Defence Research and Development Canada
Recherche et développement pour la défense Canada

The Federal All Hazards Risk Assessment Framework Body of Knowledge: Volume II

Supporting Material

Ian Bayne
Jim Duncan
Brad Mills
Maxsys Inc.

Shaye Friesen
Alain Goudreau
DRDC Centre for Security Science

Defence Research and Development Canada – CSS

Technical Note
DRDC CSS TN 2013-015
September 2013

The Federal All Hazards Risk Assessment Framework Body of Knowledge: Volume II

Supporting Material

Ian Bayne
Jim Duncan
Brad Mills
Maxsys Inc.

Shaye Friesen
Alain Goudreau
DRDC Centre for Security Science

Defence Research and Development Canada – CSS

Technical Note
DRDC CSS TN 2013-015
September 2013

IMPORTANT INFORMATIVE STATEMENTS

Template in use: template-july2013-eng_V.03.01.dot

Abstract

Public Safety (PS) Canada and Defence Research & Development Canada's (DRDC) Centre for Security Science (CSS) are in the process of investigating improvements to the federal All Hazards Risk Assessment (AHRA) methodology that would enable the federal government to develop a national picture of high priority risks and capabilities that mitigate those risks.

This report contains the statistical data and reference materials used to develop the Technical Report, The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume 1: Establishing an Information Baseline and Way Forward, DRDC CSS TR 2013-014.

The Technical Report (TR) is intended for participants in the federal AHRA initiative and for a wider audience involved in safety, security, societal resilience and emergency risk management. The report highlights lessons from the federal AHRA approach that would support multi-mandate and multi-jurisdictional risk assessments, and enable the development of a national risk assessment (NRA).

This Technical Note is reviewed and, if required, updated annually.

Résumé

Sécurité publique Canada (SP) et le Centre des sciences de la sécurité de Recherche et développement pour la défense Canada (RDDC CSS) examinent actuellement les améliorations pouvant être apportées à la méthodologie d'évaluation tous risques (ETR) du gouvernement du Canada afin que ce dernier brosse un portait des principaux risques et des capacités atténuant ceux-ci à l'échelle nationale.

Ce rapport contient des données statistiques et des matériaux de référence utilisés pour élaborer le rapport technique, The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume 1: Establishing an Information Baseline and Way Forward, DRDC CSS TR 2013-014.

Ce rapport technique (RT) est destiné aux gens participant à l'initiative fédérale d'ETR, de même qu'à un plus large public associé à la sûreté, la sécurité, la résilience sociétale et la gestion des risques en situation d'urgence. Le rapport souligne les leçons tirées de l'approche fédérale d'ETR pouvant soutenir des évaluations de risque touchant plusieurs mandats et compétences, et permettant l'élaboration d'une ENR.

Ce document est passé en revue et, si nécessaire, mis à jour annuellement

Record of changes

Date	Description	Remarks
29 July 2013	Peer Review feedback included in Volumes I & II	

Table of contents

List of figures

List of tables

1 Folio 1: Acronyms

This list should be reviewed in conjunction with approved Public Safety Canada (PS) terminology. When there are conflicts, the PS terms should be used. It is recognized that departments and other jurisdictions use a variety of terms. It is anticipated that contradictions and ambiguities will be minimized over time through a systematic approach to terminology and applying Community Mapping techniques that were demonstrated during the AHRA activity.

Table 1: Acronyms

Acronym	Description
ADM EMC	Assistant Deputy Minister Emergency Management Committee
ADM EMRO	ADM Emergency Management and Regional Operations
ADM NSOC	Assistant Deputy Minister National Security Operations Committee
AF	Architecture Framework
AHRA	All Hazards Risk Assessment
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
AS	Australia
BAP	Border Action Plan
BCP	Business Continuity Planning
BCM	Business Continuity Management
BIA	Business Impact Analysis
BoK	Body of Knowledge
BOI	Basis of Estimate (CBIM term)
CADM	Core Architecture Data Model
C&A	Certification and Accreditation (IT system control assurance process)
CAIP	Capability Improvement Process
CARVER	Target and vulnerability analysis tool (US, critical infrastructure)
CBA	Cost/Benefit Analysis
CBIM	Capability-Based Investment Model
CBP	Capability-Based Planning
CBPMT	Capability-Based Planning Methodology and Tool (John Hopkins University)
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosives
CCRA	Climate Change Risk Assessment (UK)

Acronym	Description
CCSS	Canada’s Cyber Security Strategy
CERT	Cyber Emergency Response Team (Carnegie Mellon University, US)
CERT-RMM	CERT Resilience Management Model (US)
CIP	Critical Infrastructure Protection
CI/KR	Critical Infrastructure / Key Resources (US, DHS)
CIPBSA	Critical Infrastructure Protection and Border Security Agreement
CIR	Critical Infrastructure Resilience (AS/NZ)
CISAP	Critical Infrastructure Strategy and Action Plan
CLD	Causal Loop Diagram
CMM	Capability Maturity Model
CoP	Community of Practice
CRA	Consolidated Risk Assessment
CRHNet	Canadian Risk and Hazards Network
CRP	Corporate Risk Profile
CRSA	Control and Risk Assessment (UK, Orange Book)
CRTI	CBRNE Research and Technology Initiative
CSA	Canadian Standards Association
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program (CSS)
CTEC	Cyber Threat Evaluation Centre
DA	Decision Analysis
DHS	Department of Homeland Security (US)
DNDAF	Department of National Defence Architecture Framework
DoDAF	Department of Defense Architecture Framework
DPR	Departmental Performance Report
DRDC	Defence Research and Development Canada
ECCV	Emergency and Crisis Communications Vocabulary
EMA	Emergency Management Act
EMF	Emergency Management Framework
EMNS	Emergency Management and National Security
EMPG	Emergency Management Planning Guide
EMPS	Emergency Management Planning System (PS portal)

Acronym	Description
ERA	Environmental Risk Assessment
ETA	Event Tree Analysis
ESF	Emergency Support Function
FAA	Financial Administration Act
FAA	Federal Accountability Act
FCC	Federal Coordination Centre
FCO	Federal Coordinating Officer
FERMS	Federal Emergency Response Management System
FERP	Federal Emergency Response Plan
FMEA	Failure Mode Effects Analysis
FMECA	Failure Modes and Effects and Criticality Analysis
FPEM	Federal Policy on Emergency Management
FPT	Federal, Provincial, Territorial (governments), also F/P/T
FTA	Fault Tree Analysis
FNI	First Nations and Inuit
GC	Government of Canada
GOC	Government Operations Centre (PS)
HACCP	Hazard Analysis and Critical Control Points
HAZOP	Hazard and Operability Studies
HAZUS-MH	Hazard US – Multi-Hazard
HRA	Human Reliability Assessment
HRE	High Resilience Environment (GOC *system*)
HTRA	Harmonized Threat Risk Assessment
IACC	Intelligence Assessment Coordinating Committee
IAP	Incident Action Plan
ICS	Incident Command System
ID	Influence Diagram (also Causal Loop Diagram)
IEC	International Electrotechnical Commission
IEG	Intelligence Expert Group (Domestic Security)
IKM	Information and Knowledge Management
IMS	Incident Management System
IPC	Information Protection Centre

Acronym	Description
IRAWG	Interdepartmental Risk Assessment Working Group
IRM	Integrated Risk Management
ITAC	Integrated Terrorist Assessment Centre
IWG	Interdepartmental Working Group
ISO	International Organization for Standardization
KM	Knowledge Management
LOPA	Layers of Protection Analysis
MAA	Mutual Assistance Agreement
MAF	Management Accountability Framework
MCDA	Multi-Criteria Decision Analysis
MCDM	Multi-Criteria Decision Making
MCRA	Multi-Criteria Risk Assessment
MODAF	Ministry of Defence Architecture Framework
MOU	Memorandum of Understanding
NERS	National Emergency Response System
NIST	National Institute of Standards and Technology (US)
NL	Netherlands
NPV	Net Present Value
NRA	National Risk Assessment (NL, UK - Confidential)
NRPA	National Resilience Planning Assumptions (UK)
NRR	National Risk Register (UK – public version of NRA)
NZ	New Zealand
OGD	Other Government Departments (and Agencies)
OODA	Observe, Orient, Decide, Act
OR	Operations Research
PAA	Program Activity Architecture
PCO	Privy Council Office
PDCA	Plan – Do – Check – Act (Deming)
PESTLE	Political, Economic, Social, Technological/Technical, Legal, Environmental (EMPG)
PGS	Policy on Government Security
PHA	Preliminary Hazard Analysis
PMBoK	Project Management Body of Knowledge

Acronym	Description
PMI	Project Management Institute
PMPRR	Prevention/Mitigation, Preparedness, Response, Recovery
PRA	Probabilistic Risk Assessment
PRA	Participative Risk Assessment
PRICIE	Personnel; R&D/OR; Infrastructure & Organization; Concepts, Doctrine & Collective Training; IT Infrastructure; Equipment, Supplies & Services (Canadian, CBP construct)
PS	Public Safety Canada
QA	Quality Assurance
QRA	Qualitative or Quantitative Risk Assessment
RACI	Risk Assessment & Capability Integration (CSS section)
RACI	Responsibility, Accountability, Communications, Information (stakeholder analysis and project management tool)
RCA	Root Cause Analysis
RCSA	Risk Control Self-Assessment
RVA	Risk and Vulnerability Assessment (US, DHS)
RERMS	Regional Emergency Response Management System
RMAF	Results-Based Management Accountability Framework
RPP	Report on Plans and Priorities
RRP	Regional Risk Profile
SA	Situational Awareness
SA&A	Security Assessment & Authorization (replaces C&A)
SD	System Dynamics
SEMP	Strategic Emergency Management Plan
S&T	Science & Technology
SME	Subject Matter Expert
SPG	Strategic Planning Guidance (CSS)
SOP	Standard Operation Procedure
SOREM	Senior Officials Responsible for Emergency Management (EMF)
SRP	Sector Risk Profile
SRM	Security Risk Management
SRMBoK	Security Risk Management Body of Knowledge (AS)
SRP	Sector Risk Profile
SWIFT	Structured “What-if” Technique

Acronym	Description
SWOT	Strengths, Weaknesses, Opportunities, Threats
TBS	Treasury Board Secretariat
TCL-C	Target Capabilities List - Canada
TISN	Trusted Information Sharing Network (AS)
TOC	Transnational Organized Crime
TOGAF	The Open Group Architecture Framework
TRA	Threat Risk Assessment
UK	United Kingdom
US	United States of America
VA	Vulnerability Assessment

2 Folio 2: AHRA Program References

This list contains relevant documents that form the basis for the BoK analysis and that support future work. It is not the complete inventory, and it does not include classified documents. When the source is not Canadian, the file name includes the source nation or organization, so that references are grouped by nation and/or source (e.g., US or DHS). The products on this list were selected based on best judgement. The intent is to provide enough information for readers to find those documents on the web or from the source. This selective list is intended to be forward-focused and relevant to building a national picture of risk exposure to support strategic decision making. When presentations are cited, best effort was made to identify the most current and useful document. Canadian EM references to risk assessment are captured in Folio 3.

Table 2: AHRA Program References

Source	References
CA	AHRA - A Framework Approach, Presentation (A. Goudreau), CSS, October 2012
	AHRA Methodology Guideline 2011-2012, PS, 2012
	AHRA Community Map, Excel spreadsheet, CSS (M. Turcotte)/PS
	AHRA Community Mapping - Respondents willing to contribute to AHRA development, (6 options), Excel spreadsheet, CSS/PS
	AHRA (IEG) Lexicon, Excel spreadsheet, PS-SP-#274358-v2, 2010
	AHRA Scoring Process, Scoring Impacts and Likelihood, Presentation, A Goudreau, CSS, 2012
	AHRA Project Implementation Plan (PIP), CSS, 2007
	AH risk events taxonomy, Results of 2008 survey, DRAFT, CSS/PS
	AHRA Summary of Results 2010-2011 (risk event scenario workshops), PS, 2011 (S)
	Canadian Risks and Hazards Network (CRHNet), http://www.crhnet.ca/; 2013
	CAN/CSA-ISO/IEC 31000: 2009 , Risk management: principles and guidelines
	CAN/CSA-ISO/IEC 31010: 2009, Risk assessment techniques
	CAN/CSA-ISO/IEC 73:2009, Risk management vocabulary
	CAN/CSA Z-1600 (2009), Essentials Emergency Management and Business Continuity Programs
	Chouinard P. and Verga S. (2012), An All Hazards Risk Assessment in Support Regional Capability-Based Planning, Presentation to CRHNet , CSS, October 2012
	Consolidated Risk Assessment (CRA) Methodology, conducted annually since 2002, IEG/CSS (not dated)
	Management of Risk, TBS, 2012
	Murphy, B. & Etkin, D., Disaster and Emergency Management in Canada, Creative Commons; http://www.crhnet.ca/resources/onlineBook/Introduction%20Formatted.pdf
	Office of the Auditor General (OAG), National Security in Canada: The 2001 Anti-

Source	References
	Terrorism Initiative, Chapter 4, March 2004 Risk management guide for critical infrastructure sectors, PS, July 2010 The AHRA Process – Scoring Impacts and Likelihood, Presentation, CSS, 2012 Target Capabilities List – Canada (TCL-C), Draft, CSS, March 2011 Target Capabilities List – Canada (TCL-C), v2012-1, CSS TCL-C, Risk management definition, CSS, March 2011 Verga, S. (2012), A Holistic Cross-Government All Hazard Risk Assessment, DRAFT, CSS, 2012 Verga, S., All hazards risk framework – an architectural model, CSS (not dated)
US	DHS, Bouncing Back, How Companies Approach Resilience (2011), Research Report, DHS-2, 2011; Conference Board Inc., 2011 DHS, IT Security Essential Body of Knowledge (EBK), A Competency and Functional Framework for IT Security Workforce Development, National Cyber Security Division, September 2008 DHS, National Preparedness Goal (NPG), First Edition, September 2011 DHS, Risk assessment methodology: evolution, issues and options for congress (2007), Congressional Research Service (CRS), Order Code RL 33858, 2007 DHS, Risk Lexicon, September 2010 DHS, Strategic National Risk Assessment (SNRA), December 2011 (Full results of SNRA are classified) DHS, Threat and Hazard Identification and Risk Assessment (THIRA) Guide (2012), Comprehensive Preparedness Guide (CPG) 201, First Edition, April 2012 DHS, Threat and Hazard Identification and Risk Assessment (THIRA) Guide (2012), Comprehensive Preparedness Guide (CPG) 201,Supplement 1 – Toolkit, First Edition, April 2012 Guide to Capability-Based Planning, The Technical Cooperation Program (TCCP), Technical Panel 3, not dated (discovered in 2009) FEMA's Risk Mapping, Assessment and Planning (RiskMAP), Report to Congress, February 2012 Preparedness for All Hazards, Center for Disease Control and Prevention, http://emergency.cdc.gov/hazards-all.asp ; 9 Feb 13 Presidential Policy Directive 8 (PPD 8), National Preparedness, White House, March 2011 Quadrennial Homeland Security Review (QHSR), DHS, February 2010 Strategic National Risk Assessment, DHS, December 2011 Capability-Based Planning Methodology and Tool, John Hopkins University
AS	AS, Critical Infrastructure Resilience Strategy, 2010 Australia (AS), National Emergency Risk Assessment Guidelines; National Risk

