identify partners' from Focus Areas Narratives ○ Develop partner dependency matrices to support gap analysis of RA techniques and outputs to improve CSS managers' understanding of partner's risk environment and practices
Option C – Focus Area Pilot Project	• Continue with Seamless Borders • Incorporate inventory of complex scenarios, and stakeholder and impact assessment frameworks

Way Forward	Discussion of Options
	• Inventory of threat and hazard-specific scenarios (vignettes), and link to scenario management tool (CRA; AHRA; HR Emergency RA; NRP; RRAP; DHS Northern Border and Arctic) • Include flow diagrams to illustrate general and specific RA processes (i.e., risk; threat / hazard, vulnerability; criticality; resilience; etc.) • Compare objectives defined in multiple documents on multiple levels to be able to map evidence to objectives including: S&T challenges; strategic objectives (SPG); operational and S&T gaps; intermediate and long-term outcomes (logic model); priorities (Narratives) • Confirm partners' risk assessment approaches and identify most current assessment (unclassified) – review consistency and opportunities for alignment (start with SRA Report list (Appendix B) • Inventory if DHS CBP and related scenarios, RA processes; and open source RA information • Watch list of international, pubic and not-for-profit risk resources (e.g., WEF, OECD, FATF, WB, think tanks; newsletters; web sites; academic studies – PS has a master list for CA academia • Scenario planning framework, process and user guide (operational and risk scenarios) • Consolidate references (contained in multiple reports), websites (open source, priority to CA partners; US DHS; European Community; 5 Eyes partners), acronyms and terminology from the Risk Scan, Risk Assessment Framework Comprehensive Scan, SRA Literature Scan, and other project references summarized in this report • Define data collection process, plan, decision criteria and priorities to support evidence-based decision making • Confirm status, as-is linkage to existing projects, and future direction for CSS capabilities in operation research, decision support, and modeling and simulation (e.g., define minimum in-house core capability, augmented by trusted academics and contractors) • Extend Evidence-Based Assessment to include other factors, not just risk (e.g., investment history) • Compare Focus Area and CSSP performance measurement (performance and risk indicators) • Compare to capability-based planning (e.g., Canadian Core Capabilities lists); and identify process, decision criteria and priorities to fill gaps in near (1-3 years), mid 3-5 years), and long term (> 5 years) • Identify DHS S&T objectives, decision criteria and priorities • Identify CIPABS decision criteria, plans and priorities • Identify other GC priorities - sources of information that influence CSS decision making in near, mid and/or

Way Forward	Discussion of Options
	long term (e.g., RRAP; CIP; DRR; NRP; EMF; major events)
Design Questions	
Q1 Enterprise Architecture	• Does CSS plan to implement EA (e.g., QW) at the enterprise / program level? • If yes, then Option A and/or B • Scoping questions: o Is DRDC implementing QW? And other tools? Interoperability requirements? o What partners are using the same or similar approaches (e.g., CBSA has QW)? o What is CSS total cost of ownership and resource commitment? o Document expectations and training needs analysis o Track performance and end user feedback (actionable advice)
Q2 Capability Assessment	• Does CSS want to link capability-based assessment to risk assessment as two inputs to decision making? • If yes, then Option C to streamline and test concept • Scoping questions: o Status of CA and US Core Capabilities Lists; criteria, history; trends; and how is risk used in assessment process o Performance measurement (indicators)
Q3 Policy	• What is strategy to track distribution of investments? o For example; policy decision to allocate a % of budget to counter-terrorism (e.g., CBRNE); a % to other security and safety portfolios; and a % to internal / S&T capability building o Alternatively, define approach for trend analysis o Define risk tolerance levels o Clarify what is meant by evidence-based distribution of investments

Way Forward	Discussion of Options
Expected Benefits	• User-friendly; intuitive; and easy to maintain and update • Clarify evidence base • Guide data collection plan and analysis • Guide requirements definition for future collaboration environment • Interoperability with other tools • Operational and risk scenario planning / management processes • Inventory of strategic / complex risk scenarios • Inventory of existing specific threat / hazard scenarios (i.e., AHRA, CRA, HP Emergency RA)