

Risk scan:

A review of risk assessment capability and maturity within the Canadian Safety and Security Program

Ian Bayne
Ian R. Bayne & Associates
Orleans, Ontario, Canada

Shaye K. Friesen
Risk Assessment Analyst
Centre for Security Science

Defence Research and Development Canada

Scientific Report
DRDC-RDDC-2014-R36
June 2014

- © Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2014
- © Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2014

Abstract

The Canadian Safety and Security Program (CSSP) management framework, with respect to governance, collaboration, project selection, financial management and accountability, policy and planning, and the evolving public safety and security environment is more dynamic than ever. The need to focus on improving the quality, timeliness and value of risk information has never been greater. CSSP Strategic Planning Guidance (2013) states the requirement to compile a compendium of risk assessment techniques with a view to building a consolidated, cross-domain capability-based perspective.

The study considered risk assessment capabilities on the operational and program levels. The streamlined methodology included interviews and literature review, including international standards and best practices. Risk Assessment Capability Profiles were developed for operational areas and for the program. A capability maturity model technique and a preliminary SWOT analysis highlight quick wins for process improvement in the near-term.

The study found that there is limited visibility of risk assessment and other decision support techniques that are being used by external organizations to prioritize requirements, and there is no internal systematic approach to communicate risk across communities and at the program level. For the most part, risk assessment is an ad hoc process, and there are missed opportunities to contribute to the program's strategic outcomes, value and evidence base.

Significance to defence and security

It is debatable whether the current approach to defining the CSSP value, risk posture and capability, if retained, would be able to adapt and function effectively in the future, as the program faces a vast array of challenges in the public safety and security environment, which will increasingly require the systematic prioritization and collaborative treatment of high-risk, high consequence situations.

A new risk assessment framework for CSS might need to be built, identifying critical risk assessment elements for each Portfolio and gaps in tools/methods including those being used by other organizations. Until such work is complete and validated, it is premature to assume the same deficiencies apply across the board (i.e., no "one size fits all" formula). The capacity of the existing risk assessment and operations research sections, combined with the broad array of capability domains and the challenges working within the federal mandate-centric construct, represent potential limits to success.

Résumé

En ce qui concerne la gouvernance, la collaboration, la sélection de projets, la gestion financière et l'imputabilité, les politiques et la planification, ainsi que l'environnement changeant de la sécurité publique, le cadre de gestion du Programme canadien pour la sûreté et la sécurité (PCSS) est plus dynamique que jamais. Le besoin de mettre l'accent sur l'amélioration de la qualité, le respect des échéances et la valeur des renseignements sur les risques n'a jamais été aussi grand. Le guide de planification stratégique du PCSS (2013) énonce le besoin de constituer un recueil de techniques d'évaluation des risques dans le but d'élaborer une perspective inter domaines intégrée et fondée sur les capacités.

L'étude a tenu compte des capacités d'évaluation des risques au niveau des opérations et du programme. La méthodologie simplifiée comportait des entrevues et une revue de la littérature, notamment des normes et des pratiques exemplaires internationales. Des profils capacitaires d'évaluation des risques ont été élaborés dans les secteurs des opérations et du programme. Une technique du modèle de stabilisation des capacités et une analyse préliminaire des forces, faiblesses, possibilités et menaces (FFPM) mettent en évidence des mesures à effet rapide pour l'amélioration du processus à court terme.

L'étude a permis de constater qu'il existe peu de renseignements sur l'évaluation des risques et les techniques d'aide à la prise de décision utilisées par les organisations externes pour établir les priorités en matière d'exigences, et qu'il n'y a pas d'approche systématique interne pour faire part des risques dans les communautés et au niveau du programme. Dans la plupart des cas, l'évaluation des risques est un processus ponctuel, ce qui fait qu'on rate des occasions de contribuer aux résultats stratégiques, à la valeur et aux données probantes du programme.

Importance pour la défense et la sécurité

On est en droit de se demander si l'approche actuelle visant à définir la valeur, la position de risque et la capacité du PCSS, une fois retenue, pourrait s'adapter et fonctionner efficacement à l'avenir, étant donné que le programme se heurte à un large éventail d'obstacles liés à l'environnement de la sécurité publique. Cela nécessitera de plus en plus l'établissement systématique de priorités et un traitement axé sur la collaboration pour ce qui est des situations lourdes de conséquences et à haut risque.

Il pourrait être nécessaire d'élaborer un nouveau cadre d'évaluation des risques pour le PCSS qui établirait les éléments critiques d'évaluation des risques pour chaque portefeuille et les lacunes des outils et méthodes, notamment ceux utilisés par d'autres organisations. Jusqu'à ce que ces activités soient terminées et validées, il est encore trop tôt pour supposer que les mêmes lacunes seront présentes de façon générale (c.-à-d. qu'il n'y a pas de formule universelle). La capacité des sections d'évaluation des risques et de la recherche opérationnelle, conjuguée au large éventail des domaines de capacité et aux défis que représente le concept fédéral centré sur le mandat, impose des limites potentielles à la réussite.

Table of contents

| | |
|--|-----|
| Abstract | i |
| Significance to defence and security | i |
| Résumé | ii |
| Importance pour la défense et la sécurité | ii |
| Table of contents | iii |
| List of figures | v |
| List of tables | vi |
| 1 Introduction..... | 1 |
| 1.1 Context | 1 |
| 1.2 Purpose | 1 |
| 1.3 Background..... | 2 |
| 1.4 Scope | 2 |
| 1.5 Limitations..... | 2 |
| 1.6 Assumptions | 2 |
| 1.7 Report structure | 3 |
| 2 Methodology | 4 |
| 2.1 Overview | 4 |
| 2.1.1 Types of risk assessment techniques (a framework)..... | 4 |
| 2.2 Use..... | 5 |
| 2.3 Inputs | 5 |
| 2.4 Process..... | 6 |
| 2.5 Outputs | 7 |
| 2.6 Strengths and limitations | 7 |
| 3 Findings..... | 8 |
| 3.1 General comments | 8 |
| 3.1.1 Variables | 8 |
| 3.1.2 Trends..... | 9 |
| 3.2 Risk assessment techniques | 9 |
| 3.2.1 Operational area techniques | 9 |
| 3.2.2 Operational area managers' insight..... | 11 |
| 3.2.2.1 Border & transportation security (maritime security) | 11 |
| 3.2.2.2 Cybersecurity | 11 |
| 3.2.2.3 Surveillance, Intelligence & Interdiction (SII)..... | 11 |
| 3.2.2.4 Critical Infrastructure Protection (CIP)..... | 11 |
| 3.2.2.5 Fire services..... | 12 |
| 3.2.2.6 Paramedic services | 12 |
| 3.2.2.7 Law enforcement services | 13 |

| | | |
|---------|---|----|
| 3.2.2.8 | Chemical, Biological, Radiological, Nuclear and Explosives, and Forensics (CBRNE/F) | 14 |
| 3.2.2.9 | Emergency Management Systems Interoperability (EMSI) & Psychosocial | 14 |
| 3.2.3 | Program risk governance..... | 14 |
| 3.2.3.1 | Program-level techniques | 15 |
| 3.2.3.2 | Managers' insight..... | 15 |
| 3.3 | Capability maturity | 16 |
| 3.4 | SWOT analysis..... | 17 |
| 3.5 | Challenges | 18 |
| 4 | Conclusions..... | 19 |
| | References | 21 |
| Annex A | Observations..... | 23 |
| Annex B | Compendium of risk assessment techniques | 25 |
| Annex C | Capability maturity model assessment | 29 |
| C.1 | Summary of risk assessment capability and maturity for operational areas..... | 33 |
| Annex D | Participants | 35 |
| Annex E | Communiqué | 37 |
| Annex F | Interview framework | 39 |
| Annex G | Risk assessment capability profiles | 41 |
| G.1 | Risk assessment capability profile – Border & transportation security..... | 41 |
| G.2 | Capability profile – BTS and Critical Infrastructure Resilience (BCIR)..... | 45 |
| G.3 | Risk assessment capability profile – e-Security | 49 |
| G.4 | Risk assessment capability profile – Surveillance, intelligence & interdiction..... | 54 |
| G.5 | RA capability profile – Critical Infrastructure Protection (CIP) | 57 |
| G.6 | Risk assessment capability profile – Fire service | 61 |
| G.7 | RA capability profile – Paramedics..... | 64 |
| G.8 | RA capability profile – Law enforcement | 68 |
| G.9 | Risk assessment capability profile – CBRNE Forensics (CBRNEF)..... | 72 |
| G.10 | RA capability profile – EMSI and psychosocial | 76 |
| G.11 | RA capability profile – Knowledge, technology & community safety | 79 |
| G.12 | RA capability profile – CSSP program support | 83 |
| Annex H | Capability Maturity Model frameworks | 87 |
| H.1 | CMM background and concept | 87 |
| H.2 | Risk scan approach..... | 88 |
| H.3 | Frameworks | 89 |
| Annex I | Affinity diagrams..... | 91 |
| Annex J | Concept of operations..... | 93 |
| | List of symbols/abbreviations/acronyms/initialisms | 95 |

List of figures

| | |
|--|----|
| Figure 1: Risk assessment components (system of systems view)..... | 17 |
| Figure 2: Preliminary SWOT analysis..... | 18 |

List of tables

| | |
|---|----|
| Table 1: Examples of risk assessment techniques (ISO 31010:2009)..... | 4 |
| Table 2: Operational area techniques & potential implications (next steps)..... | 10 |
| Table 3: Program techniques..... | 15 |

1 Introduction

1.1 Context

The Canadian Security and Safety Program (CSSP) is evolving, which includes managing more Communities of Practice (CoP) and portfolios, expanding participation in existing communities; and investigating new areas where Science and Technology (S&T) can improve Canada's overall safety and security posture, including at the community safety and resilience level. As stated in the Strategic Planning Guidance, "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. In order to deliver on its mandated program, these capabilities will be of fundamental importance to DRDC CSS in the next planning period."¹ Given that risk information contributes, implicitly or explicitly to decision making across the program at varying degrees of maturity, it was decided to perform a quick scan of the state of existing risk assessment practices within the communities and the program.

The Security and Prosperity Partnership of North America lasted for four years (2005-2009). Since then, the Government of Canada (GC) has focused on specific issues by developing national and international strategies and action plans. Departments and agencies develop plans based on their mandates and risk perception. With the exception of the federal All Hazards Risk Assessment (AHRA) Interdepartmental Risk Assessment Working Group (IRAWG) and its activities, federal mandate- and domain-specific threat evaluation, hazard analysis and risk assessment techniques exploiting a variety of methodologies and techniques continue to evolve within their respective specialist domains. Additionally, there currently is no National Security (and/or Safety) Strategy, and no strategic planning assumptions and planning goals. In this environment, CSSP faces several challenges, including identifying projects that balance national and regional perspectives, and optimizing program investments in safety and security over time. The strategic planning process considers these, sometimes competing, objectives.

Virtually all GC and departmental initiatives refer to using risk-based approaches (RBA), which implies that risk assessment is an integral part of decision making. However, there is a potential gap between theory and practice. Many organizations have not explicitly defined how they implement these RBA or how they engage stakeholders in the process.

1.2 Purpose

With this as a backdrop, the risk scan project was conceived to identify existing risk assessment processes, tools and techniques being used within the portfolios, and to investigate a capability maturity model as a technique to highlight opportunities to improve risk assessment as whole at the community (operational capability) level and risk governance at the program level.

¹ Canadian Safety and Security Program (CSSP), Strategic Planning Guidance (SPG) for 2013/14, p. 11.

1.3 Background

CSSP Strategic Planning Guidance (SPG) states the requirement to compile a CSSP risk compendium, which will identify the risk assessment methods and results across the safety and security communities of practice and portfolios, with a view to building a consolidated, cross-domain risk profile, including identified capability targets. The Risk Assessment and Capability Integration (RACI) Section conducted a scan of risk assessment techniques with a view to providing a baseline compendium, as the first part of the strategic objective. The study also identified some trends and lessons that could be shared across communities. The project did not address the cross-domain risk profile requirement because there was insufficient knowledge of bottom-up processes. However, it did develop a risk Capability Maturity Model (CMM) profile that represents a composite snapshot of risk assessment capability and maturity (Section 3.3) and individual assessments for operational areas.

1.4 Scope

The risk scan considered risk assessment capability and maturity on two levels: how CoP and portfolio stakeholders use and communicate risk information as part of the requirements analysis and prioritization process; and secondly, how CoP and Portfolio Managers (PortMans) use risk information to position their project priorities within the overall CSSP. This report does not reiterate systemic constraints that were highlighted in the Decision Support Section Analysis report, which should be considered in evaluating any follow-up action as a result of this study.²

As the scope, scale, and value of business operations have evolved, our specializations to manage the risk have similarly evolved, but in doing so each specialization has developed its own view of risk and how to describe its components. This has resulted in a significant language gap between the different specializations, all of whom are stakeholders in managing risk.

(The Risk Language Gap, TOG, 2013:50)

1.5 Limitations

Limitations for the risk scan project included: lack of detailed information on how external organizations assess and prioritize risk; lack of common guidelines on internal program risk management; and the availability of up to date information on the SharePoint Partners Collaboration site.

1.6 Assumptions

CSS is managing significant change, and the demand for risk assessment services externally and internally will remain the same or increase. Therefore, a baseline of risk assessment techniques and a demonstration of a capability maturity model assessment should support future work on

² See Decision Support Section Analysis of the June 14, 2013 CoP Summit; DRDC-CSS, 2013.

multiple levels. Moreover, the assessments are subjective and based on best judgment. The assessments are not a report card on risk assessment practices. The CMM assessments are relative to other CSS communities at the time. The colour coding might be interpreted as arbitrary, and is not an indication of risk. That is, level one or two may be acceptable levels of capability and/or maturity, depending on the operating environment and constraints.

1.7 Report structure

The front-end of this report focuses on the approach and findings. It highlights emerging trends, managers' insights and observations for future consideration. The annexes include a summary of observations and deductions, a compendium of risk assessment techniques and CMM assessments for nine operational areas and program risk governance. The annexes also contain supporting material, including: the list of interview participants, communiqué; interview framework; the profiles (record of interviews); a worksheet that consolidates interview findings; diagrammatic tools; and a hypothetical concept of operations as a potential input for a program value assessment framework.

- Annex A: General observations
- Annex B: Compendium of risk assessment techniques
- Annex C: Capability maturity model assessment
- Annex D: Participants
- Annex E: Communiqué
- Annex F: Interview framework
- Annex G: Risk assessment capability profiles
- Annex H: Capability maturity model frameworks
- Annex I: Affinity diagrams
- Annex J: Concept of operations

2 Methodology

2.1 Overview

The methodology for the risk scan included: advance communications with participants; reviewing material from the CoP Summit (2013); reviewing community-specific material that was available on SharePoint; literature review of capability maturity model best practices; interviews with CSS staff including Section Heads, and representative CoP leaders and Portfolio Managers; and iterative development of deliverables. Brainstorm sessions to validate findings and illicit further ideas on the use of risk assessment techniques were retained as follow-on activities.

The structure below adopts the ISO 31010 Risk assessment techniques standard³ format for describing techniques, recognizing that communities use a variety of assessment techniques, and most federal departments and CSS staff are probably not familiar with the international / Canadian standard. The standard, which is being updated, provides a useful framework for identifying generally-accepted management techniques that are being used by a broad cross-section of organizations that are stakeholders in Canada's safety and security posture.

2.1.1 Types of risk assessment techniques (a framework)

Types of risk assessment techniques and examples from ISO 31010 that are being used or are likely relevant to CSSP operational areas are provided below to illustrate the variety of potential techniques. The techniques cited are described in the standard along with their relevance and whether they support quantitative outputs. This construct could be a useful model for future iterations of a compendium that extends beyond this baseline assessment. It is likely not practical to develop such a broad compendium at a national level, but it should be more useful at the local and regional level to highlight domain gaps and best practices across cooperating organizations.

Table 1: Examples of risk assessment techniques (ISO 31010:2009).

| Types of risk assessment techniques | Representative techniques |
|-------------------------------------|--|
| Look-up methods | • Checklists |
| Supporting methods | • Preliminary hazard analysis |
| | • Structured interview and brainstorming |
| | • Delphi technique |
| | • SWIFT Structured “what-if” |
| | • Human Reliability Analysis (HRA) |
| Scenario analysis | • Root cause analysis (single loss analysis) |
| | • Scenario analysis |
| | • Toxicological risk assessment |
| | • Business impact analysis |
| | • Fault tree analysis |

³ CAN/CSA-IEC/ISO 31010:2009, Risk management – Risk assessment techniques.

| Types of risk assessment techniques | Representative techniques |
|-------------------------------------|---|
| Function analysis | <ul style="list-style-type: none"> • Event tree analysis • Cause / consequence analysis • Cause and effect analysis • Failure Mode and Effects Analysis (FMEA) • Hazard and operability (HAZOP) studies • Hazard Analysis and Critical Control Points (HACCP) |
| Controls assessment | <ul style="list-style-type: none"> • Layers of Protection Analysis (LOPA) • Bow tie analysis |
| Statistical methods | <ul style="list-style-type: none"> • Monte Carlo analysis • Bayesian analysis |

2.2 Use

The initial list of techniques (Annex B) can be used as a start point for community managers to document techniques that are used on specific projects or throughout the program. This requirement could be part of the Call process or a project documentation requirement. An option is to do a survey of stakeholder organizations, which could be used to identify disconnects, gaps and/or best practices in assessment techniques, but this would be a time-consuming exercise.

2.3 Inputs

Inputs to this study included: interviews; review of material on the DRDC Partners' SharePoint site and provided by participants after the interviews; review of relevant GC strategies and action plans; and knowledge of generally-accepted practices for threat evaluation, operational risk assessment, portfolio/program/project risk management, capability maturity model assessment and operational resilience.

The Carnegie Mellon University, Software Engineering Institute (CMU, SEI) Cyber Emergency Response Team (CERT) Resilience Management Model (CERT-RMM) was used as the framework for this project. CERT-RMM “is a capability-focused maturity model for process improvement that comprehensively reflects best practices from industry and government for managing operational resilience across the disciplines of security management, business continuity management, and IT operations management.”⁴

The study considered two dimensions: capability dimension, which describes the degree to which a process has been institutionalized; and maturity dimension, to define levels of organizational maturity that are achieved through raising the capability of a set of process areas in a manner described in the model.

⁴ Carelli, R. et al (2011), CERT-RMM, a maturity model for managing operational resilience (2011), p. xvii.

Resources that were not available to CSS at the time of this study were:

- Responses to Public Safety (PS) survey on critical infrastructure programs, which should include some mention of risk assessment techniques (requested by CSS);
- Virtual Risk Assessment Cell (VRAC) terms of reference and techniques being used in support of Government Operations Centre (GOC) and departments;
- PS specific tools on the Critical Infrastructure web site and/or that are being developed under the Canadian Regional Resilience Assessment Program (RRAP); and
- Tools from the Department of Homeland Security (DHS) RRAP grants program that are being evaluated or used by PS and P/T organizations engaged in cross-border projects.

2.4 Process

An interview framework was provided to participants in advance (Part 2, Annex B). CSS selected participants to provide broad coverage of the program at the section, portfolio and community levels. The study used an informal interview process to capture information on: the context (i.e., environment; ongoing initiatives; priorities with a two-year horizon; constraints; stakeholders; etc.); risk assessment techniques used by stakeholders to identify and prioritize their risks, if known; and informal or formal risk assessment techniques used by CSS staff to communicate priorities within the overall program.

To develop a compendium of risk assessment techniques, the risk scan considered nine operational domains and two strategic (management) domains, as follows:

Safety and Security Operational domains:

- Border and Transportation Security (includes maritime security);
- Cybersecurity;
- Surveillance, Intelligence & Interdiction;
- Critical Infrastructure Protection;
- Fire;
- Paramedics;
- Law Enforcement;
- CBRNE⁵ and Forensics; and
- Emergency Management Systems Integration and Psychosocial.

Strategic (management) domains:

- Knowledge, Technology & Community Safety; and
- Program decision support.

⁵ Chemical, Biological, Radiological, Nuclear and Explosives.

To develop a CMM, the risk scan approach focused on five components of a risk assessment capability including:

- People (e.g., governance; experience; complexity; knowledge; continuity; training);
- Process (e.g., governance; documented, systematic and verifiable assessment techniques);
- Technology (e.g., risk assessment, IM, decision support and collaboration tools);
- Information (e.g., easy access to relevant resources including classified and open source; information sharing infrastructure); and
- Relationships (e.g., human-controlled networks; access to SMEs; formal agreements).

2.5 Outputs

The main deliverables are the two-part report and a PowerPoint presentation. General observations and deductions are included as Annex A. The intent is to use these observations as a framework for follow-on group discussions.

2.6 Strengths and limitations

The strength of the approach was mainly that participants could speak frankly about risk assessment techniques within their areas of responsibility, and the potential role for risk information to support program decision making. A limitation was that some subject matter experts (SMEs) did not participate in the interview process. In particular, managers of discrete Chemical / Biological, Radiological / Nuclear, Explosives, Forensics and Psychosocial CoPs, and the Decision Support Section were not interviewed,⁶ although the later did participate in a brainstorming exercise prior to the commencement of the interviews. To overcome this limitation, profiles captured the perspectives of the section heads and staff with experience in these areas.

The level of independent verification and validation of Federal/Provincial/Territorial (F/P/T), partners' or other's tools; access to analytical or S&T resources by organizations doing the assessments; and the level of engagement of non-SMEs and external stakeholders in the assessment processes were not considered during this project. However, for future iterations, these aspects should be reviewed in order to obtain a more complete picture of capability and maturity. To avoid a costly independent study, this information could be obtained over time by making it a requirement of the CSSP Call process or specifying it as a project deliverable requirement.

⁶ Each individual CBRNE-f Portfolio Manager was not interviewed due to time and budgetary constraints. At the time of the project, there were also multiple vacancies within the section (i.e., there was no Portfolio Manager for Biology or Rad/Nuke). Additionally, it was felt that the CBRNE Consolidated Risk Assessment provided adequate description of the portfolio risk processes and techniques, such that further interviews beyond the section head level were not required.

3 Findings

3.1 General comments

A variety of risk assessment techniques are used within the CSSP operational areas. In most cases, CSS has no direct role and responsibility in reviewing threat and risk assessment techniques that are developed at the departmental, operational and/or tactical levels. However, CSS staffs indirectly add value to the prioritization of risks through the CSSP Call process and in interactions with their respective networks. A strength of CSS is the depth and breadth of knowledge of the safety and security operational decision making environment at the national, regional and local levels. General observations and deductions are included at Annex A.

3.1.1 Variables

Techniques that consider the following variables either individually or in combination with other variables were considered in scope, even if CSS had no direct involvement in the process:

- Threat;
- Hazard;
- Vulnerability;
- Impact / consequence / cascading effects / loss;
- Harm analysis;
- All hazards;
- Criticality;
- Interdependency and systemic risk;
- Resiliency;
- Uncertainty (likelihood), frequency, probability; and
- Risk (tactical, operational, strategic).