Source	References
	Assessment Framework, Tasmania State Emergency Service, Department of Police and Emergency, October 2010 Trusted Information Sharing Network (TISN); http://www.tisn.gov.au/Pages/default.aspx ; 10 Apr 13
UK	Cabinet Office, risk assessment; http://www.cabinetoffice.gov.uk/content/risk-assessment; 25 Jan 13 Climate change risk assessment (CCRA), Department for Environment, Food & Rural Affairs (Defra), January 2-12; UK, http://www.defra.gov.uk/environment/climate/government/risk-assessment/; 25 Jan13 HM Government, A Strong Britain in an Age of Uncertainty, The National Security Strategy (NSS), 2012 Local Resilience Forums, Contact Details; https://www.gov.uk/local-resilience-forums-contact-details; 11 Ape 13 Local to global: reducing the risk from organized crime; Serious Organized Crime Agency (SOCA) Annual Report, 2013-2014 National Risk Register of Civil Emergencies (2012) Cabinet Office; https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61929/CO_NationalRiskRegister_2012_acc.pdf; 11 Apr 13 Planning and preparation for emergencies: the national resilience capabilities programme (NRCP); https://www.gov.uk/preparation-and-planning-for-emergencies-the-capabilities-programme; 11 Apr 13 Reducing Risks of Future Disasters, Priorities for Decision Makers, Final Project Report, Government Office for Science, 2012 Risk assessment: how the risk of emergencies is assessed in the UK, Cabinet Offices; https://www.gov.uk/risk-assessment-how-the-risk-of-emergencies-in-the-uk-is-assessed; 11 Apr 13 Risk Management assessment framework: a tool for departments, HM Treasury, 2009 The Orange Book, Management of Risk (MoR) – Principles and Concepts, October 2004; http://www.hm-treasury.gov.uk/orange_book.htm; 25 Jan13
NL	Banking Industry Country Risk Assessment: The Netherlands, Nov 12 National Security Programme, National Risk Assessment Guide (2008), Minister of the Interior and Kingdom Relations; June 2008 National Risk Assessment Fact Sheet, NL, 2009 Regional risk assessments in NL, MisRar Seminar, 2010; http://www.misrar.nl/UserFiles/File/BP_1_ZHZ_annex%201%20Regional%20risk%20assessment%20in%20The%20Netherlands.pdf; 25 Jan 13 Room for the River Programme, http://www.ruimtevoorderivier.nl/meta-navigatie/english/; 21 Feb 13 Working with scenarios, risk assessment and capabilities in the national safety and security strategy of the NL, October 2009

Source	References
NZ	National risk assessment 2010; anti-money laundering / counter financing of terrorism (AMF/CFT); NZ Police, Financial Intelligence Unit; http://www.justice.govt.nz/policy/criminal-justice/aml-cft/publications-and-consultation/20110308-NRA-2010-Primary-Document-FINAL.pdf ; 25 Jan13 Reducing the risk of organizational silos on resilience (2009), Resilient Organisations Research Report 2009-01, March 2009 Risk assessments, Department of Justice, http://www.justice.govt.nz/policy/criminal-justice/aml-cft/risk-assessments; 25 Jan 13 Sector and National Risk Assessments (Financial Sector), Department of Internal Affairs, http://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Services-Anti-Money-Laundering-Sector-and-National-Risk-Assessments; 25 Jan 13
Global	GRC Capability Model 2.0, “Red Book”, Open Compliance and Ethics Group (OCEG), 2.0, April 2009 Organisation for Economic Cooperation and Development (OECD), Studies in Risk Management, Innovation in Country Risk Management; 2009 The Burgundy Book, Governance, Risk Management and Compliance (GRC) Capability assessment tools - samples, OCEG, 2009 World Economic Forum (WEF), Global Risks 2012, Seventh Edition, 2012

3 Folio 3: Canadian emergency management references that mention risk assessment

This inventory is a snapshot of federal EM references developed at different times for different purposes that mention risk assessment. It illustrates the challenge of making changes because of the level of effort, the potential ripple effects and time to compare source material. Future work would presumably consider equivalent Provinces/Territories/First Nations & Inuit (P/T/FNI) information resources. The federal AHRA activity demonstrated the value of using a systems engineering approach including the use of an architecture tool and operations research. The BoK project evaluated a couple of information and knowledge management tools that could support a more agile approach to managing this dynamic information set and convergence with a capability assessment or other decision support methodology.

Table 3: Federal Emergency Management References

Reference	Description
EM Act, 2007	6 (1) Ministers responsibilities… to identify the risks that are within or related to his or her area of responsibility – including those related to critical infrastructure – and to do the following…
Federal Policy for Emergency Management (FPEM), 2009	5. 5.1 The Government of Canada has adopted an all hazards approach to emergency management, encompassing four interdependent, but integrated functions: mitigation / prevention, preparedness, response and recovery… 5.3 The risk assessment aims to gain an understanding of potential risks associated with all types of natural and human-induced hazards and disasters. Such assessments would also identify the potential impacts of these events on people, property and the environment… 5.4 Public Safety Canada will provide operational tools, guidelines, and best practices for undertaking all phases of emergency management planning, including conducting risk assessments. **Appendix A - Definitions** All-hazard risk assessment – An approach that recognizes that the actions required to mitigate the effects of emergencies are essentially the same, irrespective of the nature of the event, thereby permitting an optimization of scarce planning, response and support resources. The intention of all-hazard generic emergency planning is to employ generic methodologies, modified as necessary by particular circumstances. All-hazards incorporates natural and man-made hazards threats including traditional emergency management events such as flooding and industrial accidents; as well as national security events such as acts of terrorism; and cyber events (FERP)

Reference	Description
An Emergency Management Framework for Canada (EMF), January 2011	**Principles** **Risk-Based** A risk based approach…emphasizes the importance of assessing vulnerability to all hazards in order to determine the optimal balance and integration of measures to address vulnerabilities and risks. The presence of a hazard or a threat that is related to vulnerability constitutes a risk. Risk Management practices facilitate improved decision-making by clarifying the dimensions of risk, including its causes, likelihood of occurrence and possible severity of consequences… **All-Hazards** …The all-hazards approach increases efficiency by recognizing and integrating common emergency management elements across hazard types, and then supplementing these common elements with hazard specific sub-components to fill gaps as required. Hazards are sources of potential harm or loss…Each hazard should be identified and assessed by appropriate authorities in order to prioritize hazards against potential vulnerabilities in society. By assessing the risks associated with all hazards in an integrated way, efforts may be broadly effective in reducing the vulnerability or people, property, the environment and the economy. **Glossary** **All-Hazards** … as such, All-Hazards does not literally mean preparing to address any and all potential hazards in existence. Rather, it emphasizes the leveraging of synergies common across hazards and maintaining a streamlined and robust emergency management system. The "All-Hazards" approach also improves the ability of emergency management activities to address unknown hazards or risks.
Federal Emergency Response Plan (FERP), January 2011 (to be re-written FY2012/1013)	**Section 2, 2.1 Introduction** The Federal Emergency Response Management System (FERMS) is a comprehensive system that integrated the Government of Canada's response to emergencies. It is based on the tenets of the Incident Command system and the Treasury Board Secretariat's Integrated Risk Management Framework. 2.5.1 Public Safety Canada Emergency Response Levels **Level 2 – Risk Assessment and Planning** … As an incident unfolds and the requirements for a federal response becomes clearer, a risk assessment is conducted. This assessment… identifies vulnerabilities, aggravating external factors and potential impacts.

Reference	Description
	2.6.3 Risk Assessment Key procedures of the Risk Assessment Function are; • Ongoing hazard analysis (threat and vulnerability analysis) and probability assessment; • Determination / analysis of mitigating or aggravating factors; • Impact analysis on critical infrastructure sectors; • Risk analysis; and • Recommendations to decision makers.
Emergency Management Planning Guide (EMPG) 2010-2011, 2010	**Preface** The EMPG … is intended to assist all federal government institutions in developing their all-hazards Strategic Emergency Management Plans (SEMP). A SEMP establishes a federal government institution's objectives, approach and structure for protecting Canadians and Canada from threats and hazards in their areas of responsibility... **Step 2 – Orientate** **Conduct all-hazards risk assessment:** • Identify risks – establish a risk register • Analyze risks – evaluate probability / likelihood of occurrence; and analyze consequences / impact • Evaluate risks – prioritize risks • Identify risk prevention / mitigation options **2-4 Identify vulnerabilities** A vulnerability assessment looks at an inadequacy or gap in the design, implementation or operation of an asset that could enable a threat or hazard to cause injury or disruption **2-5 Conduct All-Hazards Risk Assessment** …An all-hazards approach to risk management does not necessarily mean that all hazards will be assessed, evaluated and treated, but rather that all hazards will be considered. …The hazard risk domain is covered by the AHRA process. However, the strategic risk domain (e.g., political risks, reputational risks) and the operational risk domain (e.g., day-to-day issues confronting the institution) are not. The hazard risk domain can be divided into three risk areas: • **Natural hazards** – the risks associated with natural (geological, meteorological or biological) hazards (e.g., earthquake, landslide, flood, drought, pandemic influenza, foot and mouth disease, insect infestations); • **Intentional human actions** – the risks associated with chemical,

Reference	Description
	nuclear or other hazards resulting from deliberate actions (e.g., terrorism, sabotage); and • **Unintentional human actions** – the risks associated with chemical, nuclear or other hazards resulting from accidents (e.g., hazardous material spill or release, explosion / fire, water control structure / dam / levee failure). **a. Identify risks** …involves the identification of risk sources, areas of impact, events and their causes, as well as potential consequences **b. Analyze risks** Evaluate likelihood / probability of occurrence Analyze consequences / impacts
National Emergency Response System (NERS), January 2011	3**.2 Risk Assessment / Impact Analysis** …While the process of initiating risk assessment and determining impact analysis are unique to each province and territory, the end products are the result of coordinated efforts between government
AHRA Methodology Guidelines 2011-2012, 2012	**Preface** …principal audience for the methodology guidelines is federal government institutions **Introduction and Purpose** …[AHRA methodology] supports all federal government institutions in fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for EM planning… …The intention of the process is therefore to produce a whole-of-government [federal] risk picture… As well, the methodology can be used by federal institutions to perform their own risk assessment and ensure integration and alignment with the whole-of-government process. [AHRA] initiative provides a venue for the creation of a federal AHRA community of practice, and a forum for sharing risk information, tools and methodologies. Risk assessment specific to the critical infrastructure (CI) sectors is beyond the scope…Going forward the possibility of aligning these risk assessment activities will be examined. **Objectives (page 3)** Includes: capture risks that are significant and are of federal interest and raise awareness of risks that are not of federal concern…

Reference	Description
	Overview …the assessment of risks of a federal interest will be done on an annual basis, starting in June every year with the identification of priority threats and hazards [AHRA business cycle] The annual assessment will focus on the most probable and consequential risks. AHRA employs a scenario-based risk assessment approach. 5 steps – context, identification, analysis, evaluation and treatment Risk themes – activities or phenomena of a particular interest to an institution with which significant risks might be associated **Risk taxonomy – Annex 3** Risk event scenario development – Annex 4 […based on present day risk events and not on real past events…] **Step 5 Risk Treatment** **Data Management (page 54)** A major shortfall in many risk assessment processes is the lack of adequate data management capability and associated resources. Simplicity will be crucial in ensuring that the data management principles and practices can be universally applied. Finally, international work performed by the GC in relation to the sharing of leading risk assessment and risk management practices will continue to make the AHRA methodology and its process evolve, emphasizing on the federal government's commitment towards continuous improvement of the AHRA. Annex 2 – SWOT and PESTLE Analysis Annex 3 – AHRA Risk Taxonomy Annex 5 – Rating of the impact on Canada's reputation and influence Annex 6 – Economic Category Assessment Tool – Direct and Indirect Economic loss for Repair or Replacement Annex 7 – Glossary (page 69) The intention of an all-hazards approach is to employ generic emergency planning methodologies, modified as necessary according to the circumstances.
Canada's National	**1.2 Scope**

Reference	Description
Disaster Mitigation Strategy (NDMS), 2008	…Responding directly to national consultation findings, the NDMS supports all-hazards emergency management with an initial focus of reducing risk posed by natural disasters, an area that all stakeholders agree requires urgent attention. **Footnote 1**:... Mitigation activities should incorporate the measurement and assessment of the evolving risk environment and may include the development of comprehensive, pro-active instruments that enable the prioritization of risk reduction investments. **2.3 Knowledge and Research [principle 3]** Apply and promote scientific and engineering best practices in order to build a knowledge base for sustainable, cost-effective mitigation decisions that contribute to community resiliency. …The FPT Ministers agree to promote and work to enable timely access to standardized data to support hazard identification and risk assessment across Canada in order to inform disaster mitigation priority setting and decision-making. Governance structure includes a national level FPT Centre of Mitigation Excellence

4 Folio 4: Body of Knowledge Methodology

4.1 Overview

Public Safety (PS), federal departments and the Centre of Security Science (CSS), and their respective networks are valuable sources of information. Similarly, Provinces/Territories (P/T) and other jurisdictions have their own approaches and terminology. The intent of this brief description of the AHRA BoK methodology is to illustrate that this is one of the challenges facing a national risk assessment program. It is envisaged that PS will have to develop a process to manage a BoK. An example of a tool is the US Homeland Security Digital Library (HSDL). The AHRA activity demonstrated the value of Community Mapping, but the process must be dynamic and sustainable to minimize if not avoid duplication of effort and to improve consistency across jurisdictions and knowledge domains.

4.1.1 Context

Constraints on developing the BoK included:

- Documents of all types were stored on a CSS shared drive;
- Other documents are stored on PS shared drives and in other locations, but the team did not have access to these resources;
- There were multiple versions of documents, and no simple and consistent way to determine meta data (e.g., author, source, version number and date);
- Documents did not use a standardized file naming convention;
- Documents from Public Safety (PS) used a naming convention from the department's document management system (RDIMS) that included long file names and symbols, which prevented CSS from quickly uploading them to a SharePoint site; and
- It was too time consuming to determine which products were the most current or relevant, and to upload the documents manually to SharePoint. To overcome these limitations, CSS provide the BoK references on a CD ROM.

4.1.2 Scope

The Body of Knowledge (BoK) project included a proof of concept demonstration of two commercial tools as follows:

- CiriLab Organizer, an analytical tool was used to identify the most relevant inputs to the BoK by comparing content; and
- MindJet, a mind mapping tool was used to develop a BoK structure to enable mapping the BoK to the content in conceptual modules, to analyze the Taxonomy and to develop a structure for a systematic approach to benchmarking.

4.1.3 IKM Proof of Concept

The information and knowledge represented by the AHRA BoK is the result of many years of effort by participants from several federal departments. From the conception of the AHRA in

2006, federal departments have conducted working groups, published results, constructed tools for implementing an AHRA framework, and provided multiple briefings to departmental and central agency senior management including the governing body - ADM EMC.

The AHRA library was housed within the Centre for Security Science (CSS) and consisted of approximately 1600 files of various formats, structures and conventions. The task of adequately representing the stakeholders and the content of the library presented a challenge. To overcome this challenge, a knowledge management tool was employed to map concepts within the documents.

A three-step process was used to support the BOK work, as described below.

4.1.4 Step 1 – Minimize Redundancy

As a first step to ensure a representative analysis of the knowledge within the library, it was necessary to minimize redundancy in the content so that certain concepts and/or linkages were not artificially strengthened due to repetition alone. This biasing could result from the reuse of material or cycling through multiple drafts of a document before final draft. In some cases, documents never were published as a final version, leaving multiple drafts in the library.

To counter this knowledge biasing, the library was mapped for similarity among documents. When documents were found with 85% or greater similarity, the redundant document was removed. Once the library was distilled for unique pieces of knowledge, 652 documents remained. Focusing on these documents improved BOK team productivity.

4.1.5 Step 2 – Analysis

Secondly, the condensed library was analyzed for conceptual linkages. Based upon algorithms embedded within the software, knowledge tags are derived. Knowledge tags are one to several word(s) that present a discrete entity based upon nouns or combinations thereof. The strength of the concepts are evaluated and then mapped both within the documents and between the documents. The figures below illustrate outputs of the analysis, exhibiting relationships among knowledge tags.

A relational display enables a Subject Matter Expert (SME) to quickly understand conceptual linkages in their knowledge domain. This serves a dual purpose for analysts - to solidify their understanding of the knowledge domain, and to help identify where the weaknesses may be in a set of information.

4.1.6 Step 3 – Support Production of the AHRA BoK

The third step within the scope of knowledge mapping was to utilize the suite of knowledge tags derived from the condensed library to quickly look up key documents to support the writing of the BoK. For example, the suite could be used to look for the concept of Architecture or the references to the Emergency Management Act, instantly allowing the authors to view not only the key documents, but also how the concept is linked to other documents / concepts.

4.1.7 Conclusions

CSS and PS should consider the value of using IKM tools to support the AHRA and other collaborative work, and the creation of web-based libraries of reference material Figures 1&2 show the relation of reference materials contained in the AHRA file repository. The Australian Trusted Information Sharing Network (TISN) [1]capability is a good model of a collaboration resource at the national level.

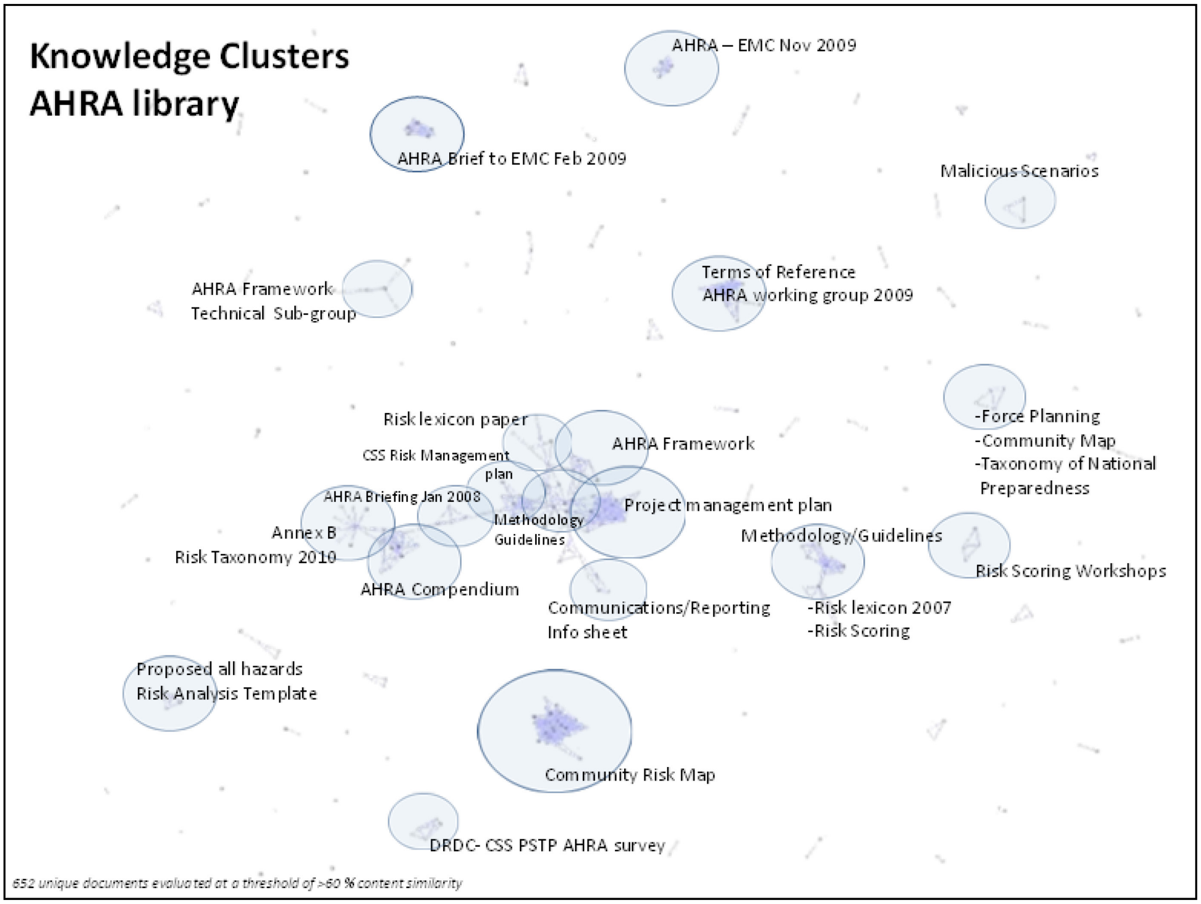


Figure 1 Knowledge Cluster AHRA Library

[1] Australian Trusted Information Sharing Network (TISN) http://www.tisn.gov.au/Pages/default.aspx

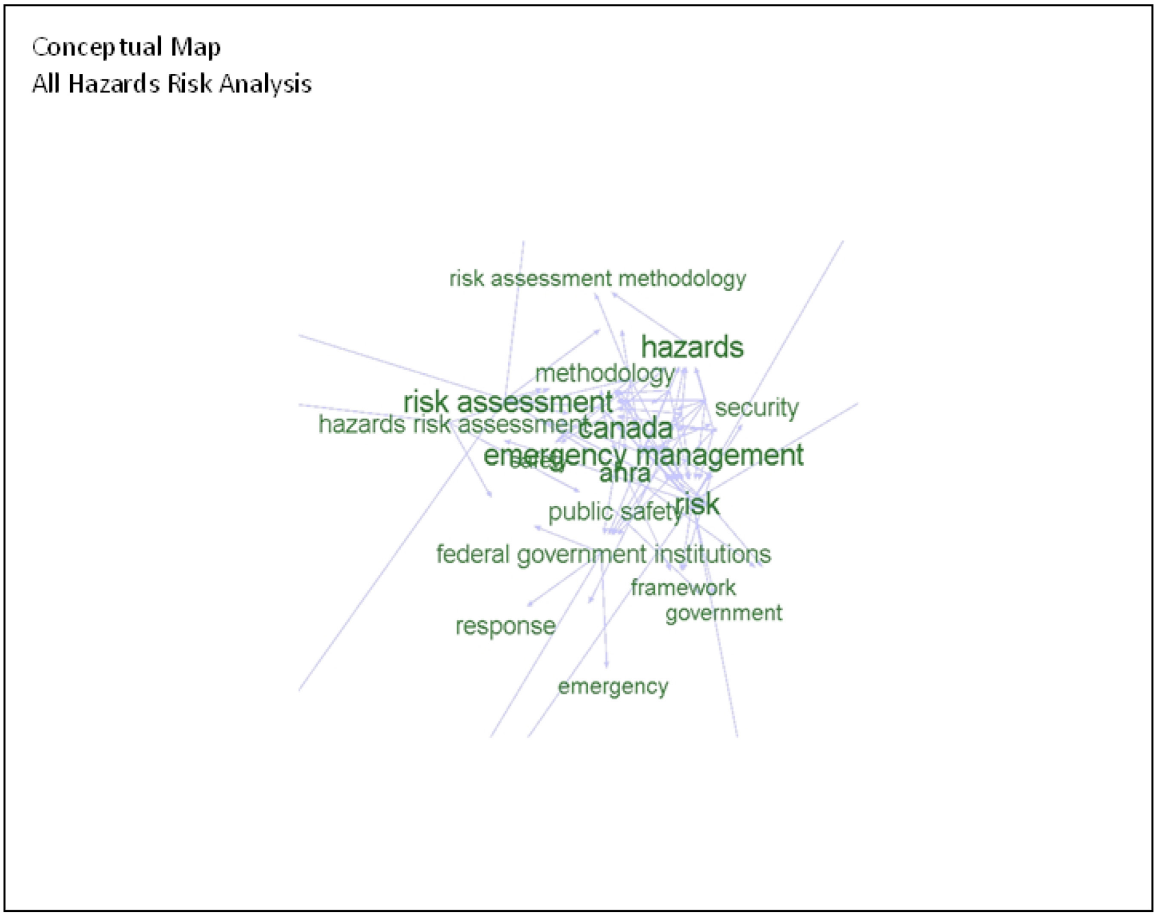


Figure 2 Conceptual Map- All Hazards Risk Analysis

4.2 Mind Mapping Proof of Concept

The BoK team also used a collaborative "mind mapping" tool to demonstrate its potential to support the AHRA activity. Two sample outputs are enclosed – BoK structure, and taxonomy. A third product is included in Folio 7 (benchmarking). The tool was MindJet.

4.2.1 Information Management

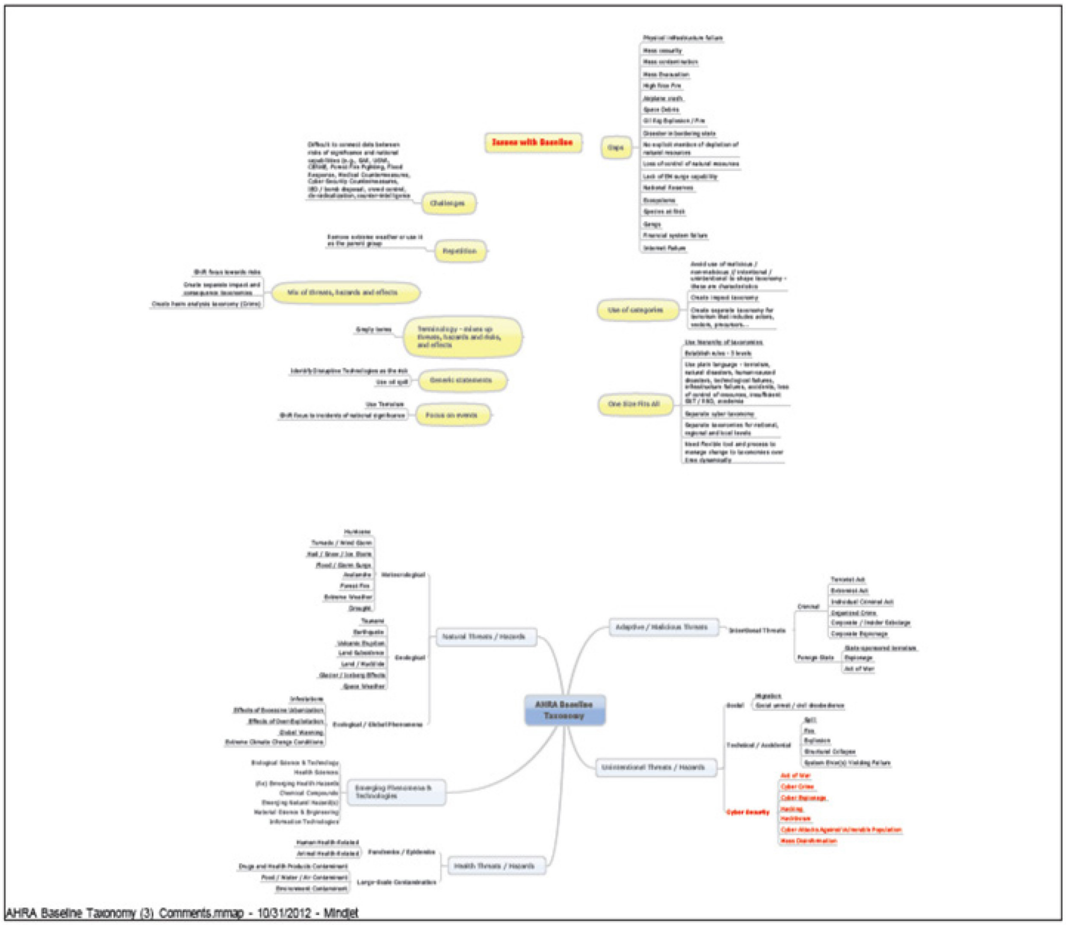
The team was presented with six modules that described the desired content. The Statement of Work is enclosed with this Folio. The mapping tool was used to develop the structure of the BoK and map it to the content in the Statement of Work. During this process, some modifications were made to the BoK structure. It was decided to add chapters on introduction and governance, and to separate the implementation strategy from the transition plan. It was also decided to include a separate chapter called the Exploitation Model. To keep the BoK size to a manageable level given all the content requirements, it was decided to produce two volumes – Volume I -

AHRA Project Overview, and Volume II - Supporting Material. The development of these volumes was supported by reviewing the information contained within the AHRA file repository- see figures 1 & 2.

Separate maps were created for each chapter. For this project, to conserve time, the maps were not used dynamically. One analyst used the tool and distributed the maps (in PDF format) by e-mail to get feedback.

4.2.2 Taxonomy Development

The tool was also evaluated to support taxonomy development and maintenance with the objective of demonstrating a tool that could support collaboration. An advantage of the tool is that it is flexible, and discrete parts of the taxonomy can easily be edited, moved, augmented or replaced. This means that a team could use such a tool to review and update the taxonomy in a dynamic way. Groups could also create and link sets of taxonomies. A sample is contained below



AHRA Baseline Taxonomy (3) Comments.mmap - 10/31/2012 - Mindjet

Figure 3 AHRA Baseline Taxonomy 10/31/2012 MindJet

4.2.3 Benchmarking

A third product was created to demonstrate the use of the tool to map a benchmarking process. Given the broad range of information available on the Web and from other sources, the tool could dynamically record relevant bits, and the analyst could follow his/her intuition but also be able to retrace the steps in the process. The tool could directly link to specific web sites or web-based documents. A sample for benchmarking the US is in Folio 7.

4.2.4 Conclusions

CSS and PS should consider the value of using mind mapping tools to support the AHRA and other collaborative work including more systematic processes such as taxonomy development, community mapping and benchmarking. More systematic and dynamic information management processes would also provide up to date information for OR and Architecture activities.

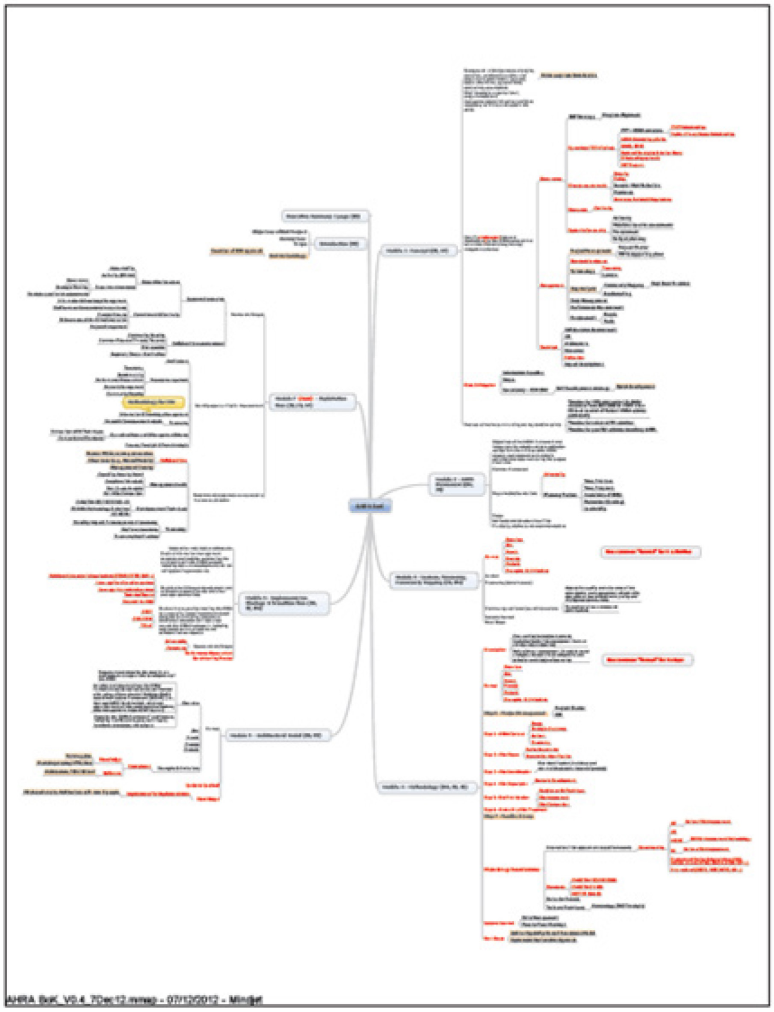


Figure 4 AHRA BoK_V0.4 07/12/2012 - Mindjet

4.3 Statement of work (Extract)

4.3.1 Purpose

This statement of work (SOW) describes the research and development professional services required for a series of special studies that develop and document the All Hazards Risk Assessment (AHRA) from a lessons learned perspective. The requirement is part of a broader effort aimed at capturing and documenting the AHRA 'body of knowledge' for use by decision-makers, policy specialists, operational communities and risk assessment practitioners at all levels.

4.3.2 Background

The Canadian Safety and Security Program (CSSP) is a federally-funded program, to strengthen Canada's ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology (S&T) with policy, operations and intelligence. The CSSP is led by Defence Research and Development Canada's Centre for Security Science (DRDC CSS), in partnership with public safety, response and emergency management organizations, non-governmental agencies, industry, academia as well as provincial and municipal governments. This program builds on the successes, lessons learned and best practices of DRDC CSS's three former programs – the Chemical, Biological, Radiological-Nuclear and Explosives (CBRNE) Research and Technology Initiative (CRTI), the Public Security Technical Program (PSTP) and the Canadian Police Research Centre, which focused on harnessing S&T for the benefit of police and other first responders across Canada.