The study also considered strategic and program risk assessment techniques, referred to as risk governance below. This initial risk scan did not consider engineering, quality assurance, audit and control assessments, or other specialist or general management techniques,⁷ such as SWOT, gap analysis and root cause analysis. It also did not consider specific decision support or operations research techniques, with the exception of the Delphi Method, which was recommended as a CSSP-wide core technique.

⁷ ISO 31010 Risk assessment techniques, identifies 31 techniques that are used to support decision making.

3.1.2 Trends

The interview process indicated that there are several emerging trends where risk information should play a role including:

- Need for a framework to describe the value of CSSP investments;
- Need for an evidence base for the program (e.g., prepare for an external audit and to support strategic relationship management with partners and supported organizations);
- Relatively urgent need for an evidence base for specific communities, in particular Fire and Paramedics; and
- More attention is being paid to understanding the “target and effects” including the consequences for vulnerable populations and society, which means that new terminology is emerging, which should be documented and standardized.

3.2 Risk assessment techniques

Techniques can be considered in two categories: those that CSS controls or supports, and external techniques, where CSS has no direct role, unless requested by the partner. Examples of the former include: the Consolidated Risk Assessment (CRA), the AHRA Framework and the Capability-Based Planning and Capability Assessment Methodology solutions. Examples of external techniques include those used by: individual federal departments; other levels of government including municipalities; and critical infrastructure asset owners.

Whereas in the past, CSS focused primarily on the assessments of threats, vulnerabilities and to a lesser extent impact, the focus is evolving to include more awareness of targets and effects, often using specific risk event scenarios to add clarity. Emerging techniques, such as dependency, risk and loss modelling are opportunities to engage a broader stakeholder base and gain greater insight into the safety and security risks facing Canadian society.

The benefits of documenting and tracking the evolution of risk assessment techniques include:

- Identify cost-effective techniques (easy to use; adaptable; verifiable; sustainable);
- Identify risk terminology that should be standardized (e.g., CSSP risk glossary)⁸;
- Identify solutions that CSS controls to assess value, scalability and potential for reuse;
- Identify techniques that CSS does not control to highlight risks (e.g., incorrect math; double accounting of impacts; lack of traceability and rigor); and
- Identify opportunities to describe program outcomes and strategic value in qualitative and quantitative risk management terms.

3.2.1 Operational area techniques

Although CSS SMEs do not participate directly, and in most cases, have little or no visibility into techniques being used at the operational level, there are opportunities to indirectly add value to

⁸ PS probably does not have the breadth of experience or focus to develop such a “national” glossary.

the process as priorities emerge. Communities are prioritizing their gaps and solutions using a variety of informal and formal techniques. In most cases, it is not clear how risk information is being used. More in-depth analysis would be needed to add more granularity to the techniques being used by external organizations.

The advantage of the existing bottom-up approach is that the people closest to the risk are the ones who identify the priorities. The disadvantage is that people are using a variety of techniques that are difficult to validate or compare. The fragmented and overlapping nature of federal mandates, jurisdictions and critical infrastructure sectors also mean that some risk assessment processes may have flaws that are not being discovered as the priorities make their way to CSSP.

Annex B establishes a baseline of risk-based approaches and risk assessment techniques that are being used or are emerging within communities, as of Spring 2014. With this start point in mind, managers could be tasked to review and update the baseline on a regular basis as part of the normal planning process. Managers are in the best position to determine if they require more visibility into the risk assessment and prioritization processes being used by departments and partners. Examples of techniques from the compendium at Annex A are highlighted in the table below based on the following criteria to assess relevance to a capability maturity model, and potential impact on the RACI and/or Decision Support sections:

- Clarifies the role of risk information in the decision making process at the community (operational, tactical) and program (strategic) levels;
- Enriches the understanding of risk variables including stakeholders’ risk perception;
- Clarifies how risk mitigation could contribute to the CSSP value proposition; and
- Facilitates a broader coverage of risks including interdependency and systemic risks.

Table 2: Operational area techniques & potential implications (next steps).

| Relevant techniques | Potential implications |
|--|--|
| <p>CSS-controlled / managed</p> <ul style="list-style-type: none"> • Consolidated Risk Assessment • AHRA and hazard/threat-specific scenarios • Capability-Based Planning • Dependency, risk & loss modeling • Factor-based analysis... • Expert Choice voting technology • RiskOutlook • Simulation and lab tools (e.g., HAZUS; @risk) | <ul style="list-style-type: none"> • Review adaptability & sustainability • Centrally manage scenarios & integrate AHRA with capability assessment methodology • Review lessons from regional CBP projects • Reuse loss data for AHRA socio-economic impact scales • Review requirement for CSS risk glossary & toolkit • Review effectiveness and sustainability • Review effectiveness and sustainability • Review RACI section and CSS capacity to exploit tools and sustain knowledge base |
| <p>Not CSS controlled / managed</p> <ul style="list-style-type: none"> • Regional Hazard, Identification & Risk Assessment (P/T/Municipality) • Regional Resilience Assessment Program (RRAP) – Critical Infrastructure (CI) site assessments; national and sector risk profiles; risk tools (PS) | <ul style="list-style-type: none"> • Identify options for independent validation of P/T/local risk assessment techniques and tools (spreadsheet reliability) • Review RRAP objectives – confirm options for direct or indirect support to PS and partners; review DHS CI techniques and tools (e.g., relevance & sustainability) |

3.2.2 Operational area managers' insight

This section presents the consultant's interpretation of what he heard during the interview process. Although the comments are grouped by operational area, the comments were selected based on capturing insight into the broader capability, community, program and risk management environment. This step in the methodology involved circling back to the profiles that were captured over a five-month timeframe, recognizing that the environment is dynamic and some thoughts may have changed in the interim. The comments were extracted from the interview profiles (Part 2, Annex D, Question 3.a). The question was: *describe how the domain prioritizes risks and presents recommendations to the next level* (comments in italics and in brackets). Caveat: summaries have not been validated by CSS staff.

3.2.2.1 Border & transportation security (maritime security)

Priorities are developed by using a bottom-up approach and through the Call process. The CSS OPI consults with a small group of SMEs to validate new ideas and gain insight into community priorities. In this way, CSS can anticipate requirements and potentially, influence prioritization choices.

3.2.2.2 Cybersecurity

The CoP is using a risk-based approach to prioritize the partnerships. Energy (SCADA vulnerability) was chosen as the first priority to improve collaboration between GC (law enforcement and others), the provinces/territories (P/T) that are responsible for energy security, and the private sector.

3.2.2.3 Surveillance, Intelligence & Interdiction (SII)

Examples of risks for projects in this domain include: projects are not fully-funded; the requirement changes before the solution can be implemented; and the sustainment costs exceed estimates. Should CSSP not be able to contribute, then the operational departments would have the option and budgets to find alternative solutions.

3.2.2.4 Critical Infrastructure Protection (CIP)

Risk is not an explicit part of the decision making process, above the departmental / stakeholder level. The assumption is that organizations are making threat-based decisions based on: accurate intelligence; projections of threat and technology trends; departmental plans; GC and regional priorities; and international commitments and compliance requirements. There is no common view of the risk modeling capability across departments or other levels of government including economic and interdependency modeling.

At the Federal level, PS promotes the application of all hazards risk management. However, at the P/T level, public and private stakeholders use a variety of techniques and tools. CI sectors use their own toolsets, and there is no overall view of the compatibility of the diverse processes. CSS is currently in a fact finding and monitoring role, except for a few projects and Targeted Investments (TI's).

A Virtual Risk Assessment Cell (VRAC) was created to support Government Operations Centre (GOC). It may also be supporting CI sector risk assessments.

(DHS) RRAP is building a database of site assessments within the Department of Homeland Security (DHS) Regional Resilience Assessment Program (RRAP). PS may be doing the same thing within its corresponding initiative.

Various techniques include:

- Threat and Hazard Identification and Risk Assessment (THIRA) – DHS RRAP term;
- Hazard Identification and Risk Assessment (HIRA) – ON term;
- Vulnerability assessment;
- Criticality assessment;
- Resiliency assessment; and
- Dependency assessment.

3.2.2.5 Fire services

At the provincial level, coordination is slightly better with the introduction of HAZMAT regional teams (e.g., Atlantic/New England/Maine sharing of resources for HAZMAT preparedness and response). Beyond that, there exists little to no coordination of equipment or response among the multiple jurisdictions. However, there are individual Mutual Aid Agreements between services and departments (e.g., dispatching services), but nothing comprehensive exists on a national scale.

The level of resources devoted to performing a separate risk analysis/risk assessment is a function of the size of the community involved. Smaller fire services do not have a lot of resources available to perform risk assessments, and the capabilities that are acquired may not be based on a valid need or functional requirement.

A better approach to risk assessment is needed in order to be able to validate requirements versus focusing on an equipment replacement strategy.

3.2.2.6 Paramedic services

This new community has established an information baseline to support future work, which includes:

- CoP map of priorities;
- Reliance on evidence-based decision making (risk management not explicit in prioritization process – potential blind spots?); and
- Priorities based on solid body of work that engage associations and frontline resources.

Capability and risk analysis are implicit in the process, which means that some risks could be missed (i.e., not a rigorous or transparent process).

3.2.2.7 Law enforcement services

The community is using a risk assessment template, version 22 (CSS, 2013), which is posted on PS web site. The CoP has included (*socio-economic impact*) loss analysis in projects since 2012, recognizing that the impact of security incidents is not just loss of life or property. It is also about the impact on the economic well-being of communities. The CoP usually gets economic modeling and analysis expertise from Finance Canada or by contracting with regional SMEs.

Spreadsheet tools are used to investigate multiple factors. The assessments are factor-based, not just threat- or risk-based assessments. The projects have experimented with voting technology.

Factors include: threat; target; people; investors. The technique builds on early RACI and OR work (e.g., Goudreau, A., and Verga, S., 2009-10).

Sample project – Delphi approach / Factor-based voting:

- Lower mainland BC project;
- 2 sessions;
- 60 participants;
- Vote on factors (not risks);
- Discussion; and
- Vote again (repeat as necessary).

Multi-dimensional assessment process:

- Threat-based analysis;
- Target-based analysis;
- Cascade effects analysis; and link to
- Enterprise Risk Management – working with City level SMEs.

Other case studies:

- Ottawa – link to strategic / City planning – trade-offs between purchase of police equipment versus spending money to increase tourism;
- Ottawa – infrastructure decision that disrupted 4-lane highway – quantification of cost impact;
- Richmond – decision to transport fuel to airport (pipeline – road – rail); and
- Yukon – Ottawa working with Yukon on automated tool for risk analysis.

Real world examples of decision that increased risk to local communities and business include:

- Liquid Natural Gas (LNG) plant located near hospital. Decision makers focused on tax revenue and employment; and
- Smiths Falls – listeriosis outbreak elsewhere, but local decisions put 700 jobs and community economic survival at risk.

CoP used factor-based voting tool for Windsor-Detroit Gateway, trans-Canada railway and Great Lakes (GL) projects.

Success story – RCMP and US police on same boats in GL – significant improvement in enforcement capability.

3.2.2.8 Chemical, Biological, Radiological, Nuclear and Explosives, and Forensics (CBRNE/F)

Threat, hazard and vulnerability assessments are an integral part of the CBRNE/F capability and requirements prioritization process. The assessments are mainly the output of a bottom-up process that is performed by the SMEs in each knowledge area.

In the past, CSS has used the CRA process to combine threat assessments. However, the risk assessment environment has changed dramatically since the CBRNE Research and Technology Initiative (CRTI) timeframe. Historically, the focus was mainly on the terrorist threat, and understanding threats, hazards and vulnerabilities. The focus is now broader and includes infectious disease outbreaks and industrial accidents. The teams are spending more time on understanding the target and effects (e.g., consequence management and resiliency). This trend is consistent with transitioning to a more holistic view of risk exposure (*which suggests that the intelligence-based CRA may not be applicable or may need to be adapted, and there should be opportunities to consider other unifying approaches including risk visualization tools*).

3.2.2.9 Emergency Management Systems Interoperability (EMSI) & Psychosocial

EMSI leverages the annual symposium to do facilitated brainstorming on gaps and priorities. Risk is implicit in discussions. In 2012, CSS trialled an automated voting tool (*Expert Choice*), but it has not been exploited further in CSS. Historical examples include:

- Health Canada – EMSI observed an exercise that identified the top 10 gaps. Risk was not an explicit part of the process; and
- Detroit-Windsor Corridor (CIP) – a scoring technique was used a few years ago, but it has not been operationalized or exploited across CSS.

3.2.3 Program risk governance

There are currently no guidelines for risk assessment / management for the program. A systematic approach to risk assessment should add value by engaging managers throughout the program planning cycle to identify strategic, operational and capability risks. A structured risk-based approach would add value in other ways including: early identification of (operational) performance and risk indicators; verification of the expected value of investments to CSS, partners and stakeholders (e.g., risk mitigation); and identification of opportunities to leverage governance, risk management and compliance best practices within the Canadian, and international safety and security S&T community.

3.2.3.1 Program-level techniques

The table below highlights relevant techniques selected from the compendium (Annex B) and potential implications from a CMM improvement perspective.

Table 3: Program techniques.

| Relevant techniques | Potential implications |
|---|---|
| Program <ul style="list-style-type: none">• Value• Evidence• Risk governance | <ul style="list-style-type: none">• Measures of Effectiveness (MoEs) for (value of) risk mitigation• Integrated performance and risk indicators• Systematic approach to risk management on program, project and operational area / community levels (e.g., managers' guidebook; decision support toolkit) |

3.2.3.2 Managers' insight

3.2.3.2.1 Knowledge, technology & community safety

There are no structured or formal mechanisms to communicate risk internally (ad hoc process). This is a concern because of: rapid growth; increasing competition; shifting CSSP priorities; budgets constraints; etc.

Knowledge, technology & community safety and related CoP/portfolios face common risks both internally and within the overall CSSP direction. If risks are not considered during the development of strategic planning guidance, then there could be a missed opportunity to lay the groundwork for a more systematic approach to risk management.

Two trends are highlighted:

Trend 1: Risk information – More strategic focus, including on risk information.

Broader responder community is shifting focus from just threats, hazards and vulnerabilities to understanding impacts, consequences and risk exposure on multiple levels, not just their own discipline or mandate. Community recognizes imperative to communicate more effectively with stakeholders including: local politicians, councils, unions, associations, academia, private industry, training and certification establishments, cross-border partners and the public.

Trend 2: Impact – Responder cultures are recognizing need to focus more attention on impact dimension.

3.2.3.2.2 Program support / challenge function

There is no structured process for communicating risk information or for describing the value of investments in risk treatment terms. This could be a problem when the program is audited in 2016. That is, there is no evidence base to support program value to federal partners and stakeholders in other jurisdictions and in the private sector. (Note: A pre-audit is being planned

for 2015 with support from Chief of Review Services (CRS, DND), to prepare for the 2016 OAG audit).

Strategic planning guidance is the key forward-focused document, which includes a risk-based approach to guide investment and internal capability improvement decisions.

CSS developed its first Environmental Scan (FY2013/14). A challenge is communications and sustainment of the scan findings (e.g., *feedback, lessons learned, and possibly, incorporating risk trends and indicators into the scan*).

Recent experience with PSTP Call indicates that the priorities are broad and not linked to risk or areas of primary interest to CSSP. (Recent Call, FY 2013/14 – approximately, 30% of the proposals were of little or no interest to CSSP).

Communities, portfolios and sections prioritize projects mainly based on the expert judgment of those close to the risks. In some cases, this means that threat is still the dominant variable, as in the CRTI days, when the Consolidated Risk Assessment (CRA) process was developed.

Most proposals are focused on closing known capability gaps, and addressing existing threats and control deficiencies.

3.3 Capability maturity

Annex C presents a preliminary CMM snapshot of the relative risk assessment capability and maturity based on a comparative analysis of the capability profiles (Part 2, Annex E). A hypothetical model is presented below that focuses on the interdependent variables to highlight where ongoing work can be leveraged to improve the overall risk assessment capability.

The model suggests that emerging initiatives that focus on describing effects and dependencies should improve the overall risk assessment process maturity, and indirectly, increase the value of risk assessments on multiple levels, including at the program level.

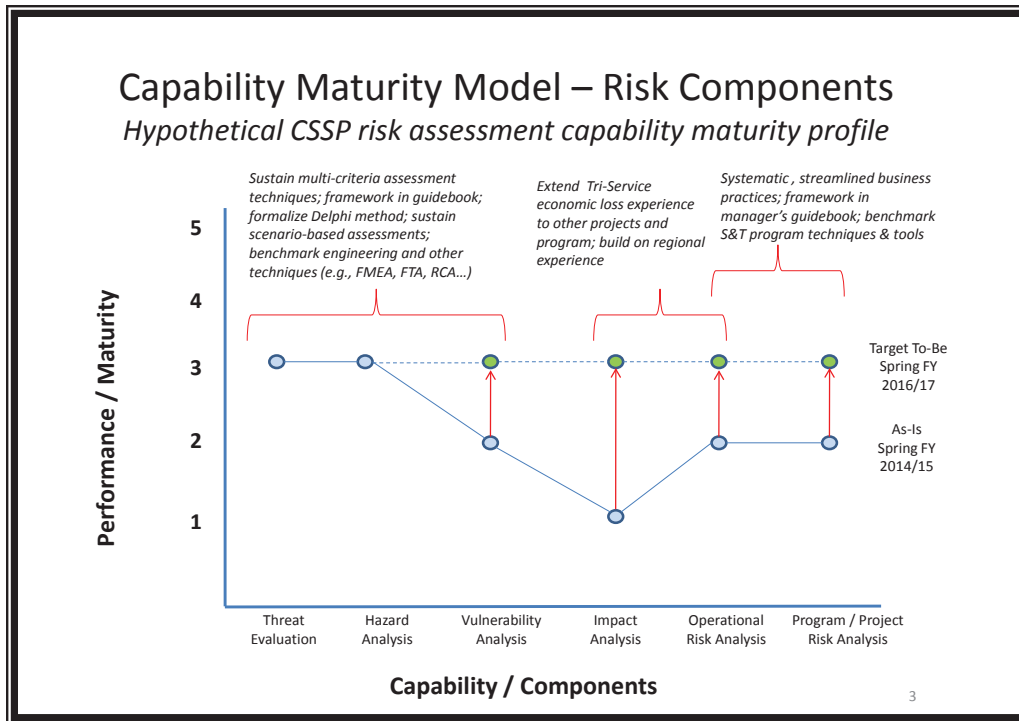


Figure 1: Risk assessment components (system of systems view).

3.4 SWOT analysis

A preliminary SWOT⁹ analysis provides a summary view of major observation from the risk scan interviews and follow-up discussions. It also illustrates another simple technique that is frequently used for as-is and to-be (gap) analysis.

⁹ Strengths, Weaknesses, Opportunities and Threats (Uncertainty) – subject summary of observations from risk scan interviews and follow-up discussions. Intent is to answer so-what? from CMM-based assessment.

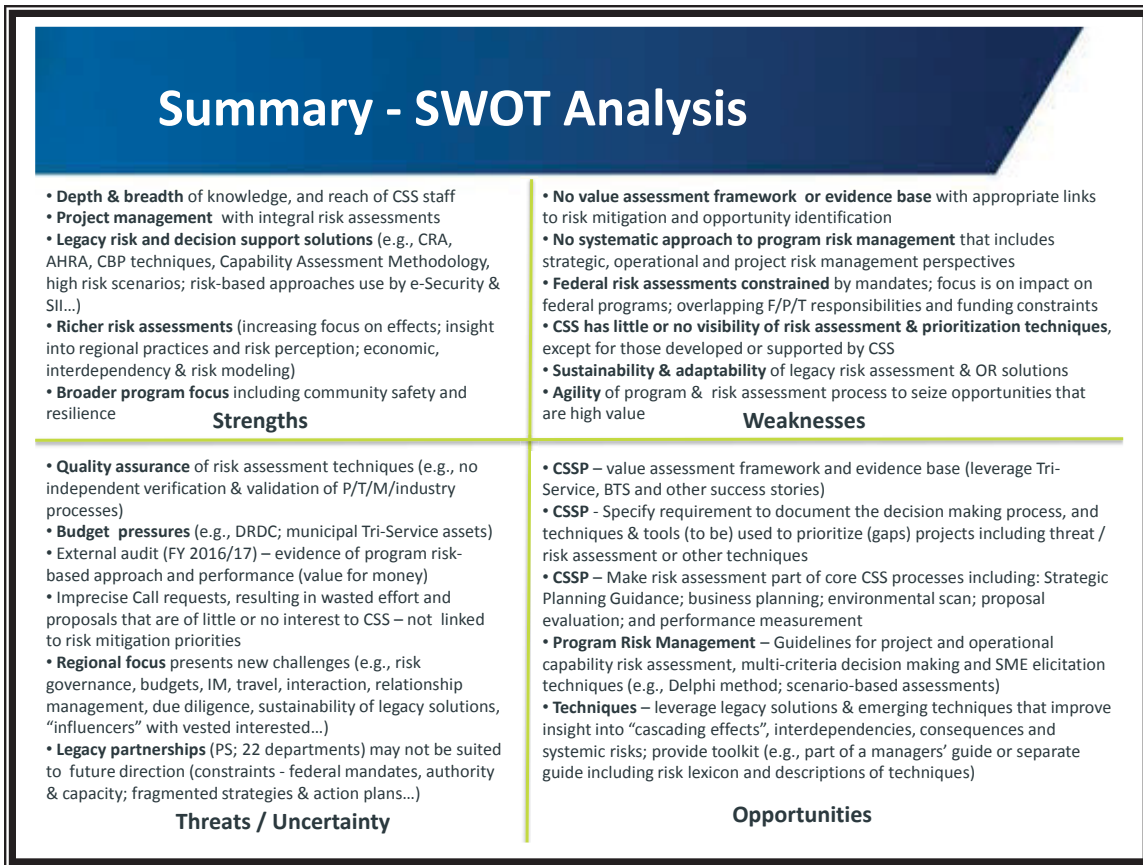


Figure 2: Preliminary SWOT analysis.

3.5 Challenges

Challenges for CSS include the capacity to: exploit legacy and emerging risk assessment and decision support techniques; implement a more systematic approach to risk assessment and risk governance; and implement process improvements without increasing the administrative burden for CoP and Portfolio Managers (i.e., take advantage of existing processes, and make risk assessment a more explicit and valuable part to decision making, internally and externally).

4 Conclusions

With the exception of communities that are using techniques that CSS developed or continues to support, CSS has limited visibility of techniques and tools that are used by federal partners, and virtually no insight into specific techniques being used by stakeholders, or the reliability and effectiveness of these techniques and tools. This report, the compendium and the CMM assessment should be considered as a baseline for an overall strategy to improve risk governance, and the value of risk information to decision making in support of the operational areas and at the strategic (national program) levels.

CSS has several foundational success stories including: Consolidated Risk Assessment (CRA) and criticality assessment work in support of security operations and counter-terrorism (e.g., 2010 Olympics, G8, G20); all hazard risk assessment framework and scenario-based assessment work in support of federal safety, emergency and risk management; and the capability-based planning methodology. Experience with the latter methodology includes: building on previous CSS risk and decision support solutions; operations research and risk SME engagement in development; experimenting with techniques at the regional and local levels; and employing collaborative techniques, such as the Delphi method with regional stakeholders.

Other emerging building blocks that should contribute to an evolutionary improvement of risk assessment and risk governance include: (program) value assessment framework; evidence bases (program and Tri-Service); senior leadership forum (Tri-Service); quantitative analysis of economic loss and the impact on society; and interdependency and risk modeling. All of these initiatives are applying, testing and adapting risk assessment and decision support techniques with input from those who are closest to the risks. Systematic improvements at the tactical (community) and operational (region including cross-border engagement) levels should translate into a better picture of risk, and more reliable and valuable risk-based approaches at the federal (national and international) level.

The study presents a preliminary CMM assessment framework for each operational area and for multi-criteria risk, target, factor and other assessments in general. The intent is to demonstrate the use of this technique to highlight opportunities to take advantage of the exiting CSS knowledge bases, emerging trends in risk assessment and other techniques; and to contribute to applying a system of systems approach to increase the value of risk information.

This page intentionally left blank.

References

This section includes some references that were considered to assess the variety of risk assessment techniques in general use and to develop a capability maturity model framework. Some community-specific references are cited in the relevant profiles.

Aon Risk Maturity Index, Insight Report, November 2013

CAN/CSA-IEC/ISO 31010:2009, Risk management – Risk assessment techniques

Canadian Security and Safety Program (CSSP), Strategic Planning Guidance

Carson, L. J., Professional Insights – *Engineering the Executive's Dashboard* – Forestry Insights into Human Metrics; Affiliated Timber Investment Advisors (ATICA) Inc., Oregon, US; February 2010

CERT Resilience Management Model, A Maturity Model for Managing Operational Resilience (CERT-RMM, Version 1.1); Software Engineering Institute (SEI) Series, Carnegie Mellon University (CMU); Addison-Wesley, US; 2011

Combining [*offender*] Risk Assessment Tools, Research Summary; Vol. 17, No.21, Public Safety, March 2012 (ISSN: 1916-4009)

Community of Practice (CoP) – specific references are included in individual profiles

Community of Practice (CoP) Fact Sheets (11), missing risk and tri-service

CoP Summit Report, June 13, 2013 (NIVA Inc for CSSP), DRDC-CSS, 2013

Dashboard Best Practices (Abstract), LogiXML, 2010

Decision Support Section Analysis of the June 14, 2013 CoP Summit; DRDC-CSS, 2013

Dziadyk, W. et al (2011), *Harmonized Threat and Risk Assessment (HTRA) Methodology – Limitations*; BDProInc, Ottawa, Canada, 13 September 2011

Framework for the Management of Risk, Treasury Board Secretariat (TBS), 2010

Giannopoulos, G. et al (2012), *Risk Assessment Methodologies for Critical Infrastructure Protection*. Part 1 – State of the art, EU 25286 – EN 2012, European Commission, Joint Research Centre, Institute for the Protection and Security of the Citizen, EU Publication Office, Luxemburg, 2012

GRiP, A Flexible Approach for Calculating Risk as a Function of Consequence, Vulnerability and Threat (ANL-DIS 11-3), Argonne National Lab (ANL), Decision and Information Sciences Division, US Government, January 2011

Harmonized Threat and Risk Assessment Methodology (TRA-1), Government of Canada (GC), 2007

Helbing, D. (2010), *Systemic Risks in Society and Economics*, International Risk Governance Council (IRGC), phase 1 of project on emerging risks, Geneva, 2010; http://irgc.org/wp-content/uploads/2012/04/Systemic_Risks_Helbing2.pdf; 2014

IRGC, <http://www.irgc.org/> (Accessed May 2014)

Management of Risk for Critical Infrastructure, Treasury Board Secretariat

National Infrastructure Protection Plan (NIPP), *The Protection Program Strategy: Managing Risk* – Section3; Department of Homeland Security (DHS), US, 2006

NIPP, *Risk Management Framework*, Fact Sheet, DHS, US (not dated)

Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements, with Guidance for Use (ASIS SPC.1:2009), American National Standard, ASIS International, US, 2009

Project Management Body of Knowledge (PMBoK), Project Management Institute

Regional Capability-Based Planning Methodology Guidelines, Draft, CSS, 2013

Regional Resiliency Assessment Program (RRAP, Department of Homeland Security (DHS), <http://www.dhs.gov/regional-resiliency-assessment-program>; 2014

Renewing Canada's Action Plan for Critical Infrastructure (2014-2017, PS, 2014)

Risk Taxonomy (O-RT, V.0), The Open Group, 2013

Security Risk Management Body of Knowledge (SRMBoK), Risk Management Institution of Australia (RMIA) Ltd, Wiley, Australia; 2009

Strategic Risk Management in Government: A Look at Homeland Security, Managing for Performance and Results Series, IBM Center for the Business of Government, 2009

Annex A Observations

The study team made several general observations and deductions pertinent to the risk scan. The intention is to use these observations and deductions as a framework for group discussion:

- The interview process unearthed concerns and issues with respect to GC / CSS roles, responsibility and accountability for risk assessment / risk management.
- While departmental accountability for mandate-specific risk is clear, and responsibilities of Ministers are well documented, the accountability and governance requirements concerning risk assessment when multiple departments are involved, and for Portfolio and CoP management, are not well defined or documented.
- Due to the importance of risk assessment as a “feeder” to the priority setting process, there is a need for a well-documented approach and framework to risk assessment across the Centre.
- As part of this framework, emphasis should be placed on risk assessment that directs/guides the next phase of investment decision making, versus a macro-level assessment of anticipated gaps and future needs. It is difficult to “track and trace” the way in which risk assessment information is integrated into Centre decision-making.
- At same time, it is recognized that the Portfolio managers need sufficient access to resources to respond (effectively and efficiently) to emerging high priority risk-informed demands, including the ability to redirect funds to meet these new needs.
- Although the Portfolios are able to tacitly refer to assessments and products on the basis of perceived importance to CSSP outcomes and priorities, there is a need for a more transparent, systematic and robust assessment of the CSS capability domains, CoPs and Portfolios, including increased visibility of partners’ risk assessment & decision making practices.
- Using subjective surveys, logic models or roadmaps can inherit and promulgate the problems of lack of analytical rigour or clouds the analysis; and the decisions and outcomes might not be entirely satisfactory.
- Without such an approach, CSS runs the risk of not having a coherent planning process with consistent Portfolio analysis integral within each of the domains to substantiate investment decisions (thereby, moving away from potentially, narrow “self-generated rationalizations of proposals”).
- With the exception of the CBRNE, BTS, Cyber, CIP and EMSI Portfolios, the focus of risk management is primarily on project delivery, monitoring, tracking and execution, and most Portfolios are insufficiently leveraging risk assessment techniques to manage the Portfolio responsibilities.
- Ad hoc risk assessment is labour-intensive and expensive in staff time, whereas a systematic approach that leverages existing management processes and interactions would build on the CSS team’s vast experience and personal networks.
- The current CSSP framework, with respect to governance, collaboration with partners, project selection, financial management and accountability, the policy planning apparatus, and the evolving public safety and security environment is more complex and greater in scope than when the program was initiated.

- The need to focus on exploiting, applying and leveraging risk information has never been greater.
- These factors highlight the importance of identifying a critical mass of science-based, safety and security risk management expertise, and the application of practical and sustainable techniques and tools to respond to emerging issues. Are these primary or secondary to the achievement of the CSSP mandate?
- The current fiscal situation is placing more pressure on DRDC to “do more with less,” and functions such as risk assessment (and decision support) may become the focus (and enablers) for identifying strategic technologies and capabilities of interest, which apply across the broadest possible set of functions along the response continuum (e.g., full-spectrum scenarios, -3 to + 3).
- In order for any risk assessment process to be sustained over time, it has to be based on good-enough (and available) information. Yet, in most cases, the study team found that most Portfolio managers are not supported by access to the available information in a timely manner to inform and support investment recommendations.
- The current “devolved/decentralized” risk-informed decision making model was designed to respond to the mostly, intelligence-based threats/hazards associated with the CRTI (e.g., counter-terrorism; malicious threats).
- It is not necessarily optimized for the interaction of complex scientific; strategic, operational and tactical environments; or the public policy requirements needed to balance investment across public safety and security domains.
- It is debatable whether the current approach to defining the CSSP risk posture and capability, if retained, would be able to adapt and function effectively in the future, as the program faces a vast array of challenges in the public safety and security environment, which will increasingly require the systematic prioritization and collaborative treatment of high-risk, high consequence issues.
- A new risk assessment framework for CSS might need to be built, identifying critical RA elements for each Portfolio and gaps in tools/methods. Until such work is complete and validated, it is premature to assume the same deficiencies apply across the board (i.e., no “one size fits all” formula).
- The choice between any options/alternatives reflects a choice about the nature, purpose and direction of the program, and strategic governance and management considerations that go beyond this project. Options might include:
 - ◆ Status quo;
 - ◆ Shared custodianship with embedded / dedicated teams within each of the directorates, with service delivery managed by OR&A staff; and
 - ◆ More resources allocated to improve internal risk assessment and decision support capacity.

Annex B Compendium of risk assessment techniques

This annex presents a consolidated view of techniques for nine operational areas and the strategic (program management) function. Tri-Service CoPs are treated separately because Fire and Paramedics are relatively new and there are some variations in gaps and approaches. The compendium captures techniques, tools and assets that related to risk-informed decision making. It does not include whole-of-government capabilities, such as the Integrated Threat Assessment Centre (ITAC) or discrete techniques acquired or being used by the Risk Assessment and Capability Integration (RACI) or Decision Support sections.

| Operational Area | Decision Support / Risk Assessment Tools & Techniques / Assets |
|---|---|
| Border & Transportation Security (BTS) and Maritime Security (and Critical Infrastructure Resilience) | <ul style="list-style-type: none"> • <i>RiskOutlook</i> (Deep Logic Solutions) – dependency mapping • Maritime Domain Awareness • Interdepartmental Maritime Security Working Group (IMSWG) risk assessment (classified) • Joint risk assessment (CBSA / DHS CBP) • CSS has no visibility of departmental, bottom-up risk assessment processes or criteria for prioritization |
| e-Security / Cybersecurity | <ul style="list-style-type: none"> • Risk-based approach to select CSS investment priorities (power, communications) – finance capability funded by others; CONOPS – self-sustaining Sandboxes / networks • Investment guide, based mainly on gap analysis techniques • National Infrastructure Test Centre (NITC); simulations from NITC (2014+) • Focus on Big Organization Radical Groups (BORG) |
| Surveillance, Intelligence & Interdiction (SII) Portfolio | <ul style="list-style-type: none"> • Risk-based approach to select priorities (avoid duplication; add value) • Departmental Security Officer Readiness Committee (DSO RC) Handbook (PCO, 2013) • Harmonized Threat & Risk Assessment (HTRA, 2007) – has known limitations • Defence Research & Development Canada (DRDC): intelligence, surveillance and reconnaissance; command and control |
| Critical Infrastructure Protection (CIP) CoP | <ul style="list-style-type: none"> • Interdependency and risk modeling (e.g., architecture framework) • PS CI Gateway; CI Multimedia Tool; CI Resiliency tools (DHS RRAP) • Virtual Risk Assessment Cell (VRAC), direct support to Government Operations Centre (GOC) • National risk profile (PS); sector risk profiles (Federal lead departments – status unknown) • Regional Resilience Assessment Program (RRAP) – All hazards site assessments • Justice Institute BC (JIBC) criticality & dependency assessment |

| Operational Area | Decision Support / Risk Assessment Tools & Techniques / Assets |
|-----------------------------|---|
| Fire CoP | <ul style="list-style-type: none"> • P/T CI programs (BC, AB, SK, ON, NB, Yukon, others TBD) – PS survey requested by CSS • All Hazard Risk Assessment Framework and risk event scenario management framework • DRDC: explosive effects, blast modeling... • P/T/ Hazard Identification and Risk Assessment (HIRA) or equivalents (e.g., vulnerability analysis) • HAZMAT assessment (local teams) • Emergency Responder Test & Evaluation Establishment (ERTEE) • Gap – evidence base (national perspective of firefighting capability, interdependencies and risk mitigation) |
| Paramedics CoP | <ul style="list-style-type: none"> • P/T Hazard Identification and Risk Assessment (HIRA) or equivalents (e.g., vulnerability analysis) • Emergency Responder Test & Evaluation Establishment (ERTEE) • Gap – evidence base (national perspective of paramedics capability, interdependencies and risk mitigation) |
| Law Enforcement CoP | <ul style="list-style-type: none"> • Regional risk assessment spreadsheet and capability-based planning guide (CSS, draft:2013) • Loss analysis tool – in development • Factor-based assessments using Delphi & Voting SW technology • Tactical – Hazard Identification and Risk Assessment (HIRA) or equivalents (e.g., vulnerability analysis) • Canadian Interoperability Technology Interest Group (CITIG) guiding principles (risk management & outcome-focused) • Emergency Responder Test & Evaluation Establishment (ERTEE) • Gap – evidence base (national perspective of policing and security operations capability including cross-border capabilities, major events and risk mitigation) |
| CBRNE and Forensics Section | <ul style="list-style-type: none"> • Consolidated Risk Assessment (CRA) – intelligence-based (classified), described in <i>Regional Capability-Based Planning Methodology Guidelines, draft, 2013</i> • Specialist threat, hazard and vulnerability analysis (e.g., deterministic and probabilistic safety analysis) • Increased emphasis on target and effects analysis including impact on specific target groups (e.g., vulnerable populations); broader safety focus including disease outbreaks, industrial accidents, etc. |

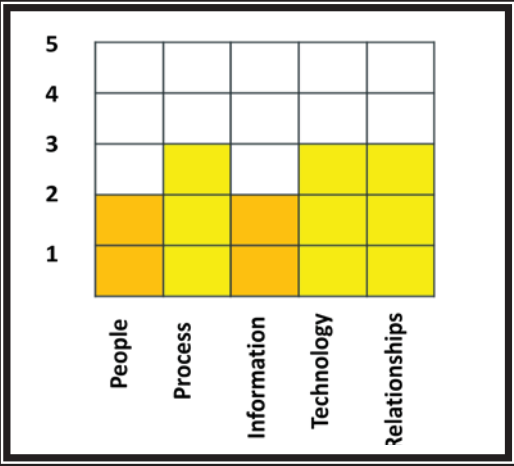
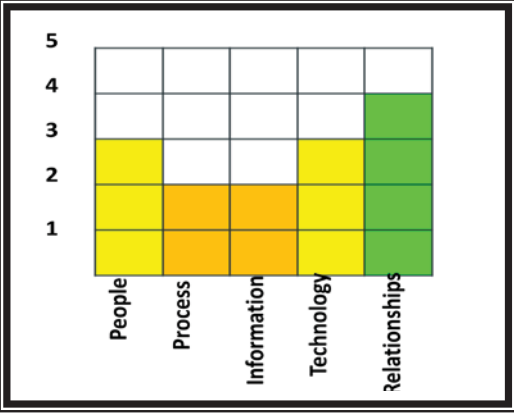
| Operational Area | Decision Support / Risk Assessment Tools & Techniques / Assets |
|--|---|
| Emergency Management System Interoperability (EMSI) and Psychosocial Section | <ul style="list-style-type: none"> • CI resilience assessment (CA/US) • Tactical HAZMAT analysis • Multi-jurisdictional Improvised Explosives Device (IED) workshops (RRAP) • Emergency Responder Test & Evaluation Establishment (ERTEE) • DRDC; personal protection; protection of assets; decontamination... • <i>Expert Choice</i> – experimented with voting technology to rate requirements • Federal All Hazard Risk Assessment (AHRA) Framework guide and scenarios • Regional risk assessment spreadsheet and capability-based planning guide (CSS, draft:2013) • Tactical/local – Hazard Identification and Risk Assessment (HIRA) or equivalents • DRDC: behavioural effects; communications networks; command and control; situational awareness... |
| Knowledge, Technology & Community Safety Section, and Program Decision Support | <ul style="list-style-type: none"> • Strategic Planning Guidance, environmental scan, implicit risk-based approach... • Gaps – program value management framework and evidence base • Other issues (managers' guidebook; technology road map; process improvement) systematic approach to risk management; central oversight and sustainability of risk / decision support capabilities and tools bought by projects; glossaries / guidelines on core processes (e.g., Delphi Method; scenarios; capability assessment methodology; economic impact / loss models; interdependency and risk models; expert elicitation; cost, benefit & risk analysis; measures of effectiveness...) |

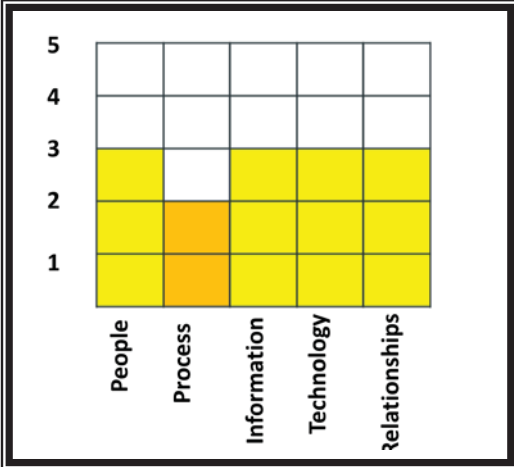
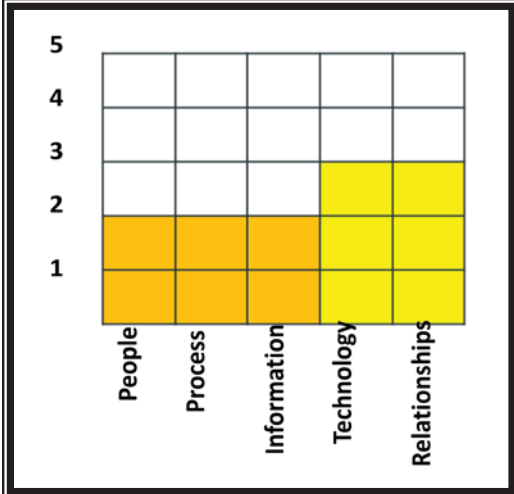
This page intentionally left blank.

Annex C Capability maturity model assessment

The preliminary CMM assessments below used a blended approach to assess the various multi-criteria risk assessment techniques from a CSSP perspective. To gain more clarity, one would need to gather evidence of the exact processes that are being used. Therefore, this is not an assessment from the partners' perspective. The assessment is used to identify quick wins across communities and to highlight ideas to improve risk assessment practices within CSS.

Communities of Practice and Portfolios are grouped into nine operational areas. Fire, Paramedics and Law Enforcement are assessed individually. The program risk management capability is assessed separately. A description of the rationale for the assessment is in a separate PowerPoint presentation held by CSS, RACI Section.

| Operational Area / Domain | Capability Maturity Model – Preliminary Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|---------|-------------|------------|---------------|--|--|---|--|--|--|--|---|---|---|---|--|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--|--------|---------|-------------|------------|---------------|
| Border & Transportation Security (BTS) and Maritime Security (and Critical Infrastructure Resilience) |  <table border="1" data-bbox="716 789 1227 1251"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td>3</td><td></td><td>3</td><td>3</td></tr> <tr><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | | 3 | | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 1 | 1 | 1 | 1 | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | 3 | | 3 | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| e-Security / Cybersecurity |  <table border="1" data-bbox="716 1314 1227 1724"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td>4</td></tr> <tr><td>3</td><td>3</td><td></td><td></td><td>3</td><td></td></tr> <tr><td>2</td><td>2</td><td>2</td><td>2</td><td>2</td><td></td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td></td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | 4 | 3 | 3 | | | 3 | | 2 | 2 | 2 | 2 | 2 | | 1 | 1 | 1 | 1 | 1 | | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 3 | | | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Operational Area / Domain | Capability Maturity Model – Preliminary Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---------|-------------|------------|---------------|--|--|---|--|--|--|--|--|---|--------|--|--------|--------|--------|---|--------|--------|--------|--------|--------|---|--------|--------|--------|--------|--------|--|--------|---------|-------------|------------|---------------|
| Surveillance, Intelligence & Interdiction (SII) Portfolio |  <p>A 5x5 grid showing maturity levels for SII Portfolio. The y-axis is labeled 1 to 5. The x-axis categories are People, Process, Information, Technology, and Relationships. The grid shows maturity levels: People (1-3), Process (1-2), Information (1-3), Technology (1-3), and Relationships (1-3). The cell for Process at level 2 is shaded orange, while all other cells are yellow.</p> <table border="1" data-bbox="745 321 1256 785"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td>Yellow</td><td></td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td>2</td><td>Yellow</td><td>Orange</td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td>1</td><td>Yellow</td><td>Orange</td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | Yellow | | Yellow | Yellow | Yellow | 2 | Yellow | Orange | Yellow | Yellow | Yellow | 1 | Yellow | Orange | Yellow | Yellow | Yellow | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Yellow | | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Yellow | Orange | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Yellow | Orange | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Critical Infrastructure Protection (CIP) CoP |  <p>A 5x5 grid showing maturity levels for CIP CoP. The y-axis is labeled 1 to 5. The x-axis categories are People, Process, Information, Technology, and Relationships. The grid shows maturity levels: People (1-2), Process (1-2), Information (1-2), Technology (1-3), and Relationships (1-3). The cells for People, Process, and Information at levels 1 and 2 are shaded orange, while Technology and Relationships at levels 1, 2, and 3 are yellow.</p> <table border="1" data-bbox="745 861 1256 1352"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td><td></td><td>Yellow</td><td>Yellow</td></tr> <tr><td>2</td><td>Orange</td><td>Orange</td><td>Orange</td><td>Yellow</td><td>Yellow</td></tr> <tr><td>1</td><td>Orange</td><td>Orange</td><td>Orange</td><td>Yellow</td><td>Yellow</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | | | | Yellow | Yellow | 2 | Orange | Orange | Orange | Yellow | Yellow | 1 | Orange | Orange | Orange | Yellow | Yellow | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Orange | Orange | Orange | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Orange | Orange | Orange | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Operational Area | Capability Maturity Model – Preliminary Assessment | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---------------------|--|---------|-------------|------------|---------------|--|--|---|--|--|--|--|--|---|--------|--|--------|--------|--------|---|--------|--------|--------|--------|--------|---|--------|--------|--------|--------|--------|--|--------|---------|-------------|------------|---------------|
| Fire CoP | <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td><td></td><td></td><td>Yellow</td></tr> <tr><td>2</td><td>Orange</td><td></td><td></td><td></td><td>Yellow</td></tr> <tr><td>1</td><td>Orange</td><td>Red</td><td>Red</td><td>Orange</td><td>Yellow</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | | | | | Yellow | 2 | Orange | | | | Yellow | 1 | Orange | Red | Red | Orange | Yellow | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Orange | | | | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Orange | Red | Red | Orange | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Paramedics CoP | <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td></td><td></td><td></td><td></td><td>Yellow</td></tr> <tr><td>2</td><td>Orange</td><td></td><td></td><td></td><td>Yellow</td></tr> <tr><td>1</td><td>Orange</td><td>Red</td><td>Red</td><td>Orange</td><td>Yellow</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | | | | | Yellow | 2 | Orange | | | | Yellow | 1 | Orange | Red | Red | Orange | Yellow | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | | | | | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Orange | | | | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Orange | Red | Red | Orange | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Law Enforcement CoP | <table border="1" style="margin-left: auto; margin-right: auto;"> <tr><td>5</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>4</td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td>3</td><td>Yellow</td><td></td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td>2</td><td>Yellow</td><td>Orange</td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td>1</td><td>Yellow</td><td>Orange</td><td>Yellow</td><td>Yellow</td><td>Yellow</td></tr> <tr><td></td><td>People</td><td>Process</td><td>Information</td><td>Technology</td><td>Relationships</td></tr> </table> | 5 | | | | | | 4 | | | | | | 3 | Yellow | | Yellow | Yellow | Yellow | 2 | Yellow | Orange | Yellow | Yellow | Yellow | 1 | Yellow | Orange | Yellow | Yellow | Yellow | | People | Process | Information | Technology | Relationships |
| 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | Yellow | | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | Yellow | Orange | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | Yellow | Orange | Yellow | Yellow | Yellow | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | People | Process | Information | Technology | Relationships | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| Operational Area | Capability Maturity Model – Preliminary Assessment | | | | | | | | | | | | |
|--|---|------------------|-------------|------------|---------------|------------|---------------|--|---|---|---|---|---|
| CBRNE and Forensics Section | <table border="1"> <thead> <tr> <th>Operational Area</th> <th>People</th> <th>Process</th> <th>Information</th> <th>Technology</th> <th>Relationships</th> </tr> </thead> <tbody> <tr> <td>CBRNE and Forensics Section</td> <td>4</td> <td>3</td> <td>3</td> <td>3</td> <td>4</td> </tr> </tbody> </table> | Operational Area | People | Process | Information | Technology | Relationships | CBRNE and Forensics Section | 4 | 3 | 3 | 3 | 4 |
| Operational Area | People | Process | Information | Technology | Relationships | | | | | | | | |
| CBRNE and Forensics Section | 4 | 3 | 3 | 3 | 4 | | | | | | | | |
| Emergency Management System Interoperability (EMSI) and Psychosocial Section | <table border="1"> <thead> <tr> <th>Operational Area</th> <th>People</th> <th>Process</th> <th>Information</th> <th>Technology</th> <th>Relationships</th> </tr> </thead> <tbody> <tr> <td>Emergency Management System Interoperability (EMSI) and Psychosocial Section</td> <td>3</td> <td>2</td> <td>2</td> <td>2</td> <td>3</td> </tr> </tbody> </table> | Operational Area | People | Process | Information | Technology | Relationships | Emergency Management System Interoperability (EMSI) and Psychosocial Section | 3 | 2 | 2 | 2 | 3 |
| Operational Area | People | Process | Information | Technology | Relationships | | | | | | | | |
| Emergency Management System Interoperability (EMSI) and Psychosocial Section | 3 | 2 | 2 | 2 | 3 | | | | | | | | |
| Knowledge, Technology & Community Safety Section, and Program Decision Support | <table border="1"> <thead> <tr> <th>Operational Area</th> <th>People</th> <th>Process</th> <th>Information</th> <th>Technology</th> <th>Relationships</th> </tr> </thead> <tbody> <tr> <td>Knowledge, Technology & Community Safety Section, and Program Decision Support</td> <td>3</td> <td>2</td> <td>2</td> <td>2</td> <td>3</td> </tr> </tbody> </table> | Operational Area | People | Process | Information | Technology | Relationships | Knowledge, Technology & Community Safety Section, and Program Decision Support | 3 | 2 | 2 | 2 | 3 |
| Operational Area | People | Process | Information | Technology | Relationships | | | | | | | | |
| Knowledge, Technology & Community Safety Section, and Program Decision Support | 3 | 2 | 2 | 2 | 3 | | | | | | | | |

C.1 Summary of risk assessment capability and maturity for operational areas

| Portfolio / Criteria | People | Process | Information | S&T | Relationships |
|----------------------|---------------------|---------------------|---------------------|---------------------|------------------|
| BTS | Level 2: Repeatable | Level 3: Defined | Level 2: Repeatable | Level 3: Defined | Level 3: Defined |
| E-Sec/Cyber | Level 3: Defined | Level 2: Repeatable | Level 2: Repeatable | Level 3: Defined | Level 4: Managed |
| SII | Level 3: Defined | Level 2: Repeatable | Level 3: Defined | Level 3: Defined | Level 3: Defined |
| CIP | Level 2: Repeatable | Level 2: Repeatable | Level 2: Repeatable | Level 3: Defined | Level 3: Defined |
| Fire | Level 2: Repeatable | Level 1: Initiating | Level 1: Initiating | Level 2: Repeatable | Level 3: Defined |
| Paramedics | Level 2: Repeatable | Level 1: Initiating | Level 1: Initiating | Level 2: Repeatable | Level 3: Defined |
| Law Enforcement | Level 3: Defined | Level 2: Repeatable | Level 3: Defined | Level 3: Defined | Level 3: Defined |
| CBRNE | Level 4: Managed | Level 3: Defined | Level 3: Defined | Level 4: Managed | Level 4: Managed |
| EMSI | Level 3: Defined | Level 2: Repeatable | Level 2: Repeatable | Level 2: Repeatable | Level 3: Defined |
| KTCS/CSSP | Level 3: Defined | Level 2: Repeatable | Level 2: Repeatable | Level 2: Repeatable | Level 3: Defined |

| | |
|--|---------------------|
| Legend: Relative to Capability Maturity Model | Level 5: Optimizing |
| | Level 4: Managed |
| | Level 3: Defined |
| | Level 2: Repeatable |
| | Level 1: Initiating |

This page intentionally left blank.

Annex D Participants

When the project was initiated, it was intended to complete all the interviews within two months. A lesson learned is that stretching out the information gathering and interview process (from two to five months) should be avoided if possible, because it disrupts the project flow and analysis process. Interviews were streamlined and informal to facilitate exploring new ideas and to minimize duplication. Sessions were scheduled with Section Heads after interviewing managers, when possible to explore both perspectives. No interviews were conducted with directors and above, which should be considered for future iterations. No interviews were conducted outside CSS, which could be considered in future iterations.

| Date | Section, CoP, Portfolio | Participants |
|--|--|---|
| 14 Feb, 1330-1430 | Border & Transportation Security (BTS), and Critical Infrastructure Resiliency (CIR) Section | Pierre Meunier |
| 7 Feb, 1400-1500 | Border & Transportation Security (BTS), Portfolio | Dr. Paul Hubbard |
| 17 Jan, 1430-1530 | Cybersecurity / e-Security CoP | Rodney Howes |
| 9 Jan, 1400-1500 | Surveillance, Intelligence & Interdiction (SII), CoP | Stephane Lefebvre |
| 14 May, 1400-1500 | Critical Infrastructure Protection (CIP) | Lynne Genik |
| 12 Mar, 1100-1200 20 Mar, 1000-1100 2 May, 0900-1000 | Tri-Services Portfolio | Fire – David Matschke EMS – Dough Socha LE – Sheldon Dickie Strategic Leadership – John Neilly (not interviewed) |
| 28 Jan, 1100-1200 | CBRNE and Forensics Section | Norman Yanofsky |
| 25 Feb, 1400-1500 | Emergency Management Systems Interoperability & Psychosocial (EMSI/P) Section | Jack Pagotto |
| 3 Apr, 0930-1030 | Knowledge, Technology & Community Safety (KTCS) Section | Colin Murray |
| 11 Apr, 0900-1000 | Program Support Portfolio Management tools | Ahmad Khorchid Brian Greene |

This page intentionally left blank.

Annex E Communiqué

Subject: CSSP Risk Scan & Compendium

In response to the CSSP Strategic Planning Guidance (2013), the Risk Assessment & Capability Integration section has been charged with developing a compendium of risk assessment techniques being used by Portfolio Managers, Communities of Practice and working groups. The project will review the existing processes for managing risk information internally and for sharing with other communities that have exposure to similar threats, hazards and/or risks. It will also highlight mechanisms for supporting CSSP decisions on high-payoff projects that include cross-domain consideration of risks that are unlikely, but that could have a very high impact locally, regionally or nationally.

The expected outcomes by 31 March 2014 include: a consolidated view of risk assessment approaches, strengths, challenges and strategies; a snapshot of CoP capability maturity; preliminary tools for discussion; and opportunities for CSS attention in the next 3-5 years. CSS has hired a consultant (Mr. Ian Bayne) to develop capability profiles and a draft report that will be validated by participants electronically or possibly, by workshop.

The approach includes interviews with CSS staff and a review of material stored on the Partners' Collaboration SharePoint site. The interviews are expected to last up to 90 minutes (max). Participants are requested to provide samples of risk assessment process descriptions and assessment outputs. An interview framework and the proposed list of participants are attached. The Project Authority, Shaye Friesen will contact participants directly to establish the interview schedule. It is hoped to complete the first wave of interviews before the Christmas holidays, and to conduct follow-up meetings or interviews in January-February.

It would be appreciated if you could make yourselves available for these interviews as all will benefit from having a greater understanding of how our risk posture is driving investment.

Attachments:

Interview Schedule

Interview Framework

Collegues :

En réponse au guide de planification stratégique du PCSS (2013), la section de l'évaluation des risques et de l'intégration des capacités a été chargée d'élaborer un compendium de techniques d'évaluation des risques utilisées par des gestionnaires de portefeuille, des communautés de pratique et des groupes de travail. Le projet permettra d'examiner les processus actuels de gestion des données sur les risques à l'interne et de partage avec d'autres communautés exposées à des menaces, des dangers ou des risques semblables. Il soulignera également les mécanismes pour appuyer les décisions du PCSS concernant des projets très rentables incluant la prise en compte interdomaine des risques qui sont peu probables, mais qui peuvent avoir une très grande incidence à l'échelle locale, régionale ou nationale.

Parmi les résultats attendus d'ici le 31 mars 2014 : vue d'ensemble des méthodes, des forces, des difficultés et des stratégies d'évaluation des risques; aperçu de la maturité des capacités des communautés de pratique; outils préliminaires aux fins de discussions; possibilité d'attention du CSS au cours des 3 à 5 prochaines années. Le CSS a retenu les services d'un consultant, M. Ian Bayne, pour élaborer des profils de capacités et un rapport provisoire qui seront validés par des participants par voie électronique ou possiblement lors d'un atelier.

L'approche comprend des entrevues avec le personnel du CSS et un examen du matériel sauvegardé sur le site de collaboration SharePoint des partenaires. Les entrevues peuvent durer jusqu'à 90 minutes (maximum). Les participants doivent fournir des exemples de descriptions de processus d'évaluation des risques et de résultats d'évaluation. Vous trouverez ci-joint un cadre d'entrevue et la liste de participants proposés. Le chargé de projet, Shaye Friesen, communiquera directement avec les participants afin d'établir le calendrier des entrevues. Idéalement, la première vague d'entrevues devrait prendre fin avant la période des Fêtes et les rencontres ou entrevues de suivi devraient avoir lieu en janvier et février.

Nous vous serions reconnaissants de bien vouloir être disponibles pour ces entrevues. Le fait de mieux comprendre comment notre position par rapport aux risques stimule l'investissement sera avantageux pour tous.

Pièces jointes :

Calendrier des entrevues

Cadre d'entrevue

Annex F Interview framework

1. Context (5 minutes):

- Identify the types of risks (e.g., safety, security, resilience, technology, procurement, collaboration, policy, governance, political...).
- Identify the variables being assessed (e.g., threats, hazards, vulnerabilities, impacts, consequences, criticality, resiliency, interdependency...).

2. References (5 minutes; identify source):

- What are the primary references and tools that support the risk assessments (e.g., policies, legislation, regulations, standards, handbooks, software tools, voting technology, etc.)?

3. Risk Assessment Capability Maturity (30 minutes):

People (5 minutes):

- To what extent do participants have the right experience, knowledge and expertise to make accurate, informed risk assessments?
- As Portfolio Manager/Section Head, are you confident that risk assessments are meeting your requirements (e.g., timeliness, accuracy, relevance...)?

4. Process (10 minutes):

- Is the process for identifying, assessing and prioritizing risks well-documented?
 - ♦ Please provide samples of guides and outputs.
- Describe the analytical techniques, methods and tools for combining variables and differentiating risks at the CoP and working group levels (if not described in guides).
- Do the risk assessments contribute to forming a portfolio view of risk exposure?
- Can you trace portfolio investments to mitigation of risk?

5. Intelligence and Information Sharing (5 Minutes):

- What mechanisms are used to ensure that intelligence-related information is incorporated into the risk assessment process?
- Any comments/concerns around access to the “right” SME knowledge/information that is needed to achieve a comprehensive picture of the risk environment?

6. Networking / Collaboration (5 minutes):

- Describe the mechanisms for inter-agency coordination (either required or in place) to engage key stakeholders at appropriate times in the process.
- Describe the information infrastructure that supports planning, networking and collaboration.

7. S&T/R&D/OR Foundation (5 minutes):

- To what extent are science, engineering and academic resources leveraged to support the assessments?

8. Way Forward (5-year horizon) (20 minutes):

- What are the major challenges of the risk assessment process and what should be done to improve the assessments?
- In your opinion, where should CSS (and the Risk Network CoP) focus its attention in the next 3-5 years, and why?

Annex G Risk assessment capability profiles

Profiles are based on: interviews with CSS subject matter experts, Portfolio Managers and/or Community of Practice (CoP) leaders; in some cases, review of documents stored on the DRDC Partners' SharePoint site, and independent literature research.

G.1 Risk assessment capability profile – Border & transportation security

| BTS & Maritime Security RA Capability Profile |
|---|
| <p>1. Context: Describe the domain</p> <p>OPI: Paul Hubbard, BTS Portman and CoP Facilitator</p> <p>The CSS Portfolio Manager (Portman) supports three main areas (Refer also to Presentation to CoP Summit, June 2013 for more detail in particular MindMap slide 6):</p> <ul style="list-style-type: none">• Screening and security the supply chain (e.g., detection; air cargo and container security at points of entry; maritime commerce resilience)• Traveller safety and screening (e.g., air passengers safety at points of entry)• Domain awareness (e.g., land, air, maritime and North border crossings; data integration & analysis)• 80% of the effort is on maritime security• Priorities include: maritime situational awareness; sensors; geospatial dispatch; and radar (e.g., Great Lakes)• There are currently no projects focused on the North• CSS monitors DND surveillance and DRDC activities that are relevant to regional BTS priorities• A Rail Sub-Working Group is being considered• CSS monitors biometrics work that is ongoing within the community (RCMP, CBSA, CIC)• Air Carrier Registration Automation is a project that supports new legislation• Shippers already register on-line• Container work includes: tamper-proof seals or other counter-tampering measures; a cyber-activity that is related to countering organized crime hacking of port systems to locate specific containers; and detection and identification of contents of containers (e.g., drugs, explosives, humans)• An OAG report (Dec 13) identifies the problem of US illegals entering Canada• CSS was invited to attend the Interdepartmental Maritime Security Working Group (IMSWG), which is discussing the Arctic and other potential requirements <p>Potential future interests include: domestic ferries; pipelines; underwater acoustics; 3D printers; unintentional GPS jamming near airports.</p> |

BTS & Maritime Security RA Capability Profile

Group interdependencies include: SII, Cyber, CIP, CBRNEF, Tri-Service, and Major Events...

Stakeholders include: RCMP (e.g., biometrics); TC (e.g., Air Cargo Security program, multi-modal safety and security systems); CATSA; CBSA (e.g., Container Security Program), DND (Arctic Surveillance), DFO / CCG; DFAIT ; DRDC; AANDC; NRCan; EC; IC (e.g., infrastructure action plan); airport and port authorities; F/P/T regulators; ferry and cruise ship operators; oil and gas pipeline owners.

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

Domain stakeholders have their own methodologies for assessment and prioritization of threats, hazards, vulnerabilities and/or risks, which are not visible at the BTS CoP level. An example of a domain driver is the **Beyond the Border Agreement**, which identifies domain awareness and watch lists as priorities. There is no horizontal view of standards or guidelines related to risk assessment methods across GC or F/P/T for BTS (or any other domain/CoP).

Priorities are influenced by multiple factors including: intelligence, political priorities, regional risk perception, and recent experience (e.g., Lac Megantic rail disaster; pipeline explosions) and international agreements.

3. Risk Assessment Capability Maturity:

a. Describe how the domain prioritizes risks and presents recommendations to the next level:

Priorities are developed by using a bottom-up approach and through the PSTP Call process. The CSS OPI consults with a small group of SMEs to validate new ideas and gain insight into community priorities. In this way, CSS can anticipate requirements and potentially, influence prioritization choices.

b. Describe how the portfolio prioritizes and communicates risks within CSSP

There is no systematic approach to risk assessments or comparing risk assessments across portfolios or CoPs within CSSP. The risk is mitigated by having experienced staff and an evolving IM environment. However, it is not clear that CSSP has a systematic approach to risk management at the program or portfolio/CoP levels. That is, CSS does not have a unified process to compare how the operational level, legal-, mandate- and domain-specific threat and/or risk-based approaches influence the selection of projects. For example, a percentage of CSSP annual investment on portfolios/CoPs does not provide insight into either the effectiveness of the program or the risk mitigation effect of targeted investments.

4. Major Challenges and Current Strategy:

CoP/Domain:

A persistent challenge is information sharing across domains and stakeholder organizations. For example, the Air Carrier Registration project depends on interoperability among databases

BTS & Maritime Security RA Capability Profile

and risk assessment tools that are owned by different departments, which have different risk perceptions and information protection requirements.

RCMP must be able to guarantee a chain of evidence.

Portfolio:

CSS maintains SA by a number of methods and networks that depend on one person, the PortMan. From a portfolio and CSSP perspective, this lack of depth poses a risk. This portfolio is a new initiative and further analysis would be required to assess the level of risk from stakeholders' perspectives. Community departments have their own sources of funds and processes for prioritizing investments and capability development initiatives.

This Portfolio / CoP should have at least two FTE's given its reach and national priority in multiple areas. It is not known if CSS is planning to add resources to manage this CoP.

5. Future:

a. What areas require more attention in the near-term?

- A strategic area for CSS consideration could be to review how risk assessments are being used to influence GC investment decisions in regional infrastructure projects (e.g., bridges, roadways, harbours)
- BTS and other portfolios/CoPs might benefit from a centrally-managed, proactive process to identify work in other parts of DRDC that could be leveraged for emerging S&T requirements (e.g., commercial applications of surveillance technology)
- This project should investigate the requirement to develop a common guide for risk assessment and risk-based approaches for portfolios and CoPs, with a view to making risk part of the CSSP Call and prioritization process
- The consultation with a small group of SMEs is a potential best practice that could be applied by other portfolios/CoPs, if they are not already doing this

b. Where could RACI add the most value in the near to mid-term?

- RACI should attend the next BTS WG meeting in June to determine if there is interest and value in making the group aware of CSS experience in the Consolidated Risk Assessment (CRA), AHRA (scenario-based workshops), capability assessment methodology and/or architecture frameworks
- RACI should investigate the value of benchmark research on resilience (Note: BTS priority for maritime commerce resilience). This would be applicable to multiple CoPs. It is a logical extension of risk assessment work.
- RACI could investigate the use of HAZUS-MH or other GIS-based risk assessment tools in the BTS domain
- RACI, in collaboration with DSS, should consider work on measures of effectiveness for the overall program including an integrated approach to performance and risk indicators
- RACI should investigate the requirement for information products for portfolio

BTS & Maritime Security RA Capability Profile

managers and CoP facilitators to advance the overall risk management capability maturity including: risk-based approaches and risk assessments

- RACI could consider Risk Calls related to benchmark research on supply chain governance, risk management (i.e., risk-based approaches, risk assessments, risk modeling, simulation and visualization); and/or compliance assurance
- RACI could consider the CSS (and DRDC) potential role in developing a risk profile of the North
- RACI could consider an investigation of how risk assessments are being used to inform major events planning
- There is potential for guided academic research in risk assessments related to BTS and other CoPs. However, CSS/RACI would likely not have the capacity to take this on as a task.

G.2 Capability profile – BTS and Critical Infrastructure Resilience (BCIR)

BCIR Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Pierre Meunier, Section Head, Border & Transportation Security, and Critical Infrastructure Resilience:

- **BTS** – includes: Maritime Domain Awareness (e.g., St Lawrence and Great Lakes – support to law enforcement, anti-smuggling; anti-organized crime...); global supply chain (e.g., detection; cargo and container security; vulnerability to cyber threats)
- **CIR** – includes CI sector / asset interdependency modeling
- **E-Security** – includes supply chain (cargo) and GPS vulnerability assessments

Areas of interest include:

- Gaps in tools for CI analysis – plans to investigate interdependency modeling, including risk component using **RiskOutlook** (Deep Logic Solutions) – over next two years
- Plans to leverage in-house DSS/OR capability
- Interested in “**latent**” **vulnerability** (e.g., CI assets)
- Work on targets and effects (CIP)
- Future collaboration with DHS (S&T)

Assumptions – Transportation security is well funded, and TC and F/P/T partnerships, strategies and investment plans are addressing the right priorities from a national perspective; and (actionable) Intelligence processes and products are being synchronized and contributing to a balanced approach to risk mitigation and capability investment and sustainment.

Case Study (Success) – CSS investment in MDA in St Lawrence Seaway and GL, was successful in reducing the risk of further RCMP and partners’ investments – provided a capability baseline and helped to understand the domain and how to leverage S&T.

Case Study (Failure) – Multi-year investment in technology to support client (CBA) that bought off the shelf UK solution (Does CSS require a process to continuously review investment risk exposure and to identify the high-pay-off / most strategic value opportunities over time?).

Uncertainty – Vulnerability and resilience of Ports and their respective supply chains and interdependencies (80% GDP); North – someone is going to develop a picture of security (and safety) risks in the North.

Strengths – Maritime Domain Awareness (MDA); CSS participates in **Interdepartmental Maritime Security Working Group (IMSWG)**; visibility of **PS Cross-Sector Forum**; blast modeling; monitoring developments in GPS vulnerability reduction via the inter-departmental GNSS initiative (e.g., to intentional or unintentional jamming threat); partnerships with US DHS (e.g., sensors, e-Cargo Security).

BCIR Risk Assessment Capability Profile

Weaknesses – SA of non-government controlled and/or private sector CI asset vulnerability (e.g., port and airport authorities; small airports; small vessels; cruise ships...); no mechanisms to maintain visibility of regional CI investments and/or risk-based assessment and investment prioritization processes; lack of national security (and safety and resilience) strategy; lack of national planning assumptions and national planning scenarios; GNSS is a one-person office; CSS capacity (multiple single points of failure – one person to manage diverse relationships and projects, while maintaining SA of: S&T and decision support tools; threat environment, GC partner decision making environments and priorities; national and regional strategies and initiatives; and international agreements and priorities).

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

MDA – IMSWG has a RA methodology (classified; A. Goudreau has a copy)

Stakeholder organizations perform internal, multi-criteria risk assessments (e.g., threat, hazard, vulnerability, impact, criticality, harm, interdependencies, business impact analysis...) based on their mandates and constraints (including authority). There is no holistic view the capability maturity of these processes within or across organizations. There are no common measures of effectiveness to evaluate how risk information is adding value to decision making or to identify best practices across risk domains.

DHS meeting, June 2014 – identify opportunities for collaboration.

Technology Readiness Levels (TRL) – what is Canadian perspective on TRL (NASA index) and other US decision support techniques (e.g., Hard Problems, Target Capabilities Lists...), and other national S&T best practices.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the Section prioritizes risks and presents recommendations to next level?

Risk is not an explicit part of the decision making process above the departmental / stakeholder level. The assumption is that organizations are making security threat-based decisions based on: accurate intelligence snapshots and projects on of threat and technology trends; departmental plans; GC and regional priorities; and international commitments and compliance requirements. There is no common view of the risk modeling capability across departments or levels of government including economic and interdependency modeling.

b. Describe how the Section prioritizes and communicates risks within CSSP?

The section does not use an explicit method to review risk exposure within or across domains. The section does not review the input of risk inputs to the departmental, mandate-focused decision making processes.

BCIR Risk Assessment Capability Profile

4. Major Challenges and Current Strategy:

a. CSSP:

- How to assess the value of CSSP investments:
 - CSSP budget is relatively fixed, while the number of areas of interest has expanded
 - CSS needs a consistent way to assess the value (and risk) of investments
- CSSP does not have a methodology to assess the value of program investments to the program, nation, regions or international relationships
- CSSP / national security – fragmented view of S&T capability (e.g., government-controlled, private sector and academia; and international relationships including at the P/T level)
- Lack of view of GC analytical, modeling and simulation and related S&T / engineering capabilities that implicitly or explicitly support decision making (management by “Briefing Notes” and focusing on short-term problem solving)
- Ad hoc process to identify relevant DRDC capabilities (e.g., dual use)
- TC is not an active participant in CoPs
- Strategy to leverage DSS/OR resources across CSSP domains / CoPs / portfolios – best investment of time and effort?

b. Domain/Portfolio/CoP:

- How to incorporate risk assessments in the review of interdependencies (e.g., interdependency risk; systemic risk – refer to WEF, 2014 Risk Assessment) – review capability of RiskOutlook, and implications for sustainment, combination with DSS and other risk assessment tools, and options to leverage tool for other CoPs
- How to assess supply chain risk
- How to assess resiliency

5. Future:

a. What areas require more attention in the near-term (from CSSP and/or Section perspective)?

- DSS/OR – develop criteria and streamlined, unified process for assessing cost, strategic benefit (value) and, interconnectedness and systemic risk of CSSP investments
- Review Arctic S&T Strategy and establish a mechanism to monitor the strategy implementation (e.g., review partners’ perspectives of S&T gaps, risk exposure and investment priorities)
- Review reasons for TC reticence to participate in CSSP (i.e., BTS, CIR)
- Compendium of risk assessment techniques
- Benchmark multi-criteria assessment techniques across domains
- Benchmark 5 Eyes’ resilience programs (e.g., UK, AS/NZ)
- Review risk of lack of participation by TC to effectiveness of CSSP / CoPs (e.g., BTA, CIP, Cyber, SII) – holistic view of transportation security; review of TC’s safety and security management systems (SeMS, SMS), and approach to multi-model issues
- Review priority of pipeline and rail security in Canada

BCIR Risk Assessment Capability Profile

- Review priority of the North (safety and security future)
- Review requirement for a centrally-managed process to monitor dual use technologies and work in DRDC

- b. Where could CSS RACI add the most value in the near to mid-term?**
- Review two strategic documents produced by Pierre: MDA and Portfolio Manager:
 - Review Maritime Security Strategic Framework
 - Review Maritime Domain Awareness Strategy
- Attend June meeting with DHS (limited seats; could be at CSS – depends on classification):
 - Benchmark supply chain RA techniques across domains
 - Identify opportunities to share information with DHS (e.g., interdependency modeling; CI vulnerability assessments; multi-criteria risk assessments; measure of effectiveness for risk based approaches; S&T balance of investment...)
- Review IMSWG MDA risk assessment methodology
- Get reference of Margaret Purdy's paper on safety, security and sovereignty risks – and review for relevant today and in the future (CSSP criteria)
- Monitor, and possibly contribute to, work with RiskOutlook
- Review opportunities to participate directly or indirectly in regional-level CI initiatives for ports and airport security improvements (e.g., regional gap analysis; regional CAM pilot project; review of multi-criteria risk assessment trends and best practices; independent review of P/T /M strategies / reports / initiatives) – RACI has some experience in this area (e.g., NB), but section does not have the capacity to be proactive
- Review priority to develop a set of national planning scenarios with first priority on BTS and CIR
- Review status of PS effort to produce Sector Risk Profiles (CIP), and develop one or two models of SRPs (e.g., transportation, border management, maritime security, national oil spill response capability...)
- Review opportunities to apply capability assessment methodology
- Review opportunities to develop a risk profile of the North
- Benchmark resilience programs (e.g., UK, AS/NZ)
- Review cost, benefit/value (and risk) of preparing a compendium of security risk assessment techniques being used by public and private sector CI stakeholders

G.3 Risk assessment capability profile – e-Security

e-Security Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Rodney Howes, CoP Manager

The CoP is focused on two of the three GC pillars described in Canada's Cyber Security Strategy (CCSS, 2010): Partnerships and Protecting Canadians. The CoP determined that the other Government pillar (GC capability) was being addressed by the major stakeholders.

Sandbox Concept

The strategy consists of implementing “sandboxes”, which transition from testbeds to self-sustaining stakeholder networks. The sandboxes are evolving from a number of CSS-sponsored studies completed over the past 3-4 years through the CSSP (e.g., Bell; Lofty Perch). The sandbox is an unclassified, collaborative environment based on SharePoint, where subject matter experts (SMEs) articulate the problem-space, share information, management knowledge and develop solutions. The sandboxes are intended to facilitate collaboration among Government, industry and academia, including with US and counterparts. The communities will be governed by a Board of Directors from stakeholder organizations. CSS would transition from a facilitator to an S&T advisory role. The assumption is that the community will assume ownership and sustain the sandbox.

The CoP strategy is based on three components, referred to as “enablers” (for CSS): Power – Communications – Money (P-C-M). The focus on Power and Money because the Communications component is being addressed by the major GC cyber stakeholders, regulators, P/T agencies and the private sector.

Power (SCADA / ICS / DCS / PCS¹⁰; Smart Grid, etc.):

- National Energy Infrastructure Test Centre (NEITC)
- Stakeholders include NRCan (lead department)
- It is envisaged that the NEITC will transition to a National Infrastructure Test Centre (NITC) with the completion of the next set of four CSSP-sponsored projects (summer 2014)
- Outputs will include: business plan; training; SCADA testing; and Smart Grid (vulnerability) testing; and identification of next steps
- **Simulations** will be used by the nuclear and hydro service providers
- This initiative is being linked to the Explosives and CIP CoPs, and other CSSP activities

Money (organized crime; cyber-crime; Big Organization Radical Groups):

- Partnership with the National Cyber-Forensics and Training Alliance (NCFTA, Pittsburgh, US) – signed MOU – <http://www.ncfta.net/>
- There is a Canadian NCFTA based at Concordia University whose focus is mainly research and training – <http://www.ncfta.ca/>

¹⁰ ICS = Industrial Control System; DCS = Distributed Control System; PCS = Process Control System.

e-Security Risk Assessment Capability Profile

- The partnership is with NCFTA (US) because of its operational focus and reach, including with its community including the FBI and the National White Collar Crime Centre (NW3C)
- The initial focus is on organized crime (OC), cyber-crime and Big Organization Radical Groups (BORGs). It is anticipated that there will be a link to the international effort on Anti-Money Laundering / Combating Financing of Terrorism, which is led by Finance Canada
- Stakeholders include Bank of Canada, S&I community
- Two people from the RCMP Cyber Crime Fusion Centre (CCFC) are receiving training this FY
- This sandbox is just being formed and it leverages the NEITC experience
- This initiative is being linked to the CIP, Forensics and Radicalization CoPs, and other CSSP activities

Communications:

- The way forward for this component has not been defined
- An example of ongoing work at a government-controlled lab is the National Research Council (NRC), Venus Project

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

Security

The GC risk assessment / management capability related to security in general, and energy, finance and cybersecurity in particular is fragmented and decentralized. Multiple central agencies and departments with specialist knowledge are involved in their mandate-specific areas, and indirectly, in providing direction, guidance, standards, technical reports, threat evaluations and other references.

PS facilitates interdepartmental committees at the ADM and DG level of most cybersecurity major departments. PS is also the lead department for coordination of Canada's critical infrastructure resilience initiatives and the Federal Emergency Response Plan (FERP), which includes response to cyber incidents.

Canada's Cyber Security Strategy (CCSS) is the foundational GC document. PS is the lead department. It is not clear that PS is using a risk-based approach to prioritize GC investments. For example, RCMP, CSIS and CSEC are submitting separate Memoranda to Cabinet (MC) for ongoing investment in cyber security. Although, PS has the All Hazard Risk Assessment (AHRA) Guidelines, which are being used to some extent in the emergency management area. The Government Operations Centre (GOC) and Canada's Cyber Incident Response Centre (CCIRC) are responsible to maintain situational awareness of the dynamic cyber threat environment. It is understood that the Office of the Auditor General (OAG) will audit the CSS strategy in the near future. CSS might be asked to provide input to the audit and possibly, the prioritization of follow-up action plans.

The GC cyber partners provide advice to departments, but it is up to departments to implement their IT and cyber security approaches. CSEC publishes the IT Security Guidelines (ITSG)

e-Security Risk Assessment Capability Profile

series, ITS Bulletins (ITSB) and other resources. For example, ITSG-33 is a guide for implementing a lifecycle approach to IT security risk management, which includes the shift from a threat- to a risk-based approach.

TBS is responsible for the operational standards for Management of IT Security (MITS) and business continuity planning (BCP). It is also the authority for the Departmental Directive on Security Programs (DDSP).

Large departments have significant IT security and cyber protection capabilities, while small departments have very limited capabilities. Further, some organizations are not subject to GC directives or standards. The SSC Federal Information Protection Centre (FIPC) capability became operational on 31 October 2013.

In summary, there is no consolidated view of the GC capability maturity in risk assessment in the cybersecurity area. RACI completed a pilot project to evaluate the use of Architecture Frameworks (AF) to support this environment, but there was no appetite to pursue the work.

Power

For ICS, techniques include gap analysis and vulnerability analysis that leverage stakeholder SME's experience, open source intelligence and risk trends. The US energy sector has many resources for risk and vulnerability assessment, and for developing Sector Risk Profiles, which can be adapted by Canadian organizations. NR Can has experience with the Hazards US Multi-Hazard (HAZUS-MH) program, and CSS has co-funded work to adapt HAZUS and other techniques to the Canadian environment.

Money

Banks use Basel iii, Enterprise Risk Management (e.g., COSO ERM model) and financial risk management techniques. COSO has been mapped to ISO 31000. However, most organizations look inwards, and RACI is finding that there are gaps in common approaches and tools for risk assessments.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level

The CoP is using a risk-based approach to prioritize the partnerships. Energy (SCADA vulnerability) was chosen as the first priority to improve collaboration between GC (law enforcement and others), the provinces/territories, which are responsible for energy security, and the private sector.

The main technique is capability assessment, and a mapping technique, which maps projects to outcomes and the three CCSS pillars. **Risk assessment is not an explicit part of this approach.**

e-Security Risk Assessment Capability Profile

b. Describe how the portfolio prioritizes and communicates risks within CSSP

The CoP has developed an **investment guide** that is based primarily on gap analysis techniques. The manager recognizes that the CoP needs to consider risk as a next step to support the identification and prioritization of projects that address operational priorities.

4. Major Challenges and Current Strategy:

A challenge is that there is no National Security Strategy, which is common to all CSSP initiatives:

a. CoP/Domain:

Power

The energy security risk management domain is mature in the private sector and at the P/T levels. There are many lessons to be learned from US counterparts, cross-border and North-South relationships at the regional level.

PS is supposed to be developing Sector Risk Profiles for critical infrastructure sectors. The e-Security CoP and/or RACI should probably review, if not provide risk advice on, the energy sector profile validation.

b. Portfolio:

It is not clear that CSSP has assessed the risks associated with the Sandbox concept, which is unique among the CoPs. To do this, CSS would need to interview stakeholders in the two sandboxes that are being developed. Examples of risk categories include: Management; sustainability (e.g., cost, information and knowledge management, relationship management, database and environment management); data sovereignty; and GC stakeholder capacity (e.g., resources).

5. Future:

a. What areas require more attention in the near-term?

The CoP manager identified the opportunity for RACI to brief the community, and explore options for applying a more systematic approach to risk assessment. This effort should start in the summer of 2014 when the ongoing four projects are completed. The level of effort is undefined.

Power (and Communications)

RACI probably does not have the capacity to break new ground in these areas. There will likely be opportunities to review Sector Risk Profiles that are part of the CIP CoP.

Money

Early RACI experience with the interdepartmental committee on AML/CFT is that while

e-Security Risk Assessment Capability Profile

the domain uses a so-called risk-based approach, there are different views of threat, vulnerability, control, consequence and risk assessments, depending on which group is doing the assessment and for what purpose.

Security (in general)

RACI will likely continue to support PCO-led DSO Readiness Committee on a best effort basis, which could include: review the risk portions of the DSO Handbook (risk is not well covered) and the role of risk in selecting future priorities.

b. Where could RACI add the most value in the near to mid-term?

CSS has not been directly involved in risk assessments or evaluating risk assessment capabilities in this domain. NRCAN, CNSC, AECL, TC, CATSA, CBSA and EC would have SMEs in different aspects of energy security; and threat, risk and vulnerability assessments but there is no common view of processes.

RACI /DSS should review situation after four ongoing projects are completed – summer 2014, and support CoP development of the way forward.

G.4 Risk assessment capability profile – Surveillance, intelligence & interdiction

SII Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Stephane Lefebvre, SII Portman

The CSS Portfolio Manager (Portman) supports two client groups:

- **Departmental Security Officer Readiness Committee (DSO RC)**, which is led by Privy Council Office (PCO) and Public Safety (PS), include DSO representatives from eighty (80) federal organizations. Department representatives have a variety of backgrounds (e.g., corporate or physical security, IT security, HR, policy). The group is focused on developing a consistent approach to security (risk) management across GC.
- **Security & Intelligence (S&I) community**, which includes projects that are co-sponsored by any of the forty-eight (48) organizations that have S&I roles. The PM works directly with S&T counterparts in organizations that have this capability. In most cases, the PM support PMs with a variety of experience and background (e.g., operations, policy, project management...). The proponents are focused on improving capabilities and closing gaps including management, technology and procedural controls. The CSS Portman adds value by identifying opportunities to leverage project outcomes across organizational and other boundaries. The value to CSS, even for limited funding, is significant because the lessons can be applied across CoPs.

Role: The PM provides S&T advice and project management support, including reporting within the CSSP management program (e.g., Quarterly Reports).

Scope: The scope of risk assessment work is focused on project risk management, which is the responsibility of the designated Project Manager (PM).

Decision Support: The Portman is not directly involved with the multi-criteria risk assessments that are part of the project lifecycle. However, the Portman does have unique insight into the value of the projects in comparison to other CSSP initiatives (e.g., balance of safety and security investments).

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

DSO RC – This community is promoting transformational change in how security services are managed across GC. It is developing tools to enable a whole-of-government approach to security. For example, the DSO Guide. Other references include:

- GC Harmonized Threat & Risk Assessment (HTRA)
- DSO Handbook (v4, 2013)
- TBS Operational Security standards (e.g., Readiness Levels; Physical Security; Management of IT Security; Business Continuity Planning Programs)
- TBS – Directive on Departmental Security Programs (DDSP)
- TBS – Integrated Risk Management; Management of Risk for Critical Infrastructure
- Departmental security and project risk management practices

SII Risk Assessment Capability Profile

- International and national standards and best practices (e.g., ISO 27001 Information security management system – requirements; ASIS SPC1:2009 Organizational Resilience; NFPA Z-1600:2013; CAN/CSA 31000 Risk management ; CAN/CSA Z1600)
- Industry best practices (e.g., Continuous risk management; PMBoK)

S&I Community – Visibility of risk assessment references used by this community may be more visible in other security-focused portfolios or CoPs.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

Examples of risks for projects in this domain include: projects are not fully-funded; the requirement changes before the solution can be implemented; and the sustainment costs exceed estimates. The risk tolerance level for S&I projects is relatively high. Furthermore, should CSSP not be able to contribute, then the operational departments would have the option to find alternatives.

DSO RC:

- The aim of this group is to improve consistency and quality of security services in GC. The group has identified 14 or 15 priorities. It is not known how risk informed the selection of these priorities.
- The community has not applied a capability assessment methodology
- CSS RACI has evaluated the applications of Architecture Frameworks to support this group

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

- The Portman monitors the project risk management practices, but is not directly involved in discussions of risk at either the project or operational levels
- The Portman has unique insight into the opportunities and risks associated with leveraging the project output among a broader community and identifying next steps

4. Major Challenges and Current Strategy:

a. CoP/Domain:

DSO RC:

- Historically, departments have developed their own approaches to security. If there has been any sharing of best practices, it has been on an ad hoc basis
- The RC is trying to stimulate change to eliminate duplication of effort and to improve the overall capability and value to the organizations
- Security is currently a fragmented and siloed capability (e.g., one department has invested millions in awareness; while another has invested zero; collaboration between IT security and physical security is still uneven)
- Specialists recognize that there are limitations to the legacy HTRA methodology and that there is little of no consistency across organizations. A logical way forward is to

SII Risk Assessment Capability Profile

transition towards a more holistic organizational resilience and/or security risk management framework. There are examples of this shift in some domains (e.g., IT security has shifted from the Certification and Accreditation, threat-based approach to a Security Assessment and Authorization risk-based approach).

S&I Community:

- This would require further investigation and probably, interviews with department PMs or project sponsors. A limitation would be the classification or sensitivity of department operational risk assessment processes.
- This remit is not part of the Portman or CSSP scope

b. Portfolio:

- There are no measures of effectiveness to evaluate the success of projects in this space or to enable comparative analysis of the value of investments in national security compared to federal investments in public safety or emergency management, which are the purviews of the Provinces/Territories.
- S&I departments have access to significant resources already. The value of CSS participation is three-fold: S&T advice especially in departments that have no integral S&T capability; early identification of risks, issues and opportunities related to leveraging the investment in multiple organizations; and access to information via CSS S&T networks including the defence, energy and other R&D communities that invest in SII S&T.

5. Future:

a. What areas require more attention in the near-term?

- **Portman** – Monitor how risk is addressed in project documentation including operational risk, and identify best practices, concerns or gaps, as part of the normal project management support workflow
- **CSSP** – Review CSSP guidance and tools for Portman’s and CoP leaders on project risk management including risk, issue and opportunity management, and the escalation process
- **CSSP** – Review potential for highlighting strategic and operational residual risk (i.e., after project completion), and describing the value of the project to mitigate these risks early in the project lifecycle or in the project prioritization process

b. Where could CSS add the most value in the near to mid-term?

- **RACI** – There appears to be an opportunity to apply a capability assessment methodology to the DSO RC initiative. The major limitation is the capacity of RACI to perform work in this area. Another possibility is to participate in the development of the next generation of security risk management frameworks and tools (e.g., replace the HTRA).
- **CSS** – There could be other opportunities to sustain the AF work or to apply OR support to optimize the security workflow in departments with diverse missions and resources.

G.5 RA capability profile – Critical Infrastructure Protection (CIP)

CIP Risk Assessment Capability Profile

1. **Context:** Describe the domain

OPI: Lynne Genik

CoP has been dormant for two years – way forward TBD

Ongoing project priorities – interdependency models and analysis; information sharing; and (lower priority) structural resilience

GC structure includes (based on 10 CI sectors, described in FERP and CISAP):

- National Cross-Sector Forum
- F/P/T CI WG (Murray Saunders) – PS has not shared information with CSS. WG is not representative of CI sector (public officials; not industry CI asset owners – 80-85% CI is owned and operated by private sector)
- Sector Working Groups (e.g., NR Can – energy; IC – ICT; PS – government, communications and safety)

PS web site has a CI Gateway for sharing information (UID & password-protected).

These groups identify gaps and priorities. It is not known how risk assessments factor into the decision making processes of these groups. Most decisions are based on bottom-up vulnerability assessments.

CSS has supported some P/T projects, but has limited visibility of risk assessment landscape. P/T have their own methods and risk assessment techniques to support of decisions on CI priorities:

- ON EMO – hazard identification and risk analysis (HIRA); ON also uses the federal Harmonized Threat & Risk Assessment (HTRA) guidebook for physical (and IT) security threat assessments; may be exposed to DHS tools in work on Windsor-Detroit corridor (?)
- BC – Justice Institute of BC (JIBC) / Alaska – using tool originally developed in collaboration with CSS OR team (for 2010 Olympics) and presumably DHS resiliency assessment tools(?)
- SK (CI Assurance Program) – own spreadsheet tools
- NB EMO/ Maine (did 3 sites) – using home grown spreadsheet and DHS tools (?)
- AB EMO – using home grown spreadsheet tools

Targeted Investments:

- **Polytechnique Institute** – work on framework for sharing information – sensitivity of data is a longstanding systemic constraint and industry concern (show stopper)
- **Interdependency and risk modeling** work using *RiskOutlook* tool

CIP Risk Assessment Capability Profile

PS was supposed to be developing Sector Risk Profiles but CSS has not seen any. The whole program could be shifting to resiliency and mapping to DHS RRAP and its associated tool sets.

Note: Ten Canadian CI sectors have not been updated, and in some cases, are ambiguous or are missing key sectors (e.g., S&T/R&D/education)

DHS RRAP CI priorities – water, energy and telecommunications (common points of failure for all sectors)

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

National Strategy (2009) and Action Plan (2014-2017) for Critical infrastructure: calls for PS to develop a national risk profile for CI, starting in 2014; to prioritize scenarios for high-impact; low frequency events (2014: 7); develop risk assessment products (2014: 8); and AH risk management approach.

<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx>

<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf>

Building Resilience Against Terrorism –

<http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/rsln-cgnst-trrrsm/index-eng.aspx> – no mention of S&T

Regional Resiliency Assessment Program (RRAP) – <http://www.dhs.gov/regional-resiliency-assessment-program>

- AHRA Framework Guideline, PS
- Federal Emergency Management Plan (FERP) – identifies CI sectors, and primary and supporting departments, PS
- Management of Risk for CI – TBS guide

ASIS SPC.1-2009, Operational resilience

Various EM and business continuity management standards and guides including CAN/CSA Z-1600 EM/BCM – updated in parallel with US-equivalent standard (NFPA 1600)

Risk Assessment Methodologies for CIP, Part 1: A State of the Art, JRC Technical Notes, EUR 25286, EN 2012, Joint Research Centre, European Commission, Italy, 2012 – 19 RAMs for CIP – not been evaluated by Canada

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

- Describe how the domain prioritizes risks and presents recommendations to next level:**

CIP Risk Assessment Capability Profile

At the Federal level, PS promotes the application of All Hazards Risk Management. However, the reality is different as the P/T level where public and private stakeholders use a variety of techniques and tools. CI sectors use their own toolsets, and there is no overall view of these processes. CSS is in a fact finding and monitoring role, except for a few projects and Targeted Investments (TI's).

Virtual Risk Assessment Cell (VRAC) created to support Government Operations Centre (GOC) – also believed to be supporting CI sector risk assessments

(DHS) RRAP is building a database of site assessments – CA situation is not clear

Various techniques include:

- Threat and Hazard Identification and Risk Assessment (THIRA) – DHS RRAP term
- Hazard Identification and Risk Assessment (HIRA) – ON term
- Vulnerability Assessment
- Resiliency assessment
- Dependency assessment

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

TBD – overlap with several communities; Public Safety fragmented organization; limited CSS resources...

4. Major Challenges and Current Strategy:

a. CoP/Domain:

Techniques and processes – P/T are using a variety of spreadsheet tools and mathematical formulas to combine variables. P/T EM organizations are not necessarily applying rigorous analytical techniques to verify the accuracy of the tools. **Potential problems include:** incorrect mathematical formulas; missing important variables; double accounting of factors / effects; inaccurate weighting; combinations of linear and logarithmic estimates – mathematical errors; etc.:

Implications are that P/T decision makers are being given information that is incomplete or inaccurate, and they do not have a true picture of capability gaps or risk exposure, which leads to wasted investment or some sectors being given resources when they do not need them. A national CI program should pick such inconsistencies, but it is not clear that PS is asking the right questions or perceives that it has the mandate (e.g., independent verification and validation) to intervene or to recommend that P/T partners perform IV&V / third party reviews of risk assessments as part of federally-supported projects. (IB)

PS could be putting together national risk pictures that are based on flawed P/T pictures. There is no overall view of risk assessment techniques being used across Canada. The PS survey may shed some light on this area, but the structure of the survey, and the rate and quality of responses are unknown. (IB)

CIP Risk Assessment Capability Profile

Interdependency modeling – DHS has tried, and this is a difficult and labour-intensive problem

Investment – CA has assigned limited resources to manage a voluntary CI program. Adopting DHS models and tools could have resource and other implications for Canada

Structure & Capability:

- GC – global limitations include Canada’s geo-political and legal structure; PS authority and organizational structure; PS resource capability and capacity; science-based departments’ S&T capability and capacity (and lack of a national S&T vision); and national security strategy)
- P/T – lack of analytical capability to support use of tools; risk of reliance on flawed assumptions and tools

b. Portfolio:

Limits to success include: complexity of CI community of communities; CSS two-year gap (lessons for continuity and KM?); single CSS resource; overlap with other portfolios and CoPs; pressures on C SSP budget; working relationship with PS (pull system to get relevant information); and resource constraints of RACI (3) and DSS (5)

5. Future:

a. What areas require more attention in the near-term?

- Review survey of P/T CI programs – CSS requested a copy
- There may be value in PS/CSS defining a requirement for third party evaluations of risk assessment tools as part of future investments in P/T initiatives
- Monitor DHS RRAP success stories (e.g., risk assessment; measures of effectiveness; dashboards)
- Monitor Alaska cross-border, DHS RRAP, phase 1 (2014)

b. Where could RACI/DSS add the most value in the near to mid-term?

- Review lessons from P/T use of existing spreadsheets and DHS RRAP CI tools
- Review mandate, capability and objectives of VRAC
- Monitor results of interdependency and risk mapping project (Canadian RRAP)
- PS CI Gateway – review/monitor PS guidance on risk assessments (Is it based on DHS RRAP toolset? What are PS plans to develop tools?)

G.6 Risk assessment capability profile – Fire service

Fire Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Dave Matschke – Fire Portfolio / CoP

The Canadian Fire Community of Practice (Fire CoP) was created in 2012; focus is on threats to communities handled by fire services. Goal is “to identify the required knowledge and technology that will reduce the personal, socio-economic and environmental impacts of fire (and all emergencies) through the anticipation, prevention and mitigation of hazards.”

CSS approached CAFC (Canadian Association of Fire Chiefs) with a proposal to put a Fire Community of Practice together. Two original meetings were held between CSS and CAFC, to develop the business plan, membership list, etc., which consists of roughly 14-15 reps from across Fire Services.

The membership of the Fire CoP consists of subject-matter experts in fire-related matters such as firefighting, prevention, recovery, education and instruction, research, and engineering.

Membership (stakeholders) in the Fire CoP includes reps from: NFPA (National Fire Protection Association), Underwriters Laboratories Canada (ULC), CAFC, industry (mine firefighting), CIFFC (Canadian Interagency Forest Fire Centre (CIFFC), labour, CCFMC (Council of Canadian Fire Marshals and Fire Commissioners). A diverse, wide-ranging group with lots of ‘opinions’ on risk and risk assessment.

Current Community Development projects:

- Project to help define the priorities for the development of a **national fire research agenda** (see contractor report) Stakeholders include PHAC, HC, CFIA, AAFC, TC, CATSA, NRCan, P/T, industry, medical and PH service providers, etc.
- Project to develop a **national evidence-based policy manual**

There is recognition in the Fire Portfolio of the need for more than just expert opinions to identify risks and associated capability gaps/priorities.

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

1) Report on the **Intermediate S&T Priorities** of Canadian Fire Services. Survey of all fire service agencies across Canada; ~250 responses out of 3000. The output has been a list of priorities from survey responses and rankings to a series of questions. These outputs have been documented in a report. The list of priorities is intended to be generic; and the scope was kept at a national (pan-Canadian) focus versus at the tactical level.

2) **Framework for writing policy** for the fire services – seeks to create a common view of policy development, towards a guideline/manual for policy development.

Fire Risk Assessment Capability Profile

Assessing risk is difficult in light of the fact that municipalities fund fire service agencies and decide on allocation of resources, placement of assets, allocation of budgets, etc.

Risk and hazard identification (e.g., loss of life, destruction of property) are inherent elements of the fire department and their response process. However, that is done at the operational level in response to an event or emergency, and not the product of a deliberate planning process performed by EM planners with decision support tools or techniques.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

At the provincial level, coordination is slightly better with the introduction of HAZMAT regional teams and (in some cases) CBRN response assets (e.g., Atlantic/New England/Maine sharing of resources for HAZMAT preparedness and response). Beyond that, there exists little to no coordination of equipment or response among the multiple jurisdictions. However, there are individual Mutual Aid Agreements between services and departments (e.g., dispatching services), but nothing comprehensive exists on a national basis.

The level of resources devoted to performing a separate risk analysis/risk assessment is a function of the size of the community involved. Smaller fire services do not have a lot of resources available to perform risk assessments, and the capabilities that are acquired may not be based on a valid need or functional requirement.

A better approach to risk assessment is needed in order to be able to validate requirements versus focusing on an equipment replacement strategy.

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

Tri-Services and National Leadership CoPs: tried to identify **common areas** between the portfolios/communities of practice. Leadership of the four CoPs and four Portfolio Managers sat down together as a group to identify ideas that could be applied to all four areas (Fire, EMS, Law Enforcement, National Leadership, etc.).

Focus was on interoperability and common areas that applied across the board, given the reduction in funding for all areas. Again, no formal process; informal, largely subjective, non-rigorous or empirical, but based on informed (expert) judgement. The results of this meeting have been documented.

4. Major Challenges and Current Strategy:

Given the high costs of providing fire services to municipalities, there is an increasing trend that municipalities are starting to question why fire service agencies require 'X' amount of resources. If the cost of fire services are 'X', and the amount of damage is 'Y', then how much

Fire Risk Assessment Capability Profile

fire services does a community really need? Is it cheaper to pay insurance costs instead?

And why are municipalities paying so much money for fire services if they are only getting ‘Z’ calls per year? This situation is forcing fire service agencies to justify their resource allocation plan.

Risk is becoming a key part of the area/jurisdiction that needs to be serviced.

Provincial Hazard Identification Risk Assessment (HIRA): highlighted the City of Ottawa Risk Assessment, but nothing exists at the national level.

5. Future:

a. Opportunities

Framework – CoP membership could use methods/models to help them prioritize and rank their greatest risks in a more systematic and repeatable manner. It’s not the lack of issues that’s the concern, but the absence of an overarching method to rank risks. There’s always a great deal of polarization depending on the individual or group – need to mitigate the bias by creating a coherent structure that allows for the application of judgement, and allows the Fire CoP to seize opportunities.

(Comment RACI: Not at the maturity of Capability Assessment/CBP yet)

G.7 RA capability profile – Paramedics

Paramedics Risk Assessment Capability Profile

1. **Context:** Describe the domain

OPI: Doug Socha, Paramedics CoP Manager

Paramedic Chiefs of Canada (PCC) – <http://www.paramedicchiefs.ca/>
Annual conference (next June 11-13, 2014, Vancouver)

Paramedics Association of Canada (PAC) – <http://paramedic.ca/>
National Occupational Competency Profile (NOCP) for paramedics practitioners, 2001
Annual conference

Areas of interest include: **national standards** project (national framework for standards, with CSA participation); **national gap analysis** (with CPRC); **competency** profiles (with PHAC); physical work analysis (with two universities; ergonomists); **national database** with clinical information, which can be extended in future to capture performance data; **community resilience** (expanded role for paramedics because of local situational awareness and trust within community; social media; and training to deal with mental health.

CONOPS – solid baseline of documentation to support priorities and recommendations; and leverage jurisdictions that have overcome structural, financial and other obstacles to implement pilot / demonstration projects, and then, leverage success and communicate lessons to other jurisdictions.

Environment challenges:

- Governance – many “influencers” – chiefs; associations; medical professionals; local and provincial politicians; educators; providers; security, safety, health and emergency management specialists; lawyers; policy makers; consultants; lobbyists; regulators...
- Communications (opportunity and challenge – two streams):
 - Public safety (PS), but PS dominated by security and EM)
 - Public health (HC, PHAC), but dominated by physicians
- Operational communications – 7 dispatch centres in ON – managed by performance agreements – what are measures of effectiveness (MoEs) for dispatch (not controlled by EMS)?
- Evidence-based data versus looking forward – may not consider future risk enough
- **Lack of national policy and strategy**
- Changing roles of professionals, nurse practitioners, paramedics, care service providers..., and implications for future of EMS
- Funding – EMS is downloaded by provinces to municipal level; many different models (e.g., NFP; ON province MOHLTC owns dispatch, but City EMS manage resources, and there are cross-border constraints on, and liability issues for, what paramedics can do in ON or QC)
- Historically EMS has not had a national voice
- **SOREM has no municipal representation** – does not consider EMS issues and

Paramedics Risk Assessment Capability Profile

challenges – for ON, MOHLTC at table; Office of Fire Marshall (ON rep)

- Many **organizational models**: cooperatives; contracted services (e.g., Atlantic Canada – Blue Cross; NB, NS and PEI three private companies); part-time and full-time resources; different standing orders, even in the same organization
- No **national standards** (e.g., ambulances, equipment, training, certification, operations, dispatch)
- Air medical transportation is one of 54 services in ON, and yet, all institutions depend on this one NFP service

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

Priorities are based on bottom-up analysis of known deficiencies and capability gaps. Specialists use all hazards emergency management risk analysis and hazard analysis techniques. CSS does not have visibility of methodologies or techniques, other than because of Portfolio/CoP manager's experience.

Significant body of work that documents priorities including:

- Canadian National EMS Research Agenda, Emergency Medical Services Chiefs of Canada (EMSCC) and Paramedics Association of Canada (PAC)
- EMS Priority Gap CoP Map (strategic goals)
- Gap Analysis for EMS, S&T Research, CPRC #09-1076; DiMonte, D., Premergency Inc, ON, 2012:
 - Note: of 40 survey questions, there were none related to organizational or operational risk assessment or risk management
 - National EMS research does focus on evidence-based decision making
- Methodology for the development of a national EMS research agenda, BMC Emergency Medicine, 2011
- The Canadian National EMS Research Agenda: a mixed methods consensus study, Jensen, J. et al; Canadian Association of Emergency Physicians, Canadian Journal of Emergency Medicine (CJEM 2013; 15(2):73-82
- The Future of EMS in Canada, Defining the New **Road Ahead**, EMSCC, Calgary, 2011

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

This new community has established an information baseline to support future work, which includes (consultant's comments in italics, in brackets):

- CoP map of priorities
- Reliance on evidence-based decision making (*risk management not explicit in prioritization process – potential blind spots?*)
- Priorities based on solid body of work that engaged associations and frontline resources

Paramedics Risk Assessment Capability Profile

Capability and risk analysis are **implicit** in the process, which means that some risks could be missed (i.e., not a rigorous or transparent process).

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

- Techniques for communicating strategic and operational priorities

4. Major Challenges and Current Strategy:

a. CoP/Domain:

- Have good grasp on priorities for projects at strategic and operational/tactical levels – could be **best practice** for other CoPs – solid information baseline for future work
- Communicating the value of EMS investment compared to other CSSP investments in security
- Bureaucratic and other systemic constraints on implementing cross-jurisdictional projects that lie outside the remit of federal departments

b. Portfolio:

- No visibility of capability assessment methodology or (AHRA) scenario-based workshop experience (RACI in support of PS and interdepartmental working group)

5. Future:

a. What areas require more attention in the near-term?

- Evaluate *EMS Priority Gap CoP Map* process and visualization technique as a potential best practice for CSSP (consider how to include value and risk mitigation factors, and MoE, over time?)
- How to communicate value of investments (engage DSS and RACI – see Jack’s EMSI profile)
- **Economic modeling** – in support of future paramedics role and options analysis – reduce load on hospitals; improve community resilience and trust in medical system

b. Where could RACI add the most value in the near to mid-term?

- CoP / RACI – consider role/place of risk management training in leadership development (e.g., refer to: Gary Klein, Cognitive Task Analysis research)
- RACI – Review EMS documentation, identify potential role for risk and capability assessment
- RACI – consider options and feasibility to become more engaged (e.g., brief CoP on capability assessment methodology; scenario work; architecture framework...)
- RACI/DSS – consider scan and potential work on MoEs – call volume; response times; consider “chain of care” of patients; governance models...
- Decision support – engage with DSS to review organizational models
- Future – consider options to leverage analytics technology to complement database work
- Futures research, using road ahead as a baseline, more research into:
 - **Expanded role** for paramedics because of local situational awareness and trust

Paramedics Risk Assessment Capability Profile

within community

- **Data sharing between hospitals and EMS, and data analytics**
- Central DB and process for capturing and analyzing lessons learned from municipalities and regions

G.8 RA capability profile – Law enforcement

LE Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Sheldon Dickie, LE CoP Manager

Focus: Big 5 operational LE departments (RCMP, CBSA, EC, HC, TC)

Emerging best practice:

- Experience / framework for considering financial loss and cascading effects on community and society
- Potential to leverage / expand previous AHRA, scenario and OR work, including spreadsheet tools to support group factor-based evaluation using voting technology

CoP objectives (near-term) – leverage regional projects to advance CSSP strategic objectives and evolution. Provide building blocks for pan-Canadian improvement in LE capability to realize benefits and value at a national / societal level. Extend lessons and concepts to other CoPs and portfolios, and the way CSSP selects investment priorities, including a more consistent approach to the analysis of socio-economic impact and consequences.

Protect 1: Atlantic Canada All Hazards (AH) HAZMAT – builds on RACI CRTI experience. Project includes strategic plan and risk scenarios. Four provinces and adjoining states are participants. Risk- and scenario-based planning model. Developing evidence base including: socio-economic impact data (loss associated with flow of goods, information and people); description of value of LE response and protection of assets (ROI); and value of risk mitigation.

Project 2: NB Emergency Response Team (ERT) – Risk- and scenario-based approach including active shooter scenario. Documenting evidence base and value of skilled responders. Leverages early CSS OR work on capability-based flow chart and security multi-criteria risk analysis. Includes loss analysis (weak link in existing security and other risk assessment processes).

Project 3: PEI (not funded in recent Call).

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

Leveraging CSS work on AHRA, scenarios and capability-based planning. Documenting approaches to loss analysis (contracted regional resources who understand economic environment and pressures).

LE community historically focused on threat. Trends is towards more emphasis on target and effects (impact) including quantification of financial impact on community and business – wellbeing of public; link to City planning; value of policing...

LE Risk Assessment Capability Profile

DHS references are mainly threat-based.

GC – weaknesses include mandate-focused risk analysis. Operational departments have good information on threats, but there is no holistic view of risks at a regional or national level.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the CoP prioritizes risks:

The community is using risk assessment template, version 22 (CSS, 2013), which is posted on PS web site. It has included (*socio-economic impact*) loss analysis in projects since 2012 because the impact of security incidents is not just loss of life. It is also about the impact on the economic well-being of communities. The CoP usually gets input from Finance Canada or by contracting with regional SMEs.

Spreadsheet tools are used to investigate multiple factors. The assessments are factor-based, not threat- or risk-based assessments. The projects have experimented with voting technology.

Factors include: threat; target; people; investors. The technique builds on early RACI and OR work (Goudreau, A, and Verga, S., 2009-10).

Sample project – Delphi approach / Factor-based voting:

- Lower mainland BC project
- 2 sessions
- 60 participants
- Vote on factors (not risks)
- Discussion
- Vote again (repeat as necessary)

Multi-dimensional assessment process:

- Threat-based analysis
- Target-based analysis
- Cascade effects analysis; and link to
- Enterprise Risk Management – working with City level SMEs:
 - Ottawa – link to strategic / City planning – trade-offs between purchase of police equipment versus spending money to increase tourism
 - Ottawa – infrastructure decision that disrupted 4-lane highway – quantification of cost impact
 - Richmond – decision to transport fuel to airport (pipeline – road – rail)
 - Yukon – Ottawa working with Yukon on automated tool for risk analysis

Real world examples of decision that increased risk to local communities and business include:

- Liquid Natural Gas (LNG) plant located near hospital. Decision makers focused on tax revenue and employment.

LE Risk Assessment Capability Profile

- Smiths Falls – listeriosis outbreak elsewhere, but local decisions put 700 jobs and community economic survival at risk

Used factor-based voting tool for Windsor-Detroit Gateway, trans-Canada railway and Great Lakes (GL) projects.

Success story – RCMP and US police on same boats in GL – significant improvement in enforcement capability.

b. Describe how the CoP prioritizes and communicates risks within CSSP:

No systematic process within CSSP. No common set of tools to assess socio-economic impact of decisions / projects / capabilities / S&T investments.

4. Major Challenges and Current Strategy:

a. National / Societal Resilience:

Systemic constraints – federal department risk assessments are constrained by mandates, PAAs, and current practices and compliance mindsets; central agencies have no remit or authority to simulate transformational change to achieve national impacts (PCO, PS, TBS); resources and common frameworks to sustain multi-agency, cross-jurisdictional initiatives; and capability to describe and compare risks, value, benefits or loss across or within regions.

Tension in system – constraints at F/P/T levels work against creating real value at the tactical and local level; dependent on local and individual initiatives that are prepared to take risk and swim upstream with uncertain outcomes.

b. CoP:

Local initiatives bump into road blocks that can only be solved at local and regional level. GC has few mechanisms to intervene. Successes at local and regional level are difficult if not impossible to sustain and exploit nationally because of system constraints and lack of tools including socio-economic impact (e.g., benefit or loss modeling).

5. Future:

a. What areas require more attention at the CSSP management level in the near-term?

Document – experience / framework for considering financial loss, and cascading effects on community, region and society.

Lessons learned report / Case Study – Provide recommendations (way forward paper) to build on outputs of ongoing regional projects (i.e., that support multijurisdictional / cross-border / regional risk- and scenario-based assessments, capability-based planning and CSSP decision support).

LE Risk Assessment Capability Profile

Risk assessment core team – establish a CSSP working group that reviews risk as an integral part of CSSP management regime (e.g., section heads) and provides advice to team.

Develop common approach for project planning deliverables to include: strategic plans and operational risk scenarios.

Review lessons learned at local level and develop a common strategy to exploit successes.

b. Where could RACI/DSS add the most value in the near to mid-term?

RACI /DSS – Develop CSSP decision support toolkit as part of a managers' guidebook including Delphi, risk assessment and other techniques that include a (CSSP investment) impact analysis framework, and assess options for modeling **socio-economic loss and value**, and other factors at local, regional , national and transnational levels.

RACI/DSS – Review portability and sustainment of spreadsheet tools, and recommend way forward.

G.9 Risk assessment capability profile – CBRNE Forensics (CBRNEF)

| CBRNE/F Risk Assessment Capability Profile |
|--|
| <p>1. Context: Describe the domain</p> <p>OPI: Norman Yanofsky, A/Section Head (Note: Creating separate profiles for each domain is an option)</p> <p>The section staff manages projects and communities in the following domains:</p> <ul style="list-style-type: none">• Chem/Bio – this is perhaps the most complicated domain because it includes: health; medical countermeasures; major infectious disease outbreaks; protection of responders; transportation of dangerous goods, an emerging priority because of recent rail and pipeline events; food and water security; industrial accidents; and supply chain integrity. Stakeholders include PHAC, HC, CFIA, AAFC, TC, CATSA, NRCan, P/T, industry, medical and PH service providers, etc.• Rad/Nuc – this domain is mature and well understood, although it is dynamic and has a broad science stakeholder base including: P/T; energy service providers and utilities; responders; and emergency / incident managers• Explosives – S&T support related to IED, suicide bomber, industrial accidents and radicalization• Forensics <p>Each domain has its own CoP and competes for CSSP investment through the Call process. CBRN is mature, and includes international agreements, standards, protocols and procedures (e.g., NATO MOU)</p> <p>This subject area interconnects with multiple portfolios and CoPs including: SII; Tri-Service; EMSI; e-Security; and Critical Infrastructure Protection</p> |
| <p>2. Risk Assessment References (directives, guidelines, frameworks, standards...):</p> <p>CSS has a mature Consolidated Risk Assessment (CRA) methodology that has been applied to CBRN. The output depends in intelligence and is normally classified (Secret and above)</p> <p>The RACI Section, in collaboration with CBRN SMEs, facilitates the CRA process to identify and differentiate threats, hazards and risk exposure using expert elicitation and interdisciplinary workshop techniques. The future of the CRA process is not clear for three reasons:</p> <ul style="list-style-type: none">• CBRN continues to evolve and include new areas of expertise and assessment techniques• Production of the CRA report is time consuming• CSS and RACI have limited resources to dedicate to this activity <p>Assessing the value, tailorability and/or sustainability of the CRA process was not in the scope of the Risk Scan project</p> |

CBRNE/F Risk Assessment Capability Profile

References are domain-specific, and encompass a wide range of: international, national and industry policies, regulations, standards and protocols; and governance, risk management, compliance and liability regimes. **A detailed review is not in scope, and they are not listed in this profile to save time.**

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

Threat, hazard and vulnerability assessments are an inherent part of the CBRNEF capability and requirements prioritization process. The assessments are mainly the output of a bottom-up process that is performed by the SMEs.

The level of independent validation and engagement of other levels of management and external stakeholders within specific domains was not assessed as part of this project.

In the past, CSS has used the CRA process to combine threat assessments for CBRN. However, the **risk assessment environment has changed dramatically since the CRTI timeframe**. Historically, the focus was mainly on the terrorist threat, and understanding threats, hazards and vulnerabilities. The focus is now broader and includes infectious **disease outbreaks and industrial accidents**. The teams are spending more time on understanding the **target and effects** (e.g., consequence management and resilience). This trend is consistent with transitioning to a more holistic view of risk exposure, which suggests that the CRA may not be applicable, and there may be an opportunity for other unifying approaches.

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

Prioritization depends on knowledgeable CSS staff, a clear description of CSSP priorities, and the motivation and commitment of willing stakeholders.

4. Major Challenges and Current Strategy:

Whole of Government:

The CBRNEF experience is that a **major challenge is communications** within and across the stakeholder communities, which includes: scientists; engineers; regulators; operations managers; and policy analysts. This interconnectedness extends to all levels of government, and engagement of specialists in the private sector, academia and international community. These trends have CSSP implications including recruitment, retention, administrative, and information and knowledge management support of CSS staff.

Accountability is recognized as a common challenge, concern and systemic risk across jurisdictions.

CBRNE/F Risk Assessment Capability Profile

Chem/Bio:

There focus for this community has shifted dramatically from detection, prevention and protection [e.g., technology; Personal Protective Equipment (PPE)] to the understanding of **effects** of threats/hazards on specific target groups including vulnerable communities (e.g., the North, infant care, etc.) to differentiate risks and capability gaps.

CBRNEF:

Areas of potential concern include: the availability of intelligence to the non-federal community; and the ability to compare priorities across regions because of diverse risk perception and risk assessment approaches.

5. Future:

a. What areas require more attention in the near-term?

CRA

RACI should investigate if there is value in developing a streamlined approach to the CRA or a successor that expands the assessment of the target. Because of the diversity of the threats hazards, vulnerabilities and “targets” within the **Chem/Bio domain**, this would be a logical future application for a uniform process to prioritize risks, to complement not duplicate domain-specific threat assessments, and preferably, with a focus on systemic and interconnectedness risks.

CBRNEF / CSSP

Given the shift in focus and scope, it may be useful for CSS to review the trends in:

- Balance of technology and other investments
- Balance of security and safety investments
- Stakeholder engagement (e.g., is the number of potential bidders increasing, decreasing or staying the same)
- CoP stakeholder, Call bidder and F/P/T/M/FNI partner satisfaction (e.g., procurement efficiency; intelligence sharing; communications)

CSSP

There may be value in RACI, in collaboration with other (e.g., decision support) developing a **glossary of risk terminology** and providing input to the CSSP portfolio management guidebook on capability and risk assessment, and other unifying decision support techniques.

b. Where could RACI add the most value in the near to mid-term?

CBRNE/F Risk Assessment Capability Profile

CBRNEF

The main source of risk expertise is the SMEs in the different disciplines. There should be value in developing a compendium for discrete domains or across this portfolio to identify best practices and gaps in knowledge or tools.

RACI can add value by investigating techniques and tools to help CSS staff and CoPs to: compare federal and regional stakeholders' perceptions of risk priorities; evaluate risk assessment approaches; and to develop toolkits (e.g., futures; scenario planning; measure of effectiveness; investment prioritization; and capability assessment).

Although it is probably not practical or useful for RACI to develop a compendium of techniques across CBRNEF domains, there may be value in performing a SWOT and benchmark analysis of risk assessment capabilities in direct support of **Chem/Bio**.

CRA

Chem/Bio would be potential candidate for a future CRA. However, it is likely that the process should be more streamlined and iterative to conserve resources. It may also be feasible to take a two-step approach – fast assessment using open source intelligence, and then, more detailed assessment using classified information. There may also be potential to leverage *crowdsourcing* and other technology solutions (e.g., *Shaping Tomorrow*) to engage broad communities on an ongoing basis.

G.10 RA capability profile – EMSI and psychosocial

EMSI/P Risk Assessment Capability Profile

1. Context: Describe the domain

OPI: Jack Pagotto, Emergency Management System Interoperability (EMIS) and Psychosocial

Community of Communities of Practice (model):

- EMSI – 3 CoPs; 3 portfolios
 - Communications (Wireless – 700 MHz; Public Alerting – next generation 911 – NG911)
 - Situational Awareness (e.g., MASAS; tsunami alerting; EM resource tracking; mutual aid agreements...)
 - Interoperable Information Exchange for EM (IE architecture, SAMSON)
- Psychosocial

Concept – CoPs are self-forming and self-sustaining. CSS has many F/P/T/M touch points (e.g., National Alerting; Sub-committee; Federal SOREM Interoperability WG; Federal EOC Working Group (currently 37 federal EOCs); Tri-Service EM Committee (Toronto, Ontario; Information and Communications Technology (ICT) federal and municipal WG of CIOs.

Canadian Association of Chiefs of Police (CACP) – CITIG Workshop

National interests include: wearable video; social media (in support of policing; evidence of video to support investigation and prosecution)

Communications Research Centre (CRC) Technical Advisory Group (700 MHz) – 6 CRC engineers; one CSS FTE

Operations Centre Interconnectedness Portal (OCIP) – SharePoint – information sharing hub; PS GOC

Quebec – has MASAS; used during Lac Megantic rail disaster

Conference Board of Canada – mentioned Lac Megantic – lack of air sampling technology and protocol; lack of ICS...

2. Risk Assessment References (directives, guidelines, frameworks, standards...):

EM:

SOREM – varies by province. Arctic, NL and PEI do not have dedicated teams

Focus is mainly on after-action reviews after real incidents (e.g., Lac Megantic rail disaster; Albert flooding; 2013)

EMSI/P Risk Assessment Capability Profile

EMSI experimented with **voting technology** to score the significance of project / requirements, and to get consensus from policy and operational SMEs on priorities (not as part of a risk assessment). OR and RACI were not involved. Risk was not part of the exercise.

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

EMSI leverages the annual symposium to do facilitated brainstorms on gaps and priorities. Risk is implicit in discussions. In 2012, CSS trialled an automated voting tool (Expert Choice), but it has not been exploited further in CSS. Historical examples include:

- Health Canada – EMSI observed an exercise that identified the top 10 gaps. Risk was not an explicit part of the process
- Detroit-Windsor Corridor (CIP) – a scoring technique was used a few years ago, but it has not been operationalized or exploited across CSS

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

Risk assessment is a bottom-up process. CSS has limited visibility of techniques and tools that are used by federal partners, and virtually no insight into techniques being used at the P/T and municipal levels, or in the private sector. The primary focus is on addressing known deficiencies. The process is dominated by recent events, and AAR's.

Therefore, CoP priorities are selected using best judgement, and priorities are presented to CSSP without an assessment of risk, or more importantly the value of the project in terms of improving capability.

4. Major Challenges and Current Strategy:

a. CoP/Domain:

- **Strategy** – leverage OGD S&T capabilities (e.g., CRC); collaborate with US DHS, FEMA and bordering states and SME networks (e.g., firefighting)
- **Value** – the major challenge is being able to identify, describe and compare the value of proposed CSSP investments
- **EM** – lessons learned and AAR's are the primary means to identify and prioritize requirements. There may be value in reviewing P/T/M (regional) best practices, and identifying some common tool and techniques including to support risk-based approaches and improve consistency across borders and stakeholder communities.
- **Resilience Concept – 3 general capability areas:**
 - Systems and planning
 - SA modeling
 - Response of governance (e.g., Katrina – governance gridlock; rail safety standards weak; Hurricane Sandy – state of SA capabilities)

EMSI/P Risk Assessment Capability Profile

Challenge – Measure outcome of resilience improvements?

b. Portfolio:

• Communications:

- What if PS does not auction off 20 MHz; may not have compatibility with US emergency services; next steps are not clear
- Standards or wireless cell phone alerting
- Air operations coordination – concern for wild fires; no SA to allocate resources in near-real time

• EM Interoperability remains a high priority (e.g., Megantic and Alberta Flooding AARs):

- Pilot projects expensive (US has seven pilots – \$100M each; CA has difficulty getting one 2-3 year pilot for \$50M)
- PS Interoperability Development Office (IDO), PS – Stephanie Girard

• Identity, Credentials & Access Management (ICAM):

- Dynamic identity management, accreditation of users and authorization on networks
- Next CSSP Call includes projects in this area – existing solutions are very expensive (e.g., IAM architecture, SSC; Oracle; Open Stack, TBS)

5. Future:

a. What areas require more attention in the near-term?

- OR should investigate options for describing the value of projects / outcomes, and monitoring and measuring CSSP ROI over time
- OR and RACI should get involved in evaluating the use of automated decision support technology to determine how to exploit this capability for other CoPs and CSSP
- Review need for common view of resilience and techniques to describe and measure improvements
- Fire – unable to share data across provinces
- Quebec – lack of ICS during Lac Megantic response

b. Where could RACI add the most value in the near to mid-term?

- Review paper, “Value-focused Investment Framework”, Greg Luoma study
- Review use of scenarios and capability assessment methodology in support of EM communications and other CoPs, possibly, including scenarios during annual workshops (e.g., to set scene for using voting tool)
- Investigate Consolidated Risk Assessment (CRA) for communications or other CoPs
- Consider value of a compendium of regional after-action review processes (and role of risk assessment in prioritization of deficiencies and investments)

G.11 RA capability profile – Knowledge, technology & community safety

Knowledge, Technology & Community Safety Risk Assessment Capability Profile

1. **Context:** Describe the domain

OPI: Colin Murray, Director Knowledge, Technology & Community Safety

Four key resources with significant knowledge, experience and networks – fire, police, paramedics and strategic leadership

KTCS emerging priorities include:

- Build sustainable relationships
- Communicate success stories and impact/value of investments
- Shift focus from threat/ hazards to impacts (and implicitly more holistic risk management practices)
- Manage relationship with DRDC to protect budget and flexibility

Focus includes:

- Tri-Services, EM, crisis management, resilience
- Evidence base for justifying future investments (central database, etc.)
- DRDC transformation and potential impact on CSSP

Major Initiatives:

- **Emergency Responder Test and Evaluation Establishment (ERTEE)**, Regina (14 FTEs; with university and RCMP depot) – originally funded by Canadian Innovation and Commercialization Program; CPRC was historically focused on regional level, not national:
 - Builds on CAE simulation studies
 - “Living Lab” – Physiology measurement research
- **Technology Innovation Action Plan (2012)**
- **Full Circle Community Safety Model (2012)**

CSS Stakeholders include: Support to Operations cell [exercise program; support to deployed operations; reach back (to S&T); and support to federal operations planning]; Tri-Service; EMSI; others

2. **Risk Assessment References** (directives, guidelines, frameworks, standards...):

Technology Innovation and Action plan includes the principle: risk management and outcome-based

Community recognizes need to improve risk management practice within the CSSP, without adding overhead

Knowledge, Technology & Community Safety Risk Assessment Capability Profile

3. Risk Assessment Capability Maturity (See attachments 6 & 7):

a. Describe how the domain prioritizes risks and presents recommendations to next level:

There are no structured or formal mechanisms to communicate risk internally (ad hoc process). This is a concern because of: rapid growth; increasing competition; shifting CSSP priorities; budgets constraints; etc.

Knowledge, Technology & Community Safety and related CoP/portfolios face common risks both internally and within the overall CSSP direction. If risks are not considered during the development of strategic planning guidance, then there could be a missed opportunity to lay the groundwork for a more systematic approach to risk management.

Two trends are highlighted:

Trend 1: Risk information – More strategic focus, including on risk information. Broader responder community is shifting focus from just threats, hazards and vulnerabilities to understanding impacts, consequences and risk exposure on multiple levels, not just their own discipline or mandate. Community recognizes imperative to communicate more effectively with stakeholders including: local politicians, councils, unions, associations, academia, private industry, training and certification establishments, cross-border partners and the public.

Trend 2: Impact – Responder cultures are recognizing need to focus more attention on impact dimension.

b. Describe how the portfolio prioritizes and communicates risks within CSSP:

TBD

4. Major Challenges and Current Strategy:

a. CoP/Domain:

- **Major challenge is evidence base** (factual information, including risk information) to support decisions and justify investments for a diverse stakeholder audience:
 - Need balance of evidence-based (quantitative) and forward-focused (qualitative) risk perspectives
 - Scenarios should help (e.g., local and regional levels)
- **Communications:**
 - **PS** – is more concerned with federal policy cover, which is not directly related to this capability, which is P/T/FNI jurisdiction. Probably need communications strategy for a variety of audiences including PS policy analysts – describe value of investment (ROI) in terms that relate to PS mandate, policies, strategies, action plans, etc.
 - **Governance** – directors and sections heads do not have consistent methods to communicate risk and value of the program to internal decision makers and to:

Knowledge, Technology & Community Safety Risk Assessment Capability Profile

- Steering Committee (PS, CSS partnership)
- Program Review Board
- Advisory Board (non-federal)
- **Strategic Relationship Management** – if CSS loses confidence of frontline participants, then past achievements could be at risk, and the ability of CSS to achieve its strategic objectives in the community safety and resilience areas, could be jeopardized.
- **Dependency on 4 key Resources** – without commitment and affordable funding mechanism for four key resources, credibility, relationships and the knowledge base are at risk:
 - Historically, funding was O&M – more flexible budget and more CSS control
 - Now Salary Wage Envelop (SWE) is at risk
 - A-Base used to be protected. Now is it open to DRDC influence (FY 2014/15 – ADM DRDC took \$3.1M – precedence?)
 - Some participants have to take holidays and pay their own way to attend meetings
 - Cost of SMEs is a CSSP issue (salary, T&L, overtime...)
- **Culture:**
 - Complicated problem space and stakeholder community, which includes: mixture of public, private, and academic stakeholders
 - Many influencers including municipal and provincial officials, councils, police boards
 - Many often competing agendas
 - Diverse models across Canada

5. Future:

a. What areas require more attention in the near-term?

Domain is different from past CSSP experience:

- Governance model may not be right fit for the future (CSS/PS – 50/50 partnership):
 - PS may not see need, value and/or support CSSP focus on this domain
 - PS historical focus is on federal policy “cover”
 - PS may question Targeted Investments in this domain
- **Strategic Planning Guidance** – historically this process consisted of an environmental scan of threats, hazards and capability gaps (known deficiencies) within and sometimes across similar communities/portfolios. While this practice may be evidence-based, it may not be considering emerging trends and the future risk environment.
- **DSS** – consult with DSS to determine how it could contribute to this CSSP transformation (e.g., dashboards; value definition; communication of success stories to diverse audiences with diverse situational awareness, cultures, experience and risk perception).

b. Where could RACI add the most value in the next 12-18 months?

- **Situational Awareness** – ensure RACI (and DSS) section is invited to all cross-community meetings, and has access to supporting documentation

Knowledge, Technology & Community Safety Risk Assessment Capability Profile

- **Evidence base** – review community documentation, direction and outcomes, and identify options for RACI to leverage risk information and to support prioritization of investments:
 - Review concepts, approach and road maps, and do a gap analysis of risk’s contribution
 - Identify options for capturing relevant risk information in the planned central database (e.g., leading and lagging indicators; risk exposure over time; impact threshold; control frameworks; stakeholder analysis; responsibility assignment matrices; range of treatment strategies) on multiple levels
 - Investigate application of system dynamics techniques to support analysis, relationship building and communications (e.g., soft systems; systems thinking models, etc.)
- **Techniques and tools** – review four priorities above and determine options for RACI engagement, compared to other CSSP activities:
 - **Describe impact (i.e., value)** – in collaboration with DSS, review domain success stories and develop consistent method to assess and explain value, internally to CSSP peers and externally to diverse stakeholder community including other levels of government (P/T/FNI and municipal authorities)
 - **Scenario planning toolkit** – leverage AHRA work (e.g., scenario planning methodology and management framework)
 - **Continuous Program Risk, Issue & Opportunity Management** framework and toolkit – recommend techniques & tools for program risk management, without increasing process burden on managers (e.g., issue log and risk register; dash boards; measures of effectiveness; value criteria / description)
 - **Start small** – with a program issue log and risk register; with risk as a standard agenda item at appropriate, forward-focused meetings where decisions on priorities are being made
 - Develop a risk toolkit to support program management; benchmark analysis of similar S&T initiatives... (e.g., input to CoP/ Portfolio Managers’ Guide)
- **SPG** – Review options to participate in development of Strategic Planning Guidance to make risk management an inherent part of the process
- **CMM** – work with DSS to develop capability maturity models for two levels – individual communities – operational, and program – strategic, and assess usefulness as a tool to support dashboard development, and value knowledge management, etc.

G.12 RA capability profile – CSSP program support

| Program Support Risk Assessment Capability Profile |
|--|
| <p>1. Context: Describe the domain</p> <p>OPIs: Ahmad Khorchid, Brian Greene:</p> <ul style="list-style-type: none">• Role is <i>challenge function</i> in support of program and senior management• Activities include support to strategic planning process• Role does not include direct support to management team (e.g., PM discipline)• First Environmental Scan (in approval process) |
| <p>2. Risk Assessment References (directives, guidelines, frameworks, standards...):</p> <ul style="list-style-type: none">• CSSP does not use a structured approach to program risk management• A manager’s guide is being produced• A new environmental scan process was initiated in 2013 |
| <p>3. Risk Assessment Capability Maturity (See attachments 6 & 7):</p> <p>a. Describe how the CSSP prioritizes risks and presents recommendations to the next level (PRM)?</p> <p>There is no structured process for communicating risk information or for describing the value of investments in risk treatment terms. This could be a problem when the program is audited in 2016.</p> <p>That is, there is no evidence base to support program value to federal partners and stakeholders in other jurisdictions and in the private sector.</p> <p>Note: A pre-audit is being planned for 2015 with support from CRS (DND), to prepare for the 2016 OAG audit.</p> <p>Strategic planning guidance is the key forward-focused document, which includes a risk-based approach to guide investment and internal capability improvement decisions.</p> <p>Developed first Environmental Scan (FY2013/14). Challenge is communications and sustainment (feedback and lessons learned).</p> <p>Recent experience with PSTP Call indicates that the priorities are broad and not linked to risk or areas of primary interest to CSSP.</p> <p>Recent Call (FY 2013/14) – approximately, 30% of the proposals were of little or no interest to CSSP.</p> <p>Communities, portfolios and sections prioritize projects mainly based on expert judgment of those close to the risks. In some cases, this means that <i>threat</i> is still the dominant</p> |

Program Support Risk Assessment Capability Profile

variable, as in the CRTI days, when the Consolidated Risk Assessment (CRA) process was developed.

[However, interviews with Tri-Service and others indicate a trend towards more emphasis on target, effects, impacts and cascading consequences. Author]

It is not clear whether CBRN/E or others are using CRA or any other process for assessing risk. Most proposals are focused on closing capability gaps, and addressing existing threats and control deficiencies.

Note: CRA is labour-intensive and there is a time delay before it is published, which may not keep up with changes in threat, which could reduce value of the process.

b. Describe how the CSSP prioritizes and communicates risks to stakeholders:

TBD

4. Major Challenges and Current Strategy:

a. CSSP:

Audit in FY 2015/16. CSS plan is to do pre-audit with DND CRS support year before. Known issues are not being managed

Risk description: CSS has high overhead because of level of experience. Could come under scrutiny by DND/DRDC, client departments and others as there are pressures on budget. If CSS cannot demonstrate value, then someone could ask why CSS does not just become a grant agency. Therefore, CSS needs a solid evidence base for past and future investments, and a story that explains the value of having a core team of senior domain experts in-house, with a story on how this knowledge is being leveraged and sustained.

b. PM Support Role:

There is a defined requirement to develop a solution set for program management. The existing governance and processes are well defined. However, there are some issues and known gaps that are not being addressed.

5. Future:

a. What areas require more attention in the near-term?

- **Program** – There are known gaps and issues related to CSSP management. CSS appears to have at least three options:
 - CSSP support staff develop guidelines themselves
 - DG tasks DSS and RACI to do a gap analysis and develop/recommend a solution set
 - Contract out a project, which is jointly managed with DSS, RACI and CSSP program oversight staff (e.g., technical authority could be. Mr. Khorchid)

Program Support Risk Assessment Capability Profile

- There may be a requirement to review the role of the *program challenge function* to include a more direct support role including: analytics, decision support to the CSSP management team, and directing administrative resources into other areas beyond traditional administrative staff duties
- **Risk** – Need to define what CSSP means by a risk-based approach. Options appear to include:
 - **Status quo** (bottom-up process dominated by threat and vulnerability; with an emerging shift in focus to include target and effects analysis)
 - **Risk- and Capability-based Investment** – CSS developed some solutions for clients, but there is no equivalent solution internally – leverage risk assessment, scenario management, capability-based investment management as baseline
- **[Author's opinion] Organization and Technology Environment** – For an S&T organization, there appears to be a gap in IM/IT and collaboration technology, no information and communications technology road map, and only limited ad hoc compensating controls:
 - It may be time for CSS to consider instituting a CIO (Chief Information Operations or Chief KM) role with a focus on internal and external collaboration and relationship management (not just IT infrastructure and network services, per say), and reviewing the role and competency requirements for administrative staff:
 - For example, if CSS relies on research and evidence, and there are rich resources that are not being systematically mined and shared internally (e.g., senate committee reports; public inquiries; disaster lessons learned reports; OAG reports; departmental scans; DPR/RPP; strategic plans), then maybe administrative staff should take on more of a research identification/benchmarking support role. Alternatively, tools exist to sift through volumes of big data and mine relevant information (e.g., CiriLab, demonstrated during RACI project in FY2012/13).
- **Process Improvement** – The following five areas should be considered for process improvement, and a plan should be developed before the CRS audit:
 - **Value** (of program) to Canada – define evidence base (Note: Paramedics initiative is relevant – see profiles on EMS and Knowledge Technology & Community Safety)
 - **Risk Management** (how does risk inform prioritization of resource allocation on multiple levels – Section (CoP /Portfolio); Program; and national strategic planning objectives:
 - Integrated approach to key performance and risk indicators
 - **Issue Management** (simple process to proactively manage known issues)
 - **Environmental Scan** (balance – consider relationship between environmental scan, benchmarking of other S&T organizations [5 Eyes] and domains of priority interest; and futures thinking...); include S&T / national-level safety and security risk and decision support systems in benchmarking project / scan work
 - **ICT road map** (focus on CSSP evidence base, collaboration, Information and KM [IKM], productivity, measures of effectiveness, improvements)

Program Support Risk Assessment Capability Profile

- **Futures** – It appears that Futures work has limited priority for CSS. However, DRDC should probably have such a capability/program, and CSS should provide input/advice. Furthermore, CSS should have a strategy, which could be leveraging Policy Horizons (GC capability: academia; or having a minimal internal capability (e.g., subscribe to futures research as a service – e.g., Shaping Tomorrow).

- b. Where could RACI (and DSS) add the most value in the near to mid-term?**
- RACI and DSS should complete a gap analysis, and investigate the requirement to provide internal support to CSSP (in the form of a formal project). Objectives could include:
 - Root cause analysis of why 30% of proposals on a recent PSTP Call were not of interest to CSSP or had a very low likelihood of ever being funded
 - Develop a methodology to define value
 - Identify options for a productivity, and IKM toolset for the CSSP management team that adds value without increasing workload
 - Review what section-specific tools exist now and determine which ones should be sustained and made available to the broader team
 - Provide a program, portfolio and project continuous risk (and audit) management framework
 - Review how intelligence and threat information is managed within CSS
 - Develop a program decision support solution (e.g., dashboard, management simulation, soft systems / OR / system dynamics / architecture framework toolset)
 - Develop a streamlined process that makes risk information and decision support more explicit in existing management and decision support systems (e.g., Environmental Scan; Strategic Planning Framework; PSTP Calls, and proposal submissions and evaluations, issue management; internal capability management including: IM/KM, collaboration, strategic relationship management, benchmarking, futures...).

Annex H Capability Maturity Model frameworks

H.1 CMM background and concept

Capability Maturity Models (CMM) have evolved since the 1980's, but they are a relatively under-exploited tool within the Government of Canada (GC) including in the area of safety and security, and risk, emergency and resilience management. The technique originated with the Carnegie Mellon University, Software Engineering Institute (CMU, SEI) work on system and software engineering. The qualitative analysis technique that is adaptable for multiple applications. SEI recently published the Cyber Emergency Response Team (CERT) Resilience Management Model¹¹ (CERT-RMM).

In its simplest form, a maturity model is an organized way to convey a path of experience, wisdom, perfection, or accumulation. (2011: 18)

The authors state that although the RMM is not a CMM per se, it does contain the two maturity dimensions that are part of the CMM Integration¹² framework: capability dimension and maturity dimension (2011: 15)

- Capability dimension – describes the degree to which process has been institutionalized; and
- Maturity dimension – define levels of organizational maturity that are achieved through raising the capability of a set of process areas in a manner described in the model.

CERT-RMM “is a capability-focused maturity model for process improvement that comprehensively reflects best practices from industry and government for managing operational resilience across the disciplines of security management, business continuity management, and IT operations management” (2011: xvii).

In 1999, SEI created the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method. One of its principles was to “place responsibility for risk assessment closer to the operations activity”. The relevance for this risk scan is that the risk assessment and prioritization of projects is a collaborative effort with most of the input coming from the front lines, or from departments and their federal partners. The assessments are normally constrained by jurisdictional and/or organizational mandates, legislation, policies, standards, cultures, availability of data and intelligence, and other factors. It is not a CSS role to review the effectiveness of threat and/or risk assessment processes within the operational areas. CSS does implicitly add value to the process based on the managers’ experience and best judgment during interactions within operational silos, when recommendations for investments are reviewed as part of the Call process and during the proposal evaluation process. However, the role of risk assessments in these decision making processes is not documented or systematic.

Whereas, CERT-RMM “comprises 26 process areas that cover four areas of operational resilience management” (2011: 7), the Centre for Security Science (CSS) risk scan considered two process

¹¹ Carelli, R. et al (2011), CERT-RMM, a maturity model for managing operational resilience.

¹² Information on CMMI can be found at: <http://www.sei.cmu.edu/cmmi/> or <http://whatis.cmmiinstitute.com/>.

areas (threat and risk assessment at the operational community level and risk management processes at the program level), and it considered nine operational domains and two strategic (management) domains, as follows:

Safety and Security Operational domains:

- Border and Transportation Security (includes maritime security);
- Cybersecurity;
- Surveillance, Intelligence & Interdiction;
- Critical Infrastructure Protection;
- Fire;
- Paramedics;
- Law Enforcement;
- CBRNE¹³ and Forensics; and
- Emergency Management Systems Integration and Psychosocial.

Strategic (management) domains:

- Knowledge, Technology & Community Safety; and
- Program decision support.

H.2 Risk scan approach

The risk scan approach focused on five components of a risk assessment capability including:

- People (e.g., experience; knowledge; continuity; training);
- Process (e.g., governance; documented, systematic and verifiable assessment techniques);
- Technology (e.g., risk assessment, IM, decision support and collaboration tools);
- Information (e.g., easy access to relevant resources including classified and open source; information sharing infrastructure); and
- Relationships (e.g., human-controlled networks; access to SMEs).

Using this construct, the author made a qualitative judgement of the CMM levels for individual operational domains. He also produced a composite view of the overall domain's capability maturity of specific risk assessment techniques in comparison to other domains based on best judgment.

To adopt a CMM approach or risk assessment, the study considered a variety of multi-criteria assessment techniques that are commonly used by specialists. The study did not explore any specific techniques in-depth including those used by the Security and Intelligence (S&I) community that tend to focus on threat evaluation, and evident- and fact- based approaches.

¹³ Chemical, Biological, Radiological, Nuclear and Explosives.

Variables and techniques that analyze independent or combinations of variables that were considered include the following:

- Threat;
- Hazard;
- Vulnerability;
- Impact / consequence / cascading effects / loss;
- Harm analysis;
- All hazards;
- Criticality;
- Interdependencies;
- Resiliency;
- Uncertainty (likelihood), frequency, probability; and
- Risk (tactical, operational, strategic).

The study focused on operational and program risk assessment techniques. It did not consider engineering, quality assurance, audit and control assessments, or other specialist techniques¹⁴, such as SWOT, gap analysis and root cause analysis, and decision support or operations research techniques, other than the Delphi technique, which was recommended as a core capability for CSS staff.

H.3 Frameworks

Part 1 includes a CMM assessment of operational areas risk assessment capabilities (Part 1, Annex B). The frameworks below were developed to establish a study baseline to support the assessment of risk assessment capability and maturity within or across operational areas, and at the strategic (management) level (i.e., program governance, planning and management).

With the exception of communities that are using techniques that CSS developed or continues to support, CSS does not track assessment techniques that are being used by federal or other partners, or organizations that implement CSSP projects. Therefore, the CMM assessment is based on best judgment.

If CSS determines that having more visibility of risk assessment and prioritization techniques, then a strategy could include embedding certain documentation of processes within the CSSP Call process or within specific community project requirements. Having this information would help CSS to identify possible areas for intervention; for example, in areas where organizations do not have access to risk sciences or analytical capabilities. The best example from this scan is the techniques that are being used at the local / municipal level. Some of these techniques could actually be giving proponents a false picture of risk and/or influencing the selection of priorities in a way that is not based on risk at all.

¹⁴ ISO 31010 Risk assessment techniques, contains 31 management and/or analytical techniques.

Preliminary RA CMM Assessment (Worksheet)

| Level | Description | Self-Assessment Factors |
|---|---|---|
| Level 5: Optimizing <i>(Strategic; supports multi-criteria, multi-domain decision making)</i> | Continuous process improvement and innovation on strategic, operational (and program) and tactical (frontline) levels | <ul style="list-style-type: none"> • Industry-, engineering -focused risk assessment techniques for specific problems (e.g., rad/nuc; energy; environment...) • Some epidemiological risk assessment techniques within specific health hazard (disease) domains |
| Level 4: Managed <i>(Crosses boundaries; supports strategic and systems thinking; scenario planning; futures thinking; collaboration and insight)</i> | Detailed measures of effectiveness for process, outputs and capability improvements | <ul style="list-style-type: none"> • CBRN – CRA (anti-terrorism), evolving since post-9/11 era • CBSA (CA-US Joint TRA – check status) • Tri-Service (tactical risk assessments – normal routine) • Bio/Med – Federal level; (Health Portfolio) check status of multi-jurisdictional RA (CRHNet) • Multi-level law enforcement; forest firefighting; SAR techniques |
| Level 3: Defined <i>(Systematic, adaptive, scalable, anticipatory, and fosters innovation - known knowns, known unknowns and unknown unknowns)</i> | Process documented, standardized and integrated into domain decision making | <ul style="list-style-type: none"> • BTS – if joint threat & risk assessment has been done (PS, 2010 stated objective); CBSA – automated PAX RA tools, container screening; TC – air cargo security screening, surveillance; IMSWG risk assessment... • EMSI – Federal AHRA IRAWG; HTRA (some departments using other techniques – RCMP using AS EMRA technique) • Explosives – review work on precursors and level of collaboration (tactical domain) • SII (tactical) – check link with CPRC and F/P/T/M/FNI LE; transcontinental organized crime, anti-human smuggling, cyber crime, etc |
| Level 2: Repeatable <i>(Verifiable; sustainable; limited horizon; problem solving & issue resolution - known knowns & known unknowns)</i> | Basic processes to identify, describe and rank risks within domains with similar risk exposure | <ul style="list-style-type: none"> • CIP – check status of Sector Risk Profiles; SCADA / ICS Cyber Test Lab initiated in 2013 • Psychosocial – academic research exists; opportunity for sharing and developing impact assessment frameworks & link to RCMP Harm Analysis, Crime Prevention... |
| Level 1: Initiating <i>(Near-term; linear thinking; known knowns)</i> | Process is ad hoc and success depends on individual effort (i.e., domain SMEs) | <ul style="list-style-type: none"> • Forensics – discrete specialities; check status of R&D and targeted investment |

Adapted from: SFL Capability Maturity Model: CAP 01 116 March 2004

1

Preliminary RA CMM Framework

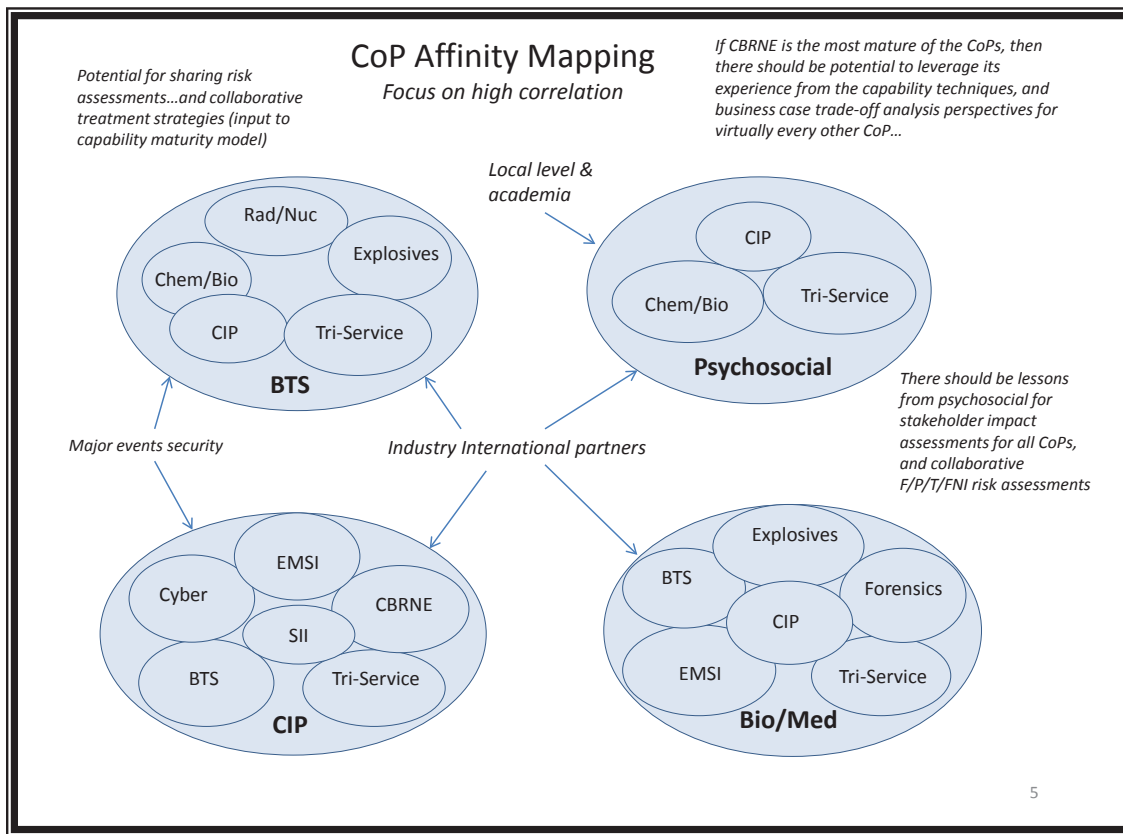
| Level | Decision Support Context | Risk Assessment / Capability Management Maturity Indicators |
|----------------------------|--|--|
| Level 5: Optimizing | <ul style="list-style-type: none"> • Support strategic decision making including with international partners ; take smart risks; address hard problems; and results in measurable improvements in societal safety, security and resilience | <ul style="list-style-type: none"> • Collaborative, transparent risk assessment processes including with international partners • Recommendations address known deficiencies and anticipated changes in risk exposure across the whole safety and security spectrum • Continuous process improvement and innovation on strategic, operational (and program) and tactical (frontline) levels • Outputs and decisions are easily interpreted and implemented • Very high confidence in process, ranking and recommendations |
| Level 4: Managed | <ul style="list-style-type: none"> • People participate in multi-jurisdictional decision making processes that achieve an effective balance of investments over time across the whole safety and security problem space | <ul style="list-style-type: none"> • Decision makers participate in and add value to the process • Recommendations address known deficiencies, and identify innovative solutions and opportunities that address anticipated risks • Detailed measures of effectiveness for process, outputs and capability improvements • Outputs are easy to understand and communicate among similar and interdependent domains, and across jurisdictional and other boundaries • High confidence in process, ranking and recommendations |
| Level 3: Defined | <ul style="list-style-type: none"> • People participate in interdisciplinary decision making on investment priorities that achieve an effective balance of investments over time within domains that have similar risk profiles | <ul style="list-style-type: none"> • Decision makers accept risks identified and prioritised by SMEs, and add some value to the process • Recommendations address known deficiencies within and sometimes, across domains, and begin to consider future risk environment • Process documented, standardized and integrated into domain decision making • Outputs are easy to understand and communicate within single or tightly coupled domains (e.g., CBRNE) • Reasonable (medium) confidence in process, ranking and recommendations |
| Level 2: Repeatable | <ul style="list-style-type: none"> • People make decisions on investment priorities that address known capability deficiencies within single or closely -related domains, and risk exposure is an explicit part of decisions & planning | <ul style="list-style-type: none"> • Decision makers consider SME advice but do not add value to the process • Recommendations consider threats, vulnerabilities and impacts in the near-term within single domains with a focus on the near-term • Basic processes to identify, describe and rank risks within domains with similar risk exposure • Outputs are clear to participants, but not necessarily to other audiences • Low confidence in process, ranking and/or recommendations |
| Level 1: Initiating | <ul style="list-style-type: none"> • People make decisions based on personal experience and advice from trusted sources; assessment of risk exposure is mostly an implicit component of decisions and planning | <ul style="list-style-type: none"> • Decision makers do not explicitly or systematically consider risk . They are at risk of making overly subjective judgments with limited or no in-depth analysis of risk environment • Recommendations are overly subjective and subject to peer /political pressure • Process is ad hoc and success depends on individual effort (i.e., domain SMEs) • Outputs are clear to people performing the assessment • Very low confidence in process, ranking and/or recommendations |

2

Annex I Affinity diagrams

The CSSP is evolving to play its role in protecting Canadians and in supporting federal and other partners. The portfolios have evolved in scope from the early clusters within the legacy program, and some communities have been combined into portfolios to facilitate collaboration and strategic management.

This study explores some diagramming techniques in order to help identify practices or lessons that could be applied in other communities or portfolios.



This page intentionally left blank.

Annex J Concept of operations

During the risk scan project, it became apparent that there is an emerging requirement to explain the value proposition for CSSP investments. For example, high priority GC requirements may already be receiving attention and funding from other large departments, and further CSS investment has limited value for either the project or for CSS. It may be that more work on regional projects that can be adapted by other regions would fit better with a CSSP value chain.

With this in mind, the author produced a CONOPS, which is intended as an input to the discussion on the CSSP evidence base and value assessment framework.

| <h1>CONOPS</h1> | |
|--|---|
| CSSP Value Concept | Rationale |
| Focus on areas that are high value to Canadians and CSSP | <ul style="list-style-type: none"> • Leverage e-Security Sandbox concept (get tangible results; reinforce and empower existing social networks) • Leverage emerging Tri-Service and national leadership relationships • Big departments and P/T partners already receive significant funding for GC priorities – consider local level gaps and constraints (lessons from CBRN, USAR, Tri-Service, MDA, Windsor-Detroit Gateway...) • Monitor reuse opportunities from DRDC |
| Focus on vulnerable populations (in regions with resource and other constraints) | <ul style="list-style-type: none"> • Fewer resources than large provinces – already implementing cross-border multi-jurisdictional solutions; faster decision cycles; industry is engaged and is a trusted partner • Example - Leverage Tri-Service / EM / CIP work in Atlantic Canada • Apply / adapt lessons for other regions [e.g., community resilience; natural disasters (flooding, sensitive ecosystems and species at risk), accidents / system failure (rail; pipelines; ferries) • CSSP strategy for the North |
| Focus on regional (and local) problem space | <ul style="list-style-type: none"> • Easier access to decision makers in government and industry; leverage networks with bordering states • Less bureaucracy and fewer management hurdles; can do attitude; creative solutions; quick wins • Create capacity in regions that has a multiplier / domino effect for other regions or nationally |
| Focus on critical economic bottlenecks and multi-modal transportation hubs | <ul style="list-style-type: none"> • Leverage work on Maritime Domain Awareness (St Lawrence Seaway & Great Lakes) for other regions (e.g., North, West Coast, Atlantic Canada, Northern Ontario) • Leverage experience with Detroit-Windsor for other corridors, hubs, networks, infrastructure assets • Leverage work on cascading effects and socio-economic impact analysis (financial / job loss) |
| Focus on solutions that are adaptable and scalable across program and across country | <ul style="list-style-type: none"> • Document success stories (e.g., CRTI, CRA, Capability-based investment, AH scenarios) and leverage internally across portfolios • Develop program evidence base (prepare for audit in 2016) (leverage EMS & Fire work) |
| Focus on streamlined internal program, process and decision support capability improvement | <ul style="list-style-type: none"> • Internal decision support toolkit (e.g., evidence base; value assessment; environmental scan...) • Technology road map (decision support; KM; collaboration; research; productivity improvements) • Streamlined processes that do not increase administrative burden (e.g., dashboards; risk management) • Agile program, strategic relationship, collaboration and communications management • Manager's Guidebook (sections on decision support; capability, risk & value assessment ; multi-criteria decision making, Delphi and other techniques) |

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

| | |
|--------|--|
| AHRA | All Hazards Risk Assessment |
| CBP | Capability-Based Planning |
| CBP | Customs and Border Protection (US DHS) |
| CBRNE | Chemical, Biological, Radiological, Nuclear and Explosives |
| CMM | Capability Maturity Model |
| CONOPS | Concept of Operations |
| CoP | Community of Practice |
| CRA | Consolidated Risk Assessment |
| CRTI | CBRNE Research & Technology Initiative (legacy CSSP program area) |
| CSSP | Canadian Safety and Security Program |
| DHS | Department of Homeland Security (US) |
| DSS | Decision Support Section |
| ERTEE | Emergency Responder Test & Evaluation Establishment |
| F/P/T | Federal / Provincial / Territorial (First Nations & Inuit is implicit) |
| GC | Government of Canada |
| GOC | Government Operations Centre |
| HIRA | Hazard Identification and Risk Assessment |
| IRAWG | Interdepartmental Risk Assessment Working Group |
| KM | Knowledge Management |
| MoE | Measures of Effectiveness |
| PS | Public Safety Canada |
| RACI | Risk Assessment and Capability Integration Section |
| RMM | Resilience Management Model |
| RRAP | Regional Resiliency Assessment Program (PS and DHS programs) |
| SME | Subject Matter Expert |
| SPG | Strategic Planning Guidance |
| SRMBoK | Security Risk Management Body of Knowledge |
| SWOT | Strengths, Weaknesses, Opportunities, Threats (Uncertainty) |
| THIRA | Threat and Hazard Identification and Risk Assessment |
| VA | Vulnerability Analysis |
| VRAC | Virtual Risk Assessment Cell (PS) |

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.) Centre for Security Science Defence Research and Development Canada 222 Nepean St. 11th Floor Ottawa, ON Canada K1A 0K2 | 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 APRIL 2011 | |
| 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 Scan: A review of risk assessment capability and maturity within the Canadian Safety and Security Program | | |
| 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.) June 2014 | 6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 106 | 6b. NO. OF REFS (Total cited in document.) 29 |
| 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.) Scientific Report | | |
| 8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Centre for Security Science Defence Research and Development Canada 222 Nepean St. 11th Floor Ottawa, ON Canada K1A 0K2 | | |
| 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.) CSSP-2012-TI-1108 | 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-2014-R36 | 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.)

The Canadian Safety and Security Program (CSSP) management framework, with respect to governance, collaboration, project selection, financial management and accountability, policy and planning, and the evolving public safety and security environment is more dynamic than ever. The need to focus on improving the quality, timeliness and value of risk information has never been greater. CSSP Strategic Planning Guidance (2013) states the requirement to compile a compendium of risk assessment techniques with a view to building a consolidated, cross-domain capability-based perspective.

The study considered risk assessment capabilities on the operational and program levels. The streamlined methodology included interviews and literature review, including international standards and best practices. Risk Assessment Capability Profiles were developed for operational areas and for the program. A capability maturity model technique and a preliminary SWOT analysis highlight quick wins for process improvement in the near-term.

The study found that there is limited visibility of risk assessment and other decision support techniques that are being used by external organizations to prioritize requirements, and there is no internal systematic approach to communicate risk across communities and at the program level. For the most part, risk assessment is an ad hoc process, and there are missed opportunities to contribute to the program's strategic outcomes, value and evidence base.

En ce qui concerne la gouvernance, la collaboration, la sélection de projets, la gestion financière et l'imputabilité, les politiques et la planification, ainsi que l'environnement changeant de la sécurité publique, le cadre de gestion du Programme canadien pour la sûreté et la sécurité (PCSS) est plus dynamique que jamais. Le besoin de mettre l'accent sur l'amélioration de la qualité, le respect des échéances et la valeur des renseignements sur les risques n'a jamais été aussi grand. Le guide de planification stratégique du PCSS (2013) énonce le besoin de constituer un recueil de techniques d'évaluation des risques dans le but d'élaborer une perspective inter domaines intégrée et fondée sur les capacités.

L'étude a tenu compte des capacités d'évaluation des risques au niveau des opérations et du programme. La méthodologie simplifiée comportait des entrevues et une revue de la littérature, notamment des normes et des pratiques exemplaires internationales. Des profils capacitaires d'évaluation des risques ont été élaborés dans les secteurs des opérations et du programme. Une technique du modèle de stabilisation des capacités et une analyse préliminaire des forces, faiblesses, possibilités et menaces (FFPM) mettent en évidence des mesures à effet rapide pour l'amélioration du processus à court terme.

L'étude a permis de constater qu'il existe peu de renseignements sur l'évaluation des risques et les techniques d'aide à la prise de décision utilisées par les organisations externes pour établir les priorités en matière d'exigences, et qu'il n'y a pas d'approche systématique interne pour faire part des risques dans les communautés et au niveau du programme. Dans la plupart des cas, l'évaluation des risques est un processus ponctuel, ce qui fait qu'on rate des occasions de contribuer aux résultats stratégiques, à la valeur et aux données probantes du programme.

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; capability maturity model; program management; scan