Through projects, studies, exercises, workshops and other activities, the CSSP creates opportunities, for experts to work with various partners from different public safety and national security fields to support the development of knowledge, tools, processes and strategies that are essential for safeguarding Canada, its people, institutions, and infrastructure. This collaborative model ensures that the best minds from government, industry, academia and international organizations work on the most pressing safety and security issues facing Canadians. CSSP funding will support projects and activities that respond to Canadian public safety and security priorities and address capability gaps. These gaps are identified through risk and vulnerability assessments, consultation with communities of practice, as well as with central agencies, and policy, operational and intelligence entities.

4.3.3 The All Hazards Risk Assessment

The AHRA, led by Public Safety Canada (PS), in close partnership with Defence Research Development Canada (DRDC) – Centre for Security Science (CSS), supports all federal government institutions in fulfilling their legislative responsibility to conduct mandate-specific risk assessments as the basis for EM planning. The AHRA initiative incorporates expertise from a wide range of federal government institutions and applies an all hazards approach. It is a comprehensive and integrated means for assessing the impact and likelihood of both malicious and non-malicious hazards and threats that Canada could face over a five year period. By assessing the risks associated with all hazards in an integrated way, efforts may be broadly effective in reducing the vulnerability of people, property, the environment and the economy. The AHRA's objectives are to:

- Enable federal government institutions to perform AHRA consistently and efficiently as part of their risk management responsibilities under the EMA and other relevant legislation and policies;
- Address the interconnected nature of Canada's risk environment and provide a means to produce a collective judgment of risk assessments currently being carried out by different federal government institutions into a whole-of-government picture to inform future actions and initiatives;
- Support the relative rating of risk events based on their ratings at a federal level, while enhancing decision-making processes within the GC; and
- Capture risks that are significant and are of federal interest.

DRDC CSS is leading an effort to capture the AHRA 'body of knowledge' to help promote the AHRA-like framework model across jurisdictions and to help support informed decision making. The intent is to provide an intellectual framework to assist policy specialists, the operational community, scientists and decision-makers at all levels in exploiting and applying risk assessment and risk management techniques, both of which are essential to sound emergency management practices. A substantial amount of information and literature exists in this area, both in the open literature and in DRDC CSS archival holdings. DRDC CSS requires additional research and development services to support this effort. The outcomes of this work are expected to:

- Raise awareness of a comprehensive risk-based approach that supports the development of core capabilities and investment targets identified in emergency management plans;
- Support the implementation of a shared Framework for the AHRA beyond Emergency Management (EM), including best practices and common tools that would support existing and emerging legislations, strategies, policies and programs (e.g., cyber security; public health, safety and security; the North, etc.); and
- Enable effective risk communications and collaboration among diverse stakeholders, including other jurisdictions, regulators, the public, private sector asset owners, interest groups and international partners.

The subsequent sections of this SOW provide an overview of the general and specific tasks and deliverables required to develop, capture and document the AHRA 'body of knowledge.'

4.3.4 General Tasks / Requirements

The contractor will, during the course of the contract period, lead and/or contribute to the following activities at the direction of the Project Authority (PA) and Technical Authority (TA):

- Meet with the PA/TA [prior to and during the project] to ensure a clear understanding of project requirements is developed, and scope out the parameters that collectively define the set of studies that describe the AHRA;
- Collect and review all available and relevant knowledge, information and data related to the initiation, development and implementation of the AHRA in Canada;
- Assimilate, compile and analyze all relevant and available knowledge, information and data related to the AHRA that can be used for creating and defining the 'body of

knowledge', and provide an objective assessment of the information from a lessons learned perspective;

- Prepare and deliver a series of publications (e.g., lexicon, community mapping, taxonomy, framework, process and methodology, synthesis, etc.) that forms the basis for developing a shared understanding of AHRA in Canada;
- Carry out all relevant and necessary data and information searches from a wide variety of scientific and technical sources (e.g., books, journal articles, government reports, monographs, conference proceedings, etc.), and review and synthesize the literature on risk assessment and risk management;
- Conduct an electronic data capture of all AHRA related products using available COTS software applications for future reference, exploitation and re-use;
- Schedule and conduct interviews with selected Government personnel [as required]. Note, the individuals selected for interviews will be coordinated with and approved by the scientific authorities. The contractor will be required to coordinate with DRDC CSS to collect data from direct observations; and
- Participate in planning sessions with the PA/TA, in order (for example) conduct brainstorm and review progress that allows for any adjustments to the analyses.

4.3.5 Specific Tasks / Work Modules

4.1 Module 1: AHRA Concept

- Document the background research on the role and historical evolution of the AHRA concept;
- Identify and define the vision/conceptual origins of the AHRA, trace its subsequent evolution, and its relationship to other risk programs in government;
- Analyze the purpose and scope of the AHRA, including timeframe, the types of risks addressed, constraints/restraints, and critical assumptions;
- Examine the reasons for advancing the AHRA concept, in particular the strategic, organizational, programmatic and management/administrative conditions necessary to initiate and sustain the AHRA;
- Identify risks and implications to the AHRA concept that were encountered along the way, and document any mitigation schemes; and
- Produce a timeline summarizing the key decision points related to historical development and evolution of the AHRA.

4.2 Module 2: AHRA Framework

- Produce a report summarizing the detailed objectives of the AHRA framework that integrates all analysis and data collection results from the various other AHRA reports and research and analysis activities that occurred during the project timeframe;
- Develop, document and capture a common framework for the AHRA, including the language structure, process, methodology, reporting and relationship to capability investment/maturity model;
- Synthesize the key principle/foundations that underlie the AHRA and examine the elements that a valid AHRA initiative should specifically address;
- Provide a complete description of the AHRA framework, including the full scope of what the AHRA Framework is required to be and do;
- Assess the various attributes and structural qualities necessary for producing an AHRA; and

- Formulate practical guidelines and recommendations on options for conceiving, designing and building a comprehensive and unified AHRA framework that can be adapted to fit the public safety and security/emergency management context.

4.3 Module 3: AHRA Lexicon, Taxonomy & Community Mapping

- Identify and define how the AHRA was supported by the development of a lexicon/common vocabulary and community mapping exercise;
- Discuss the relationships and interactions that were required between departments as part of developing the AHRA lexicon and community mapping exercise;
- Discuss and examine the role of the taxonomy in structuring and communicating the breadth of the 'domain space';
- Examine the mutual departmental awareness and contributions that assisted in the development of the lexicon and community mapping;
- Analyze how the lexicon was understood, debated and tested in the context of the AHRA, and how the community mapping exercise influenced the AHRA development process; and
- Assess the quality and relevance of the consultation and engagement of scientific, operational/law enforcement, policy and intelligence communities in preparing the AHRA, including the level of effort of all stakeholders required to support the AHRA.

4.4 Module 4: AHRA Methodology and Process

- Identify and define the overarching themes/components of the methodology and process that were used for conducting the AHRA;
- Provide a description of the analytical basis that was used for assessing the risks from an all-hazards perspective, including roles and responsibilities, process, methodology, relationship to the higher order policy and strategy, and coordination mechanisms;
- Review international risk assessment-based frameworks (i.e., UK National Risk Assessment, Netherlands National Risk Assessment, and US/DHS Strategic National Risk Assessment) that were enforced to obtain best practices and understand how this work was used to shape, influence and refine the AHRA methodology;
- Identify, describe and assess how the various risks (malicious and non-malicious scenarios and vignettes) were identified, including the role of threat assessment, foresight, trend analysis and scenario development, and selection and design of scenarios;
- Identify, describe and assess the methodology used for analyzing the risks associated with the AHRA, including sources, criteria/metrics, procedures to assess the risks in terms of their impact and estimation of likelihood/frequency;
- Identify, describe and assess the risk evaluation process associated with AHRA, including aggregation, calibration, limitations and uncertainties, and the role of expert judgment;
- Provide a comprehensive assessment of the AHRA process, including community engagement, key stakeholder analysis, role of federal lead departments, working group exercises; and
- Evaluate the tools and approaches used for generating the AHRA, including the software for assessing risks (e.g., executable architectures) data collection, visualization techniques, automation, etc. that supports AHRA development and refinement.

4.5 Module 5: AHRA Architecture Model

- Document and describe the need for an architecture to support the development of the AHRA;

- Describe the "AHRA framework" architecture, including its different layers, main inputs, functions, processes, and outputs; and
- Develop and document how the AHRA framework was conceived and experimented with, using a Department of Defense (DoD) based Architecture Framework (DODAF) (i.e., how was AHRA implemented, what was apportionment of resources, communications, data management, responsibilities, etc.).

4.6 Module 6: AHRA Transition & Exploitation Plan

- Examine the issues and challenges involved in the successful exploitation of the AHRA deliverables;
- Compile information (lessons learned, best practices, etc.) to be included in a final close-out report to support the transitioning and exploitation of the AHRA;
- Examine the follow-on development and validation process through which the AHRA must go through on the way to its successful transition by DRDC CSS to Public Safety Canada and other end-user communities;
- Explore information management concepts and tools for automating the various steps in the AHRA process, including scenario development and risk ratings/scoring procedures;
- Explore the ways of connecting the AHRA to a capability-based investment model designed for informing investment decisions / allocations of resources around the AHRA framework, including web-based communications and collaborative workspaces; and
- Recommend steps that are expected to improve exploitation.

4.3.6 Deliverable Schedule

The deliverables, developed to the satisfaction of the PA/TA (or adjusted with the PA's concurrence), from this work shall include:

Table 4: Work Breakdown Schedule for AHRA

No.	Deliverables	Format	Schedule
1	AHRA Concept Report	Electronic: MS Word format, PDF (DRDC CSS template)	October 2012
2	AHRA Framework Report	Electronic: MS Word format, PDF (DRDC CSS template)	December 2012
3	AHRA Lexicon & Mapping Report	Electronic: MS Word format, PDF (DRDC CSS template)	January 2012
4	AHRA Methodology Report	Electronic: MS Word format, PDF (DRDC CSS template)	February 2012
5	AHRA Architecture Report	Electronic: MS Word format, PDF (DRDC CSS template)	February 2012
6	AHRA Transition & Exploitation Plan	Electronic: MS Word format, PDF (DRDC CSS template)	March 2012

5 Folio 5: Additional figures[2]

AH Risk Management Framework

Figure 3 illustrates the relationship of risk assessment to the risk management lifecycle[3]. Some proposed modifications to this model and the AHRA methodology are included in The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume I: Establishing and Information Baseline.

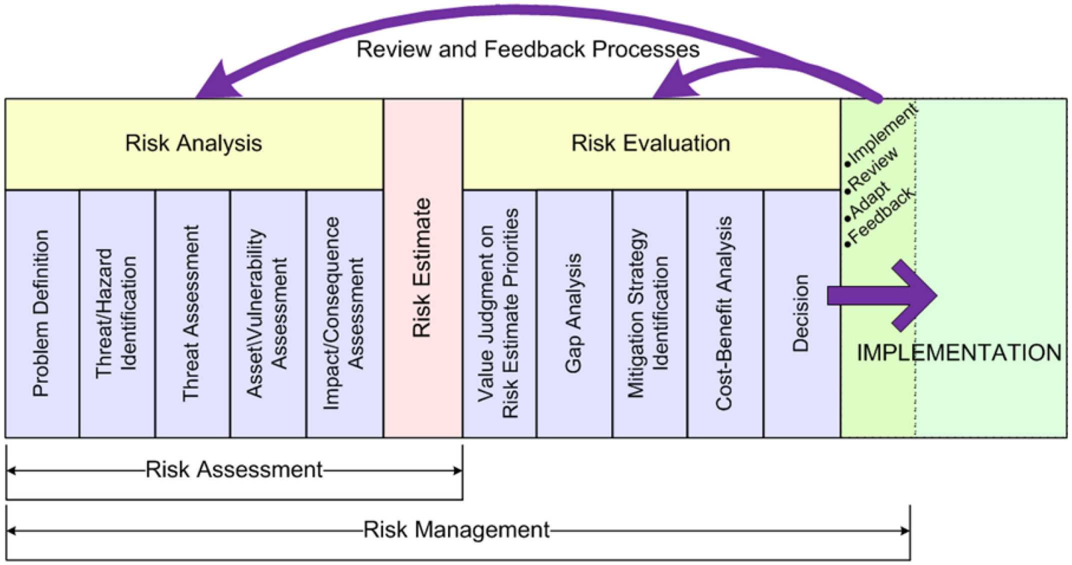


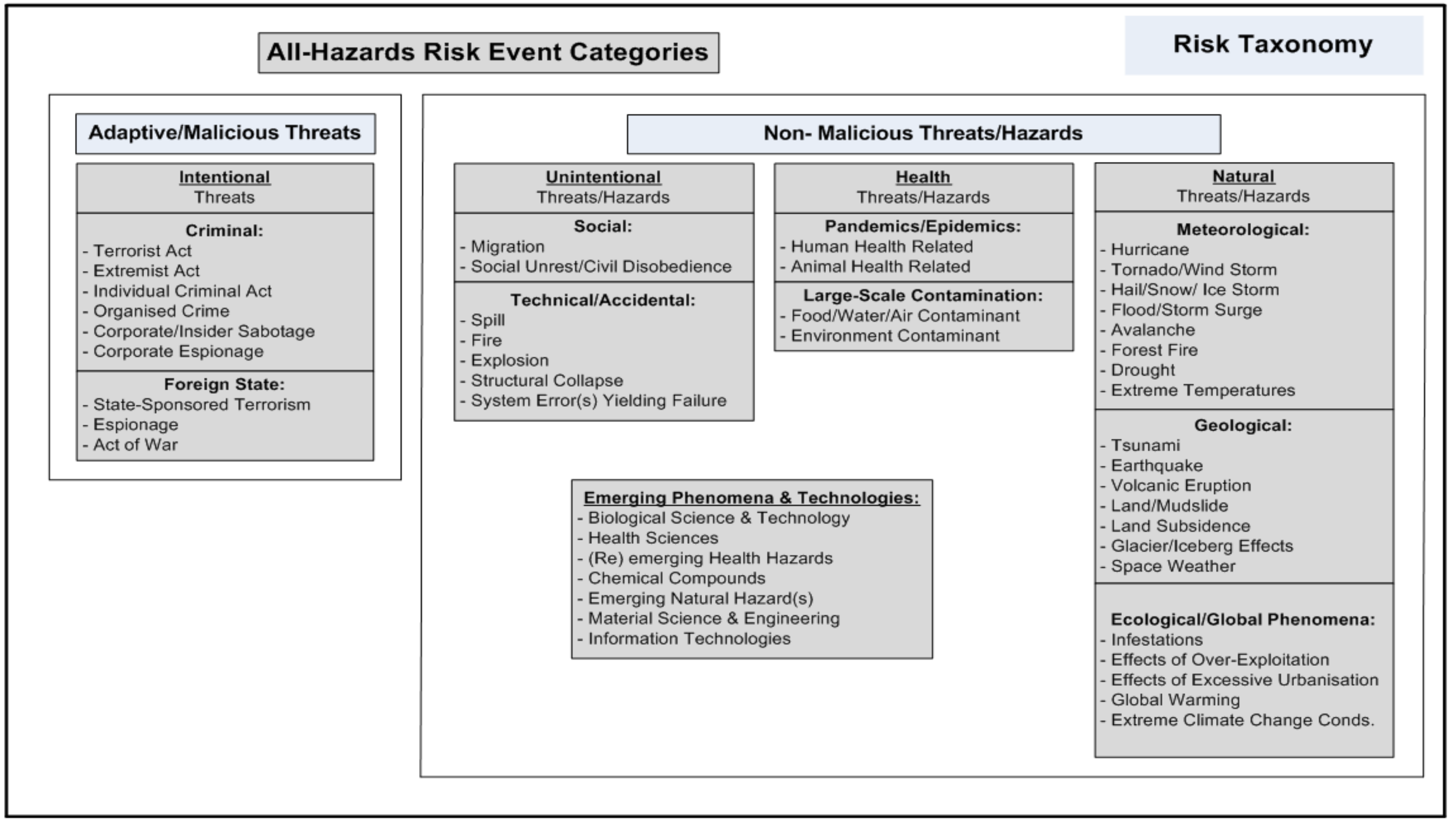
Figure 5 Relationship of risk assessment to the risk management lifecycle

[2] The figures used in The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume I: Establishing and Information Baseline[2] are listed in that volume. Some additional figures are included in Volume II to constrain the size of Volume 1

[3] Verga, S., Dr.; A Holistic, Cross-Government All Hazards Risk Assessment, CSS, 2012

Taxonomy

Two views of the AHRA taxonomy are presented – one from 2008, and the one that is in the PS AHRA Methodology Guidelines (2010).



All-Hazards Risk Event Categories

Risk Taxonomy

Adaptive/Malicious Threats

Intentional Threats

Criminal:
- Terrorist Act
- Extremist Act
- Individual Criminal Act
- Organised Crime
- Corporate/Insider Sabotage
- Corporate Espionage

Foreign State:
- State-Sponsored Terrorism
- Espionage
- Act of War

Non- Malicious Threats/Hazards

Unintentional Threats/Hazards

Social:
- Migration
- Social Unrest/Civil Disobedience

Technical/Accidental:
- Spill
- Fire
- Explosion
- Structural Collapse
- System Error(s) Yielding Failure

Health Threats/Hazards

Pandemics/Epidemics:
- Human Health Related
- Animal Health Related

Large-Scale Contamination:
- Food/Water/Air Contaminant
- Environment Contaminant

Natural Threats/Hazards

Meteorological:
- Hurricane
- Tornado/Wind Storm
- Hail/Snow/ Ice Storm
- Flood/Storm Surge
- Avalanche
- Forest Fire
- Drought
- Extreme Temperatures

Geological:
- Tsunami
- Earthquake
- Volcanic Eruption
- Land/Mudslide
- Land Subsidence
- Glacier/Iceberg Effects
- Space Weather

Ecological/Global Phenomena:
- Infestations
- Effects of Over-Exploitation
- Effects of Excessive Urbanisation
- Global Warming
- Extreme Climate Change Conds.

Emerging Phenomena & Technologies:
- Biological Science & Technology
- Health Sciences
- (Re) emerging Health Hazards
- Chemical Compounds
- Emerging Natural Hazard(s)
- Material Science & Engineering
- Information Technologies

Figure 6Taxonomy 2008

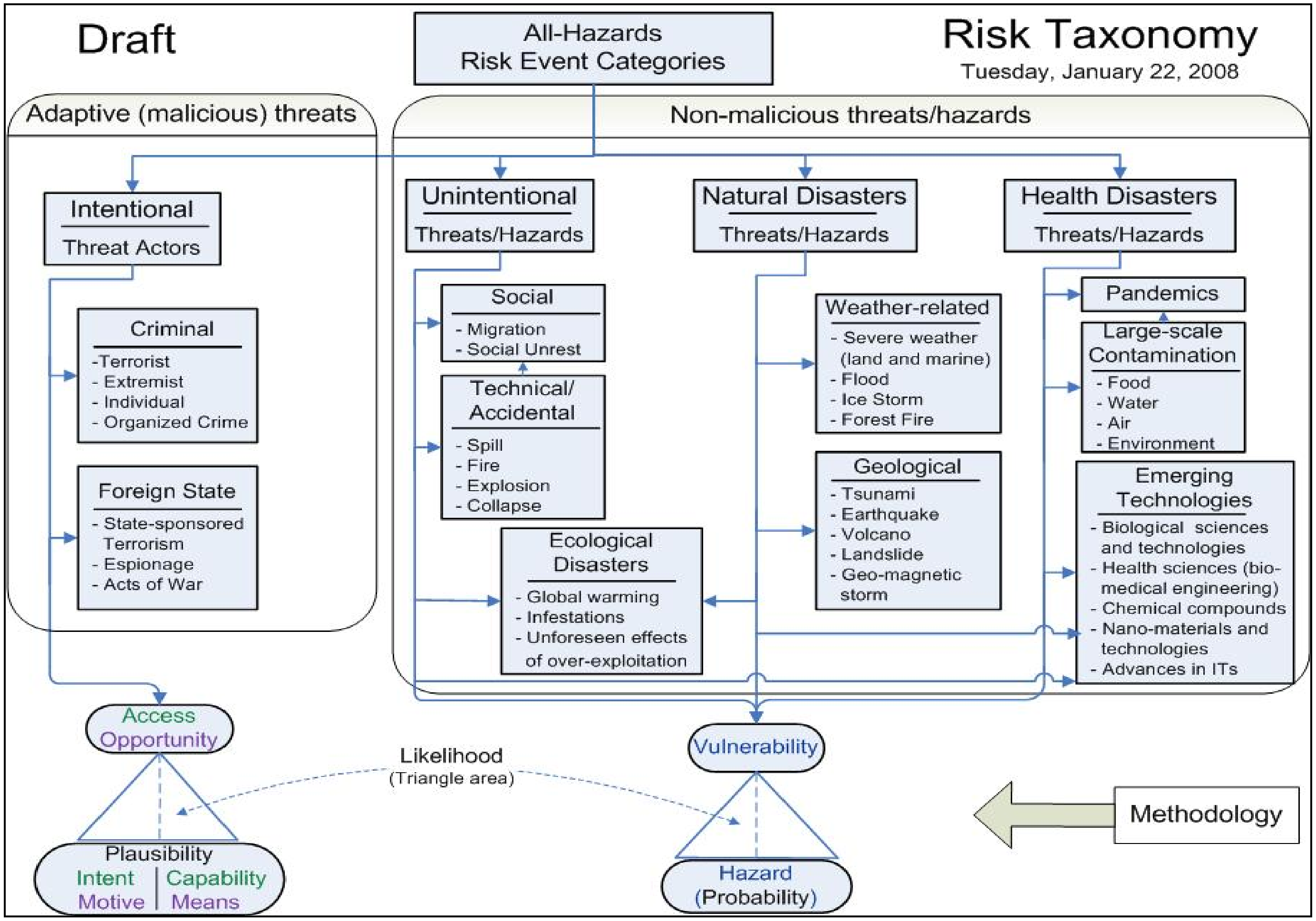


Figure 7Taxonomy 2010

Table 5 All Hazards Threat/Hazard/Risk Category

All Hazards Threat / Hazard / Risk Categories		
Security Threats	**Hazards**	**Natural Disasters**
Criminal**:** • **Treason** • **Terrorism** • **Religious extremism** • **Individual Criminal Act** • **Organized Crime** • **Espionage against the government** • **Industrial espionage** • **Sabotage** • **Violation of air cargo security regulations** • **Violation of border control measures**	**Societal**: • Poverty • Unlawful assembly • Violent protest or activism • Gangs • Radicalization • Corruption • Unethical conduct • Identity theft • Invasion of privacy • Extreme vandalism (e.g., national monument & icons) • Uncontrolled urbanization and development	**Extreme Weather**: • Hurricane • Tornado / wind storm • Hail / snow / ice storm • Avalanche • Forest Fire • Drought • Heat wave • Un-navigable waters • Flooding
Foreign State: • **Failed or failing state-sponsored terrorism** • **State-owned Enterprise (SOE) purchase of Canadian assets** • **Espionage; Act of War; Piracy** • **Human trafficking; Money Laundering**	**Technological / Accident / Safety:** • Oil spill of national significance • Fire or explosion • Physical infrastructure failure (tunnels, bridges, dams, roadways…) • IT infrastructure failure (communications, command and control, surveillance, warning systems…) • Cascading system failure • Transportation accident with hazardous materials • Failure of HAZMAT storage system • Failure of power grid • Aviation accident	**Geophysical**: • Earthquake, Tsunami • Volcanic eruption • Land / mudslide • Land subsidence • Glacier / iceberg melting • Space weather and debris
Cyber Security: • **Act of War** • **Cybercrime** • **Cyber-espionage**	**Health Hazards / Capabilities** Infectious Disease • Human or animal-borne infectious disease • Water or plant-borne infectious disease	**Environment:** • Uncontrolled use of pesticides • Infestations • Exploitation of scarce resources and vulnerable

• **Cyber-attacks against vulnerable populations** • **Security and privacy reaches of national significance** • **Unauthorized access to information** • **Denial of service** • **Mass disinformation**	• Inadequate surveillance or detection capability • Insufficient vaccine production and distribution capacity Emergency Medicine • Insufficient national coverage and slow response time for rural and remote areas Medical Countermeasures • Insufficient detection, avoidance and early warning capability	ecosystems • Adaptation fails to address climate change • Destruction of Arctic ecosystems and way of life • Failure of ecosystems, sensitive marine areas or species at risk
Large-scale Incidents • **Insufficient capacity for mass decontamination, casualty or evacuation** • **Pharmaceutical & health product contamination or shortage** • **Insufficient emergency services to respond to large-scale disaster** • **Major disruption to financial services**	• **Disruptive Technologies** • Lack of industrial S&T capability to deal with future threats • Unregulated chemical compounds • Unregulated food product contamination Insufficient focused S&T / R&D investment	

6 Folio 6: Terms of reference

This section includes terms of reference for the AHRA Pilot Project. Other relevant terms of reference that should be consulted during the planning phase for a national strategy include: governing body the Associate Deputy Minister Emergency Management Committee (ADM EMC); and the Senior Officials Responsibility for Emergency Management (SOREM). A conclusion from the BoK is that a new approach will be needed for a national strategy tailored for different regions in which the Government of Canada takes a supporting role. While defining terms of reference, roles and responsibilities and structural relationships are useful, it will also be important to consider the how-to's. For example, the Centre for Security Science (CSS) is developing a how-to guide for capability assessment. There is probably a requirement to produce a how-to guide for AHRA as both a methodology and a multi-criteria risk assessment technique, along with other techniques.

INTER-DEPARTMENTAL WORKING GROUP
ON THE ALL-HAZARDS RISK ASSESSMENT FRAMEWORK
ESTABLISHING A REQUIREMENT

Table 6 Terms of Reference

Mandate
• (Insert the final decision from the ADM-EMC) • ADM-EMC supports a further investigation of the requirement and concept for an All-Hazards Risk Assessment (AHRA) Framework Initiative through the engagement of an ad-hoc interdepartmental Working Group to examine three questions: o Is there a requirement for a federal government-level All-Hazards Risk Assessment framework? o If so, what would be the nature, scope and dimension of this framework? and o How can Science and Technology (S&T) play a role in moving this item forward? • The Working Group will report back to ADM-EMC, within the next two to three months, with the findings in the form of a White Paper on All-Hazards Risk Assessment and the associated government role.
Background
• In the fall of 2006, the RCMP Critical Incident Preparedness and Response initiative published an integrated risk management report identifying the need for a common All-Hazards Risk Assessment picture for the Government of Canada. The Department of National Defence (DND) Canada Command also identified this need in its survey of the Canadian operational environment. • In 2007, an Intelligence Expert Group on Domestic Security was charged by the Intelligence Assessment Coordinating Committee (IACC) to develop a national All-Hazards Risk Assessment. The IEG sought the expertise of DRDC Centre for Security Science (CSS) to assist with the project management aspects and the coordination of the S&T contribution in the development and demonstration of an

All-Hazards Risk Assessment framework. The IEG, which at the outset represented exclusively federal departments and agencies with mandated intelligence capacities, grew to include some 20 federal departments and agencies that share responsibility for assessing and monitoring various risks to the safety and security of Canadians.

- The IEG recognized that the scope of the all-hazards risk issue reached beyond the intelligence domain and sought direction as to the way forward. Following a series of meetings and discussions involving PCO, it was suggested that the item be brought forward to a senior committee for discussion and guidance on the way forward.
- A number of existing and recent government policies and initiatives, for instance the Emergency Management Act (EMA), have generated a demand for expertise in the field of risk assessment and risk management in general. It remains very important to establish the need for something like an All-Hazards Risk Assessment initiative and assign to it appropriate priority and resources.
- There has also been a rise in interest in the psycho-social domain with issues like radicalization getting increased attention. An important area of risk deals with the psycho-social or human aspects of decision making, and the concepts of risk perception, risk tolerance and risk communication.
- There is no declared government entity that has built a risk analytical capability and provided that expertise in the form of advice and guidance.

Potential Benefits

- There are a number of reasons why we might want to promote a whole-of-government solution for All-Hazards Risk Assessment:
    - To provide consistent advice and analytical expertise;
    - Promote a common understanding of the underlying principles around risk and risk assessment, all the while leveraging on the body of knowledge in government, academia and industry;
    - Establish capacity able to research, guide and assist with the implementation of AHRA frameworks, and support analysis;
    - Provide a capacity to integrate and/or fuse multiple risk assessments into a common risk picture or view;
    - Build an adequate capacity to leverage collaborations with international partners and take advantage of a larger body of knowledge and expertise; and
- Naturally, sufficient capacity would be required in order to ensure the appropriate level of coordination and management of the above, as well as to take advantage of the potentially large body of knowledge generated.

ADM-EMC Observations

- The ADM-EMC members expressed a number of observations that will be considered by the Working Group. Here is a sample:
    - Current resource constraints and the number and diversity of issues being managed by the departments/agencies; (i.e. will this add to this burden?)
    - The need for any initiative to deliver results in a reasonable timeframe and the need to be EMA (or other policy) compliant; (i.e. will we have adequate policy cover?)
    - Fundamental differences in the management of natural hazards versus security threats;

    - The vocabulary (lexicon) seen as a fundamental issue to be resolved;
    - The challenges posed by any whole-of-government solution and the associated complexity in implementing; and
    - Assuming we had a risk assessment process for the government of Canada, would it apply equally across government, bearing in mind the need to characterize the approach to the appropriate issue?

Scope

- Identify the Working Group representatives from amongst the list of EMC member departments and maintain a current list.
- Establish the additional membership needed to cover the spectrum of All-Hazards.
- Convene two to three meetings/workshops or other activity, as necessary, in order to fulfill the WG's mandate.
- Capture the results of the consultation in a consolidated document (White Paper) that will be circulated to member departments for review prior to submitting to the ADM-EMC for decision.
- Note: Due to departmental obligations and ongoing commitments, the meetings and consultations will be kept to the minimum possible to fulfill the mandate.

Chair and Membership

- PS _(TBA)__ and PCO _(TBA)__ are to jointly oversee and manage the execution of the WG's mandate.
- The AHRA WG will be co-chaired by ____(TBA)____, PS and ____(TBA)___, PCO.
- Membership in the AHRA WG is open to Federal departments and agencies that are represented at the ADM-EMC.
- Additional WG members from non-EMC departments/agencies, identified to fulfill the mandate of the WG, will be referred to the EMC Secretariat for a decision.
- Other participants (which may include private sector, academic or other departmental risk experts) may be invited by the co-chairs, on an ad-hoc basis, as determined by the subject-matter being discussed.
- The WG will convene a first workshop/meeting in early April 2009, and conclude its activities and report findings by not later than 30 June 2009.
- The WG will report to the ADM EMC as necessary during the consultation, and at the conclusion.
- The DRDC CSS will initially provide the staff resources for the secretarial and management functions during the Working Group consultations.
- The EMC Secretariat will coordinate the distribution of the draft and final reports to the EMC departments.

Deliverables

- Revised community map of WG members and represented departments.
- Updated All-Hazards risk taxonomy of risk events with correspondence to the departmental mandates.
- Minutes or reports, as required, summarizing the major issues, findings and recommendations discussed by the WG at the workshops, meetings or other activity.

- In answer to the mandated questions, a final report summarizing the membership, consultative activities, key findings, recommendations, and options for the way ahead, including the governance.
- PowerPoint presentation summarizing the previous findings to be presented to ADM-EMC at the conclusion.

Key Assumptions

- ADM EMC members will assign a representative to the WG who will possess sufficient experience and knowledge in the department/agency's role and their risk management activities and responsibilities.
- The WG co-chairs and/or their representative will be communicating directly with the WG members as department/agency representatives on the WG.
- DRDC CSS is committed to furthering the exploration of risk assessment fundamentals and knowledge, as they apply to all-hazards, in the formulation of Public Security S&T Program investment priorities.

Critical Path

- End March 2009: Approval of the Terms of Reference – AHRA WG.
- Mid-April 2009: First of a series of inter-departmental consultations.
- End May 2009: End of consultations.
- Mid-June 2009: Draft report out for review.
- End June 2009: Final report tabled and briefing to ADM EMC on findings.

Budget

- Department contributions in the form of staff time allocated towards the WG consultations within the existing funding levels of participating federal departments and agencies.
- Secretarial and associated costs for the WG consultations will be absorbed and captured by the DRDC CSS, under its Public Security S&T Programs.

7 Folio 7: International benchmarking framework

The AHRA activity has done some ad hoc benchmarking of other nations' approaches to national risk assessments. Public Safety has initiated dialogue with other jurisdictions (P/T/FNI) on a broad range of EM topics including critical infrastructure protection, which automatically links to cross-border capabilities. CIP and EM capabilities are mainly managed at the P/T/FNI levels. It is assumed that this outreach includes discussions about sharing information, collaborating on risk assessments, and adapting federal tools such as the AHRA and capability assessment methodologies.

It is envisaged that a more systematic approach to benchmarking would consider the following requirements:

- Support collaborative risk assessments;
- Provide relevant information that can be dynamically updated;
- Support a process that is repeatable, traceable and sustainable;
- Includes non-traditional sources (e.g., other nations and cultures that experience significant incidents on a regular basis; and other stakeholders such as the insurance industry, professional associations, and non-government and not-for-profit organizations…);
- Benchmark outputs can be included as a layer in an architecture tool;
- Outputs can be viewed, modified and used on a mobile device; and
- Benchmarking is included in the PS AHRA annual business cycle, possibly including links to existing institution mandate-focused environmental scans.

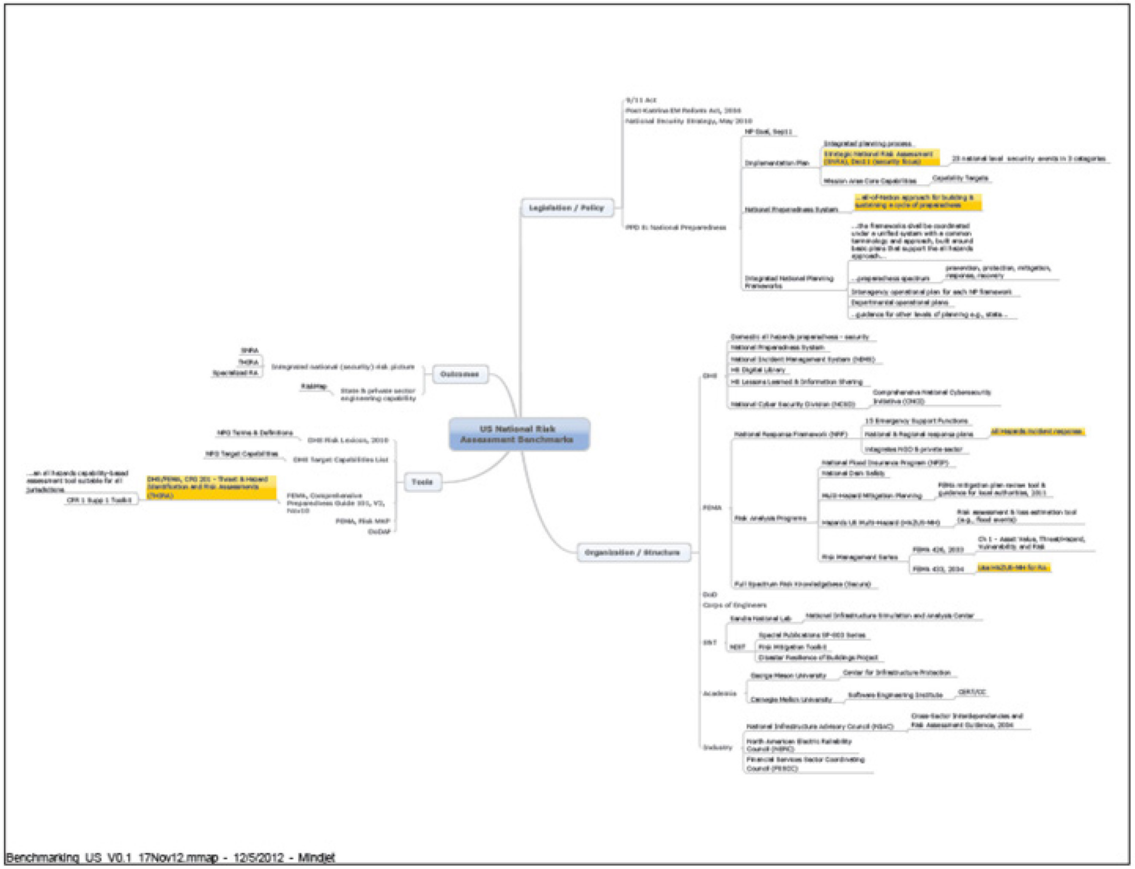

US National Risk Assessment Benchmarks
Legislation / Policy
9/11 Act
Post-Katrina EM Reform Act, 2006
National Security Strategy, May 2010
PPD 8: National Preparedness
NP Goal, Sept11
Implementation Plan
Integrated planning process
Strategic National Risk Assessment (SNRA), Dec11 (security focus)
23 national level security events in 3 categories
Mission Area Core Capabilities
Capability Targets
National Preparedness System
...all-of-Nation approach for building & sustaining a cycle of preparedness
Integrated National Planning Frameworks
...the frameworks shall be coordinated under a unified system with a common terminology and approach, built around basic plans that support the all hazards approach...
...preparedness spectrum
prevention, protection, mitigation, response, recovery
Interagency operational plan for each NP framework
Departmental operational plans
...guidance for other levels of planning e.g., state...
Outcomes
Integrated national (security) risk picture
SNRA
THIRA
Specialized RA
State & private sector engineering capability
RiskMap
Tools
DHS Risk Lexicon, 2010
NPG Terms & Definitions
DHS Target Capabilities List
NPG Target Capabilities
FEMA, Comprehensive Preparedness Guide 101, V2, Nov10
DHS/FEMA, CPG 201 - Threat & Hazard Identification and Risk Assessments (THIRA)
...an all hazards capability-based assessment tool suitable for all jurisdictions
CPR 1 Supp 1 Toolkit
FEMA, Risk MAP
DoDAF
Organization / Structure
DHS
Domestic all hazards preparedness - security
National Preparedness System
National Incident Management System (NIMS)
HS Digital Library
HS Lessons Learned & Information Sharing
National Cyber Security Division (NCSD)
Comprehensive National Cybersecurity Initiative (CNCI)
FEMA
National Response Framework (NRF)
15 Emergency Support Functions
National & Regional response plans
All Hazards incident response
Integrates NGO & private sector
Risk Analysis Programs
National Flood Insurance Program (NFIP)
National Dam Safety
Multi-Hazard Mitigation Planning
FEMA mitigation plan review tool & guidance for local authorities, 2011
Hazards US Multi-Hazard (HAZUS-MH)
Risk assessment & loss estimation tool (e.g., flood events)
Risk Management Series
FEMA 426, 2003
Ch 1 - Asset Value, Threat/Hazard, Vulnerability, and Risk
FEMA 433, 2004
Use HAZUS-MH for RA
Full Spectrum Risk Knowledgebase (Secure)
DoD
Corps of Engineers
S&T
Sandia National Lab
National Infrastructure Simulation and Analysis Center
NIST
Special Publications SP-800 Series
Risk Mitigation Toolkit
Disaster Resilience of Buildings Project
Academia
George Mason University
Center for Infrastructure Protection
Carnegie Mellon University
Software Engineering Institute
CERT/CC
Industry
National Infrastructure Advisory Council (NIAC)
Cross-Sector Interdependencies and Risk Assessment Guidance, 2004
North American Electric Reliability Council (NERC)
Financial Services Sector Coordinating Council (FSSCC)
Benchmarking_US_V0.1_17Nov12.mmap - 12/5/2012 - Mindjet

Figure 8 Benchmarking 12/5/2012 -MindJet

8 Folio 8: Standards

An output of the Community Mapping technique is identification of generic and domain-specific risk assessment techniques, practices and standards. There are opportunities to use automation support including architecture tools to facilitate comparison of these standards and learning, identifying gaps, and developing strategies to enable implementation and a reasonable level of verification.

The analysis contained in this report leads to a recommendation to extend the AHRA work to include risk treatment decision support. This is not the management of risk, but the techniques and tools to select the right treatment strategy, which is the next step in the risk management process. The standards information layer would consider risk management and risk assessment, including domain-specific standards. An output could be identification of gaps and priorities for the Canadian Standards Association (CSA), industry and others.

This folio includes a brief summary of relevant standards, which illustrates the need for a consistent layered approach that would enable capability assessment and management, and performance measurement on multiple levels. It is envisaged that the use of AHRA techniques including multilevel Community Mapping will help to include standards in the capability development process.

A standards gap analysis activity should be an integral part of ongoing PS activities including: international agreements; and updates of the Federal Emergency Response Plan (FERP), critical infrastructure protection and other plans.

National Standards

CSA publishes multiple standards on public and community safety, including Occupational Health and Safety (OH&S), and the environment. Although the federal government does not have to abide by these standards, P/T and local authorities, and private sector stakeholders in a national program would be familiar with these standards and their related compliance requirements and associated risk assessment practices. Canadian Standards Association (CSA) is currently developing four standards related to climate change.

CAN-CSA/ISO-IEC 31000:2009 Risk management is intended to support harmonization of risk management processes in existing and future standards. It provides a common approach in support of standards dealing with specific risks and/or sectors, and does not replace specialist standards. CAN-CSA/ISO-IEC 31010, Risk assessment techniques identifies 31 techniques (See next folio).

CAN/CSA Z-1600 Essentials Emergency Management and Business Continuity Programs is noteworthy because it converges two, formerly siloed, activities and moves towards a resilience mental model when combined with other risk management specialities (e.g., security, health and safety, supply chain).

Federal Standards, Guidelines and Best Practices

- Government of Canada
    - Harmonized Threat and Risk Assessment Guide (CSEC, RCMP)
    - IRM Management of Risk (TBS)
    - Operational Security Standards for Physical Security, Management of IT Security (MITS) and Business Continuity Plan (BCP) Programs (TBS, PS)
    - Directive on the Departmental Security Plan (DDSP), TBS
    - GC IT Incident Management Plan (IMP), TBS
- Public Safety
    - Emergency Management Planning Guide (EMPG)
    - AHRA Methodology Guidelines
- CSEC
    - IT Security Guidelines (e.g., ITSG 33)
- Shared Services Canada
    - *Future* directives, guidelines and standards on IT security risk assessments

9 Folio 9: Risk assessment techniques and tools

The AHRA Community Mapping activity captured a snapshot of federal techniques and tools. An example is presented below. The short list illustrates the need for an ongoing process to document, analyze and leverage these elements of a future Body of Knowledge (BoK) including extensions to other jurisdictions and sectors.

Federal Capabilities

Table 7Adapted from AHRA Community Mapping (2009)

Organization	Risk Assessment Capability
CBSA	Risk assessments for pre-arrival travellers, air and marine cargo
CNSC	Legislated threat and risk prioritization (various categories of licensees: Class I, Class II, etc.)
CFIA	Animal Health Risk Analysis Framework for Biotechnology-Derived Animals
CFIA	Food Safety Enhancement Program - Hazard Analysis Critical Control Point (HACCP) principles, based on risk assessment
CFIA	Invasive Species Risk Assessment
CSS	Consolidated Risk Assessment (e.g., CBRNE)
DND	Risk Management in CF Operations manual
EC	Environmental Risk Assessments (Canadian Environmental Protection Act (CEPA)
GC CTEC	Cyber Threat Evaluation Centre
GC-wide	Harmonized Threat and Risk Assessment Methodology
GC-wide	Security Assessment & Authorization (SA&A)
HC	Human Health Preliminary Quantitative Risk Assessment Guide for Federal Contaminated
ITAC	Terrorist threat assessments
NRCan	Expert issue-specific risk analysis for resource-related hazards; in-house, all hazards methodology informs emergency management planning (e.g., HAZUS/MH)
PS	Incident Risk Analysis Report to support strategic contingency and action planning
TC	Multi-modal risk assessments at strategic, operational and tactical levels

Other Domains

IT Security

- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE);
- Factor Analysis of Information Risk (FAIR);
- Risk Management Framework (from NIST); and

- Threat Agent Risk Assessment (TARA).

Physical Security

- CARVER (threat an vulnerability assessment)

International

ISO 31010 Risk assessment techniques identified thirty-one risk assessment techniques.

The diversity of techniques illustrates the potential learning curve and data management challenges. It also supports the notion that there is no one-size-fits-all solution, and that the central agencies that are guiding this process (i.e., Public Safety and CSS, RACI section) and possibly, the Primary Departments for significant risks require minimum cadres of dedicated risk and others specialists to sustain a credible national program that can exploit a variety of tools and techniques.

Table 8 This list is a sample of Methods and Approaches for conducting Risk Analysis

Brainstorming	Root cause analysis	Sneak analysis (SA) & sneak circuit analysis (SCA)
Structured and Semi-structured interviews	Failure mode & effects analysis (FMEA) Failure modes, effects and criticality analysis (FMECA)	Markov analysis
Delphi technique	Fault tree analysis (FTA)	Monte Carlo simulation
Checklists	Event tree analysis (ETA)	Bayesian statistics and Bayes nets
Preliminary Hazard Analysis (PHA)	Cause-consequence analysis	FN curves
HAZOP	Cause and effect analysis	Risk indices
Hazard analysis & critical control points (HACCP)	Layers of protection analysis (LOPA)	Consequence – probability matrix
Toxicity assessment	Decision tree analysis	Cost / benefit analysis
Structured what-if technique (SWIFT)	Human reliability assessment (HRA)	Multi-criteria decision analysis (MCDA)
Scenario analysis	Bow tie analysis	
Business impact analysis	Reliability-centred maintenance	

Management Toolkit

The BoK project indicates that there are several possibilities for PS to develop a management toolkit that would support the federal AHRA activity and/or a national risk assessment program on multiple levels including further work on:

- Visualization (e.g., graphics, risk matrices, EM capability indices)

- Risk management planning process models (refer to emerging GC-wide HR work)
- Sector and Regional Risk Profiles (different from risk registers)
- Architectural Viewpoints
- Techniques such as brainstorming, facilitation, mental models, Systems Thinking

10 Folio 10: Preliminary Option Analysis (October 2012)

This analysis is based on experience with various dimensions of GC risk management practices, and with the role of risk assessment in departmental decision making, planning and management systems. It is also based on developing the BoK and experience with the AHRA interdepartmental working groups. The purpose of the analysis is to stimulate dialogue. If Canada desires a national picture of risk exposure to support future investment decisions, then people need to understand the implications of implementing a national program that is credible, relevant and sustainable. Analysis of the requirements for a new *Emergency Management Act,* a *National Security Strategy* and a *National Resilience Strategy* should also be part of the discourse.

Table 9Models for National Program

Options	Advantages	Disadvantages	Deductions
Model A - Federal - GC consolidates institutional risk assessments based on scenarios within departmental mandates ,and assessments are extended to P/T and/or regional levels leveraging regional offices and their networks	• Should leverage existing relationships and GC knowledge of P/T/regions • Should not require new funding mechanisms or violate jurisdictions (F/P/T)	• Could limit diversity, and engagement of industry and public • Federal system is mandate-focused, and does not easily accommodate P/T and other sectors • GC missing support elements (data management, automated tools, performance metrics…)	• Top-down / govt led – as-is federal approach • Could be perceived as exclusive, and limited by federal perspective • **Output** – federal risk profile with institution mandate-specific sub-profiles • Difficult to consolidate, repeat and sustain • Partial risk picture
Model B - P/T/M – federal authorities play a support and facilitation role, including funding. P/T and municipal authorities lead the risk assessment activity. GC develops a consolidated risk picture	• Places lead role closer to risk environment, economy & resources • Should be easier to engage municipal level, and their networks including local industry (issues could be cost, data security and access to intelligence information)	• Requires extensive planning • P/T unlikely to afford full cost & may be limits to industry involvement (may still be seen as GC initiative or just another "consultation"; may not capture national industry perspective)	• Top-down / GC-led – as-is in some jurisdictions • Feds are participant and could support with funding, IT infrastructure and SMEs • **Output** – P/T risk profiles • Difficult to repeat and sustain • Partial risk picture

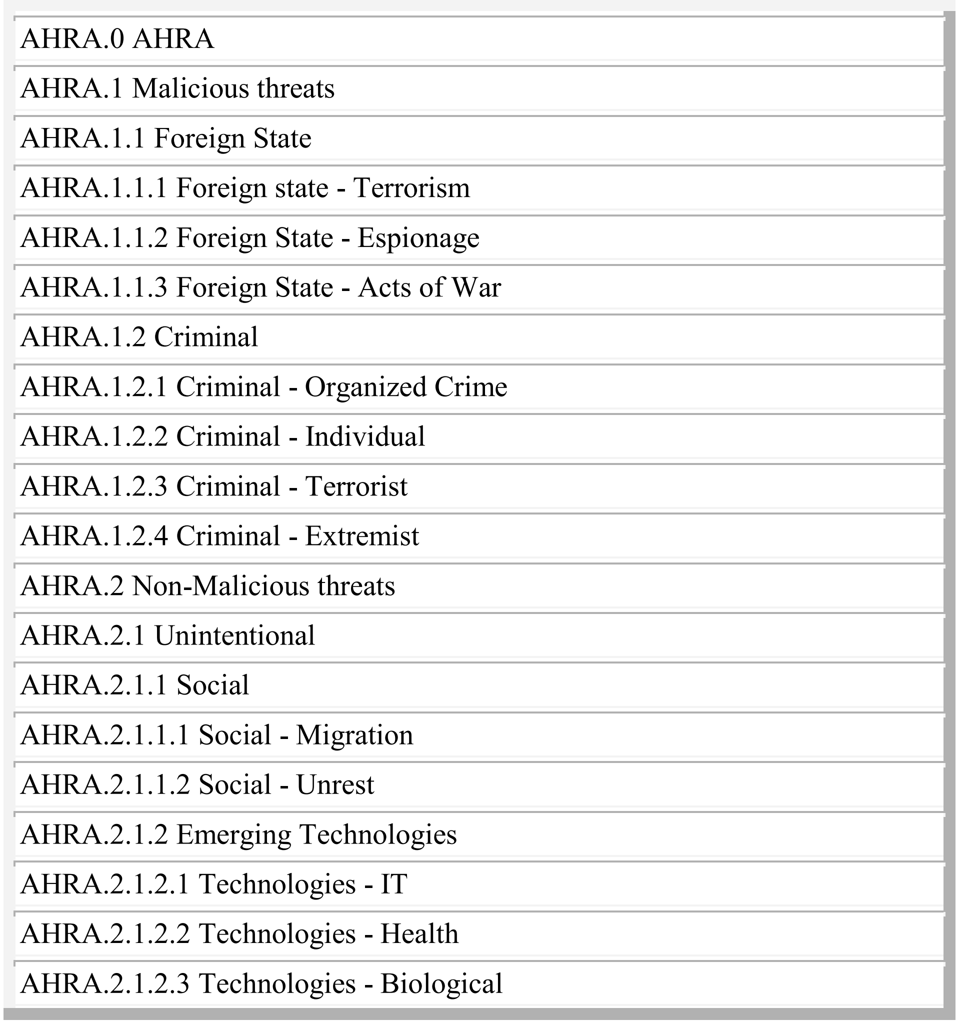
Options	Advantages	Disadvantages	Deductions
	• Lessons learned exist at P/T and local levels	• Risk picture could still be dominated by GC perspective	
Model C - Regional – cross-jurisdictional teams assess risks and produce a consolidated risk picture across P/T, public / private and international boundaries, GC develops a consolidated risk picture	• Should engage industry on multiple levels • Should leverage P/T experience including collaboration with industry and adjacent states • Should consider cultural and vulnerable population dimensions in greater depth • Lessons exist in some domains	• Complicated to transition regional picture to a national collaborative risk treatment strategy (including structural, legislative and S&T enablers) • Complicated to plan and manage • Probably requires full-time dedicated management team, financial incentives and innovative funding mechanisms	• Collaborative model / public / private • Could do one region as a pilot • Should be seen as action-oriented, not just another consultation process • **Output** – regional risk profiles that should be more useful to analyze capability gaps • More comprehensive risk picture
Enabling Option **Model D – Strategic / National** - GC replaces the EM Act to give PS authority, and to establish a Grant system (similar to the US model) that provides sustained commitment implement and sustain a collaborative program, whichever model is chosen	• Variation of Model C with suitable incentives, procurement and funding mechanisms • Fund for supporting infrastructure including: project management; documentation (read out report); and crowdsourcing, web-based risk visualization and other technology enablers)	• Requires new mechanisms • Requires extensive groundwork, planning and follow through • PS may not have the flexibility and resources to manage such a program	• Should be managed as a multi-year program with simplified governance, and build on / adapt or change management structures • Do one region as a pilot and capture lessons from similar P/T/regional initiatives including work by CSS in emergency management domain • Challenges are to define right level of participation to develop a credible risk profile, and then, engage higher levels of management, so that the initiative does not bog down by trying to combine too many perspectives

Options	Advantages	Disadvantages	Deductions
			including the political dimension, and too many levels of management too early in the process • **Strategic Outcomes** – a sustainable program that adds value on all levels of GC, and in industry and the public; and measureable improvements in national security, public safety, and societal resilience; politics-neutral, credible contribution on the international stage

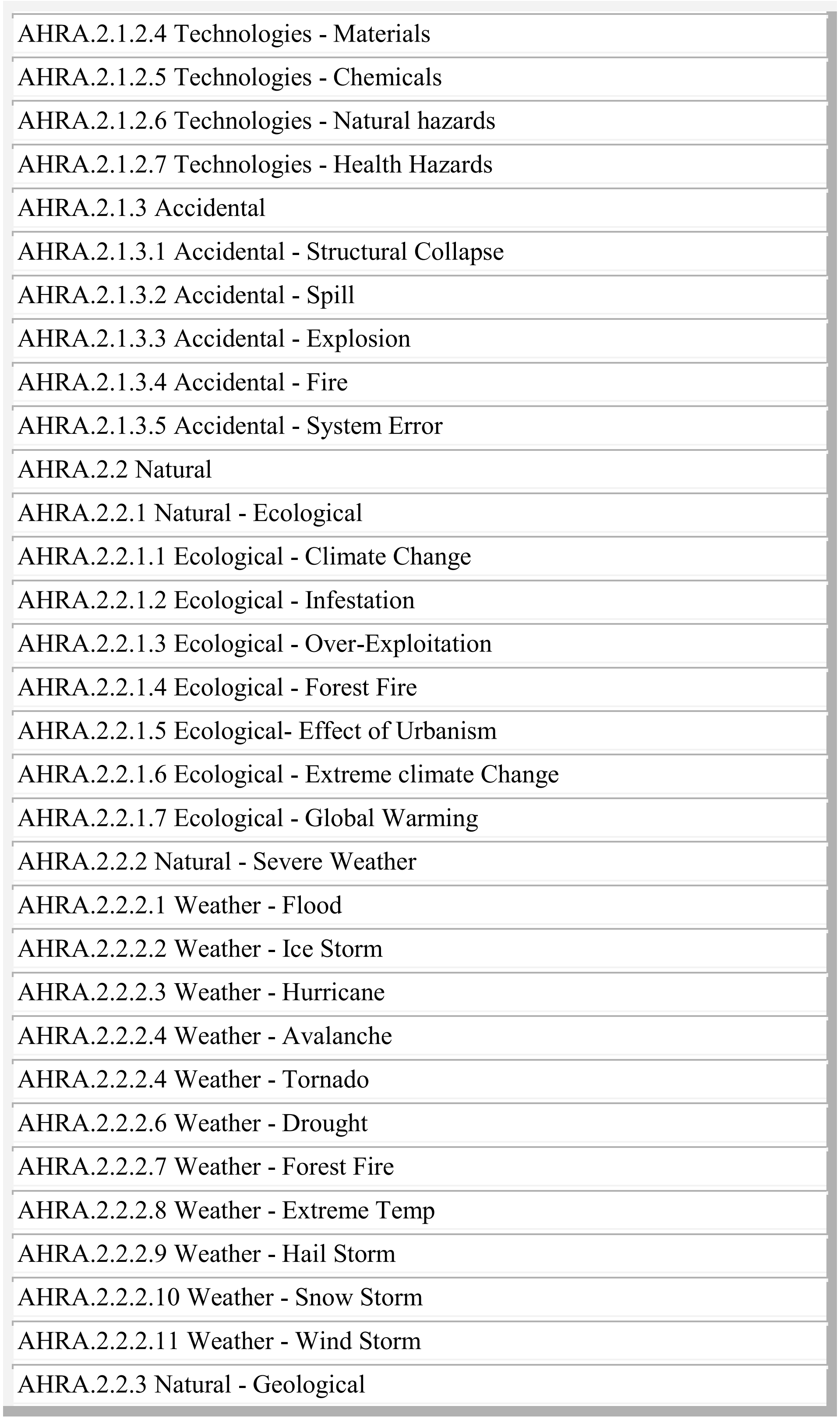
Folio 11: Architecture Viewpoints (Samples)

Architecture – View of Taxonomy

The application of architecture tools and techniques to the federal AHRA permits the development of a characteristic frame that captures the complexity of the problem, with a variety of mandates and overlapping risk domains. A preliminary architecture was built for AHRA in a system engineering application called 'CORE' by Vitech (US). The following shows a possible architecture for the AHRA, which represents successive layers of related information generated through appropriately designed processes. The development of this architecture was exploratory in nature, producing a 'strawman' or model of representative public safety and security capabilities, tasks, functions/operational activities, organizations, and risks to understand what the AHRA framework would look like. In order to apply a proper architecture approach to the AHRA, it is crucial to build, at the outset, an appropriate data model that would be the foundation for future architecture work.



AHRA.0 AHRA
AHRA.1 Malicious threats
AHRA.1.1 Foreign State
AHRA.1.1.1 Foreign state - Terrorism
AHRA.1.1.2 Foreign State - Espionage
AHRA.1.1.3 Foreign State - Acts of War
AHRA.1.2 Criminal
AHRA.1.2.1 Criminal - Organized Crime
AHRA.1.2.2 Criminal - Individual
AHRA.1.2.3 Criminal - Terrorist
AHRA.1.2.4 Criminal - Extremist
AHRA.2 Non-Malicious threats
AHRA.2.1 Unintentional
AHRA.2.1.1 Social
AHRA.2.1.1.1 Social - Migration
AHRA.2.1.1.2 Social - Unrest
AHRA.2.1.2 Emerging Technologies
AHRA.2.1.2.1 Technologies - IT
AHRA.2.1.2.2 Technologies - Health
AHRA.2.1.2.3 Technologies - Biological



AHRA.2.1.2.4 Technologies - Materials
AHRA.2.1.2.5 Technologies - Chemicals
AHRA.2.1.2.6 Technologies - Natural hazards
AHRA.2.1.2.7 Technologies - Health Hazards
AHRA.2.1.3 Accidental
AHRA.2.1.3.1 Accidental - Structural Collapse
AHRA.2.1.3.2 Accidental - Spill
AHRA.2.1.3.3 Accidental - Explosion
AHRA.2.1.3.4 Accidental - Fire
AHRA.2.1.3.5 Accidental - System Error
AHRA.2.2 Natural
AHRA.2.2.1 Natural - Ecological
AHRA.2.2.1.1 Ecological - Climate Change
AHRA.2.2.1.2 Ecological - Infestation
AHRA.2.2.1.3 Ecological - Over-Exploitation
AHRA.2.2.1.4 Ecological - Forest Fire
AHRA.2.2.1.5 Ecological- Effect of Urbanism
AHRA.2.2.1.6 Ecological - Extreme climate Change
AHRA.2.2.1.7 Ecological - Global Warming
AHRA.2.2.2 Natural - Severe Weather
AHRA.2.2.2.1 Weather - Flood
AHRA.2.2.2.2 Weather - Ice Storm
AHRA.2.2.2.3 Weather - Hurricane
AHRA.2.2.2.4 Weather - Avalanche
AHRA.2.2.2.4 Weather - Tornado
AHRA.2.2.2.6 Weather - Drought
AHRA.2.2.2.7 Weather - Forest Fire
AHRA.2.2.2.8 Weather - Extreme Temp
AHRA.2.2.2.9 Weather - Hail Storm
AHRA.2.2.2.10 Weather - Snow Storm
AHRA.2.2.2.11 Weather - Wind Storm
AHRA.2.2.3 Natural - Geological

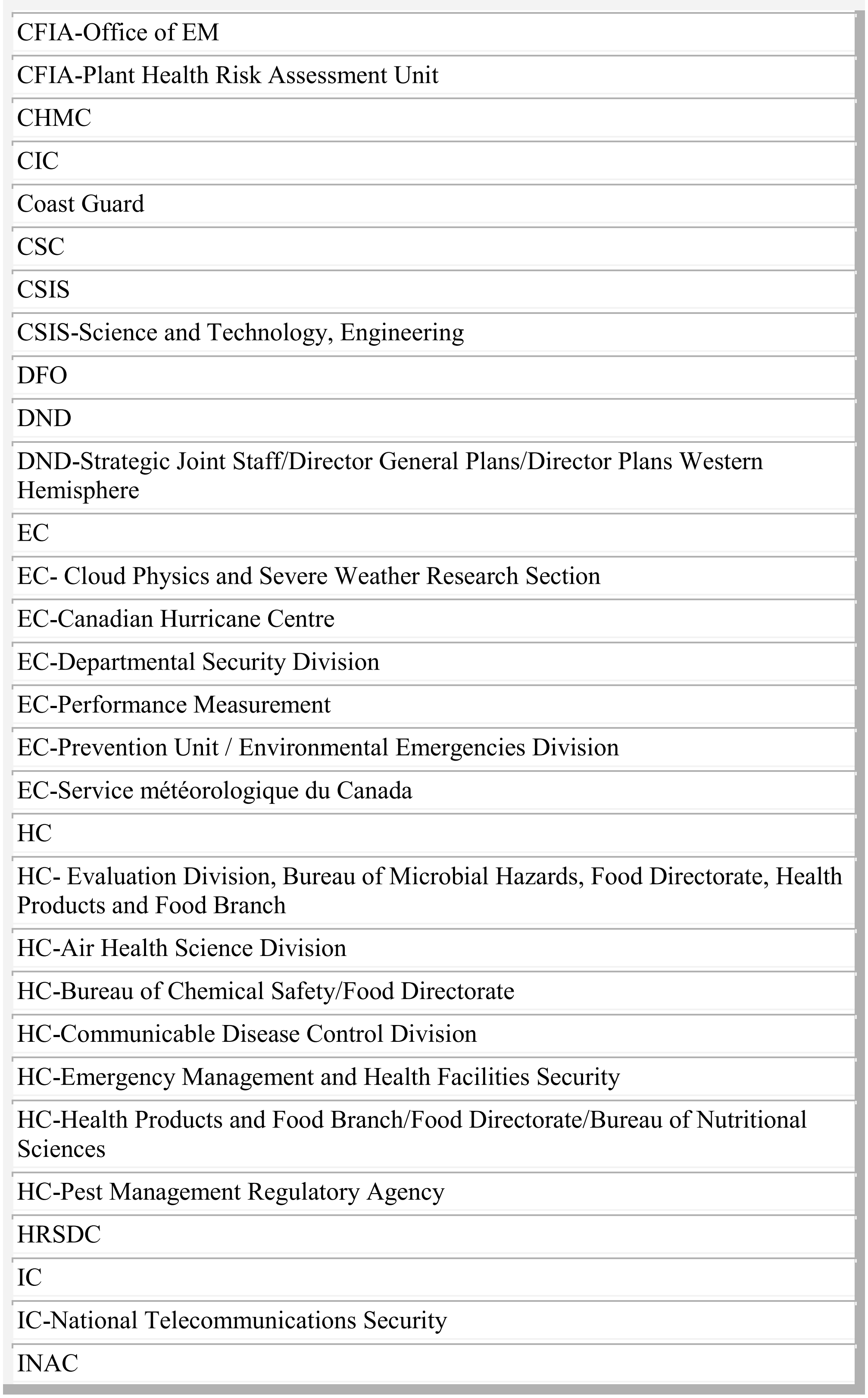
AHRA.2.2.3.1 Geological - Tsunami
AHRA.2.2.3.2 Geological - Volcano
AHRA.2.2.3.3 Geological - Earthquake
AHRA.2.2.3.4 Geological - Geo-Magnetic Storm
AHRA.2.2.3.5 Geological - Landslide
AHRA.2.2.3.6 Geological Land Subsidence
AHRA.2.2.3.7 Geological - Glacier and iceberg
AHRA.2.3 Health
AHRA.2.3.1 Health - Pandemics
AHRA.2.3.2 Health - Large Scale Contamination
AHRA.2.3.2.1 Contamination - Air
AHRA.2.3.2.2 Contamination - Environment
AHRA.2.3.2.3 Contamination - Food
AHRA.2.3.2.4 Contamination - Water
AHRA.2.3.3 Health - Epidemics (animals)
AHRA.2.3.4 Health - Epidemics (human Health related)
AHRA.2.3.5 Health - Pandemics (animals)

Powered by CORE[4]. Generated 09 June 2009.

Operational Node

0 Government of Canada
AAFC
CBSA
CBSA-Intelligence Targeting and Analysis Division
CBSA-National Risk Assessment Centre, Targeting Operations Division
CBSA-Targeting Operations, Air and Marine Goods
CFIA
CFIA-Animal health
CFIA-Corporate Security Services Division

[4] http://www.vitechcorp.com/ accessed October 2, 2013



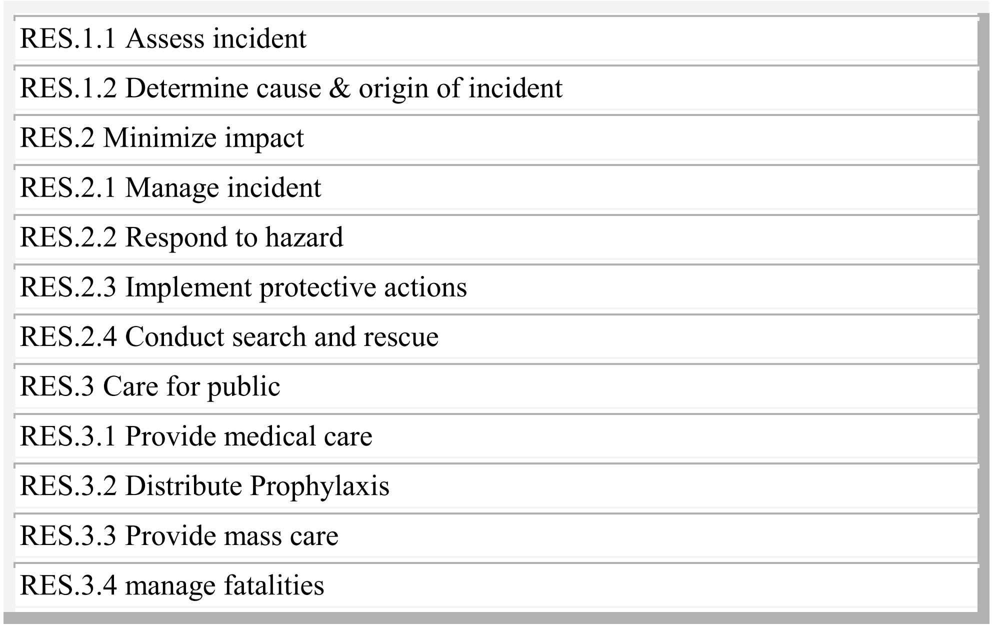
CFIA-Office of EM
CFIA-Plant Health Risk Assessment Unit
CHMC
CIC
Coast Guard
CSC
CSIS
CSIS-Science and Technology, Engineering
DFO
DND
DND-Strategic Joint Staff/Director General Plans/Director Plans Western Hemisphere
EC
EC- Cloud Physics and Severe Weather Research Section
EC-Canadian Hurricane Centre
EC-Departmental Security Division
EC-Performance Measurement
EC-Prevention Unit / Environmental Emergencies Division
EC-Service météorologique du Canada
HC
HC- Evaluation Division, Bureau of Microbial Hazards, Food Directorate, Health Products and Food Branch
HC-Air Health Science Division
HC-Bureau of Chemical Safety/Food Directorate
HC-Communicable Disease Control Division
HC-Emergency Management and Health Facilities Security
HC-Health Products and Food Branch/Food Directorate/Bureau of Nutritional Sciences
HC-Pest Management Regulatory Agency
HRSDC
IC
IC-National Telecommunications Security
INAC

INAC-Emergency and Issue Management Directorate
ITAC
Justice
Municipalities
NRC
NRCan
NRCan-GeoConnections Division/Mapping Information Branch
NRCan-Geological Survey of Canada
OAG
PCO
PHAC
Provinces and Terr
PSC
PSC-Emergency Management and National Security/Critical Infrastructure Policy
PSC-Situational Awareness and Risk Assessment, Operations Directorate
RCMP
RCMP-Critical Infrastructure Criminal Intelligence
TBS
TBS-Corporate Shared Services/Administration and Security Directorate
TBS-Strategic Planning and Reporting, Priorities and Planning
TC
TC-Civil Aviation/Management Services
TC-Emergency Preparedness
TC-Intel Branch
TC-MSI
TC-Safety and Security/ Security Program Support/Security Expertise Programs

Powered by CORE[5]. Generated 09 June 2009.

RES.0 Respond tasks
RES.1 Evaluate incident

[5] IBID



RES.1.1 Assess incident
RES.1.2 Determine cause & origin of incident
RES.2 Minimize impact
RES.2.1 Manage incident
RES.2.2 Respond to hazard
RES.2.3 Implement protective actions
RES.2.4 Conduct search and rescue
RES.3 Care for public
RES.3.1 Provide medical care
RES.3.2 Distribute Prophylaxis
RES.3.3 Provide mass care
RES.3.4 manage fatalities

11 Folio 12: Project Management Tools (Samples)

Serial	References
1	AHRA Framework Project Work Plan, 11 January 2010 see 12.1
2	AHRA PM Major Activities & Timelines, 2011 see 12.2
3	Project Implementation Plan, 2007 (CSS files)
4	Communications Plan, 2007 (CSS files)
5	Information Fact Sheet, 2007 (CSS files)
6	NRA Implementation Strategy (Volume I, Chapter 7)[6]
7	NRA Transition Plan (Volume I, Chapter 8)
8	AHRA Exploitation Concept (Volume I, Chapter 9)

12.1 AHRA Framework Project Work Plan, 11 January 2010

WBS	Tasks	Responsibility L = Lead S = Support[7]	Deliverables	Start	Finish
1.0	**AHRA Framework & Guide**	**PS – L; CSS - S**		**17 Nov 09**	**31 Oct 11**
1.0.1	**AHRA Project Management**	**PS – L; CSS - S**	**Project Plan & Work Plan**	**17 Nov 09**	**29 Jan 10**
1.0.2	Develop Project Plan	PS – L; CSS - S	AHRA Project Plan	1 Dec 09	15 Jan 10
1.0.3	Develop Project Work Plan	CSS – L; PS - S	AHRA Work Plan	1 Dec 09	15 Jan 10

[6] Vol1 DRDC CSS TR 2013-014 The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume I: Establishing and Information Baseline

[7] This version indicates areas where CSS could provide technical advice. Core Advisory Group and Technical Sub-Group participants are in support role throughout the project unless otherwise specified as the project progresses.

WBS	Tasks	Responsibility L = Lead S = Support[7]	Deliverables	Start	Finish
1.0.4	Administration of the project	PS – L; CSS - S		1 Feb 10	31 Oct 11
1.1	**EM Planning Guide**	**PS – L; CSS - S**	**EM Planning Guide**	**17 Nov 09**	**30 Jun 10**
1.1.1	Develop a risk assessment component ("generic primer") to inform the EM planning guide on how to do RAs from an all hazards perspective for the use of federal institutions	CSS – L; PS - S	AHRA component of the Guide	1 Feb 10	05 Mar 10
1.2	**Community Risk Map & Compendium of Existing RA Activities**	**PS – L; CSS - S**	**Community Risk Map & Compendium of Existing RA Activities**	**1 Feb 10**	**30 Jun 10**
1.2.1	Develop survey approach & target audiences	PS – L; CSS - S	AHRA Survey	1 Feb 10	12 Feb 10
1.2.2	Develop survey	CSS – L; PS - S		15 Feb 10	12 Mar 10
1.2.3	Distribute survey	PS – L; CSS - S		15 Mar 10	31 Mar 10
1.2.4	Consolidate and analyze responses	CSS – L; PS - S		1 Apr 10	30 Apr 10
1.2.5	Develop Compendium of existing RA activities	CSS – L; PS - S	Compendium of RA Activities	03 May 10	28 May 10
1.2.6	Develop Community Risk Map	CSS – L; PS - S	Community Risk Map	03 May 10	21 May 10

WBS	Tasks	Responsibility L = Lead S = Support[7]	Deliverables	Start	Finish
1.3	**Federal AHRA Framework[8]**	**PS – L; CSS - S**	**Proposed Federal AHRA Framework**	**1 Feb 10**	**29 Oct 10**
1.3.1	Update existing framework components	CSS – L; PS - S	Baseline AHRA Framework	3 May 10	30 Jul 10
1.3.2	Review other frameworks	CSS – L; PS - S		1 Feb 10	30 Apr 10
1.3.3	Develop a conceptual framework	CSS – L; PS - S		1 Mar 10	31 Mar 10
1.3.4	Experiment with framework	CSS – L; PS - S		1 Apr 10	31 May 10
1.3.5	Validate framework	PS – L; CSS - S		1 Jun 10	30 Jun 10
1.3.6	Develop toolbox	CSS – L; PS - S	E-Based Toolbox	1 Jun 10	29 Oct 10
1.3.7	Update Communications Plan	PS – L; CSS - S		1 Jul 10	30 Jul 10
1.3.8	Develop Federal AHRA Framework	CSS – L; PS - S	Proposed Federal AHRA Framework	1 Oct 10	29 Oct 10
1.3.9	Develop resource estimate	PS – L; CSS - S		1 Apr 10	31 May 10
1.3.10	Obtain commitment and resources for next activity	PS – L; CSS - S		1 Jun 10	31 Jul 10
1.4	**Federal AHRA**	**PS – L; CSS - S**	**Validated Federal AHRA Framework**	**15 Aug 10**	**31 Oct 11**
1.4.1	Plan implementation of one cycle of AHRA	PS – L; CSS - S	Pilot Project Plan	1 Sep 10	31 Dec 10
1.4.2	Develop planning assumptions, scenarios and other guidance	PS – L; CSS - S	Activity-Based Planning Guidance	1 Sep 10	30 Sep 10
1.4.3	Define approach[9]	PS – L; CSS - S	Program Implementation	15 Aug 10	30 Sep 10

[8] Framework may include (but is not limited to): Conceptual Model, Lexicon, Taxonomies (i.e., master and sub-taxonomies – e.g., threats, vulnerabilities, impacts…), Criticality Assessment Criteria, Federal Initial Planning Assumptions, Communications Plan, Implementation Strategy & Plan, Metrics, …

[9] Approach could include: resources, preparation (e.g., training, rehearsal…), schedule, techniques (e.g., surveys, workshops, demonstrations), data collection strategy, metrics, facilities, communications, etc, to ensure a verifiable, repeatable and sustainable activity

WBS	Tasks	Responsibility L = Lead S = Support[7]	Deliverables	Start	Finish
			Plan[10]		
1.4.4	Execute one cycle of AHRA Framework	PS – L; CSS - S	Timeline and Process Flow Diagram	3 Jan 11	31 May 11
1.4.5	Consolidate data and lessons	CSS – L; PS - S		1 Jun 11	30 Jun 11
1.4.6	Develop gap analysis	CSS – L; PS - S		13 Jun 11	29 Jul 11
1.4.7	Develop visualization tools	CSS – L; PS - S		4 Jul 11	31 Aug 11
1.4.8	Develop information lifecycle management plan	PS – L; CSS - S		1 Sep 11	9 Sep 11
1.4.9	Develop Final Report	PS – L; CSS - S	Final Report	1 Sep 11	14 Oct 11
1.4.10	Publish the AHRA results	PS – L; CSS - S	AHRA report publication	12 Sep 11	14 Oct 11
1.7.11	Perform Quality Assurance	PS – L; CSS - S		3 Oct 11	7 Oct 11
1.7.12	Close Out Project	PS – L; CSS - S	Lessons Learned Report	3 Oct 11	21 ct 11

12.2 AHRA Framework Project Work Plan with Key Sub-Activities

AHRA Project Management Major Activities and Timelines

Narratives

- Coordinate storyline around all policy narrative pieces (by Oct 30, 2010)
- Finalize overarching policy narrative (by Oct 1, 2010)

Developing AHRA Framework Process

- Develop AHRA conceptual policy process (by Oct 29, 2010)

[10] PIP could include: governance; outcomes; methodology; scope; assumptions; WBS; schedule; risk and issue management and other processes; budget; responsibility assignment matrix; metrics;…

- Develop Guidelines for process (by Oct 29, 2010)
- Develop Resource Deck for follow-on after the framework is developed (by Jan 30, 2011)

Supporting Products
- Update diagram which links key government risk initiatives (diagram) (by Nov 30, 2010)
- Update community risk map (by Nov 15, 2010)
- Revise English compendium (by Jan 30, 2011)
- Revise French compendium (by Jan 30, 2011)
- Develop Lexicon (by Nov 1, 2010)
- Update definition table (by Nov 1, 2010)
- Revise/Update communications strategy (by Nov 15, 2010)
- Revise/Update EM Planning Guide (by Jun 17, 2011 or Oct 31, 2011)
- Develop/upload PS AHRA Sharepoint site (by Nov 30, 2010)
- Manage email account (Ongoing)
- Co-develop/support development of NATO Risk Conference (by Sep or Oct 2011)
- Develop risk assessment piece for Emergency Management Planning curriculum (by Nov 2011)
- Develop Tools /templates (Risk consultant) (by Feb 28, 2011)

Implementing the Process
- Develop AHRA Call letter for departmental risk assessments and send it out (by Jan 5, 2011; Request responses by Feb 2, 2011)
- Define parameters/criteria checklist (by Oct 15, 2010)
- Compile departmental risk assessments (develop database to record RA's, track, follow-up, consult) (by Mar 2, 2011)
- Develop method to harmonize departmental risk assessments (by Nov 30, 2010)
- Develop scoring grid (By Nov 30, 2010)
- Organize workshops to validate and rate risks (identify the right players, and work out logistics for workshops) (By Mar 30, 2011)
- Host Workshops (By Mar 2 (1st workshop), 9 (2nd workshop) and 16 (3rd workshop), 2011)
- Collaborate with CSS on inventorying data (March 2011)
- Review products developed by the Risk Consultant (tools, methods and timelines for implementing the process, incl. high level engagement strategy) (Ongoing – By Mar 31, 2011)

Engagement
- Prepare gross results for dissemination (By Apr 28, 2011)

- Provide early findings to Senior Management for information and comments (by May 5, 2011)
- Provide gross results to stakeholders for comments (by May 12, 2011)
- Refine gross results in preparation for final report (By Jun 28, 2011)
- *Prepare & action media release, include tweet (by Oct 31, 2011)…if we decide to share publicly*
- Build Internal Stakeholder relationship (CIP, Strategic Planning) (Ongoing)
- Coordinate CAG meeting (On-going; Next meeting to be held in Nov 2010)
- Provide findings to Senior Management for information and decision as required (by Sep 7, 2011)

12 Folio 13: A Holistic, Cross-Government All Hazards Risk Assessment[11]

Simona Verga, PhD
Defence Research and Development Canada,
Centre for Security Science (DRDC CSS)
Ottawa, ON, Canada
email: simona.verga@drdc-rddc.gc.ca

ABSTRACT

This paper describes an approach to build a holistic, cross-government all-hazards risk assessment process, which aims to capture threats of all "stripes" and understand the extent to which they can become a risk to the safety and security of the Canadian population and society. The approach makes a conscious effort to consider the Canadian risk picture within the global risk environment. The federal All-Hazards Risk Assessment (AHRA) initiative aims to develop a mechanism for a comparative assessment and rating of risk events derived from all hazards (regardless of the source, whether malicious or non-malicious), in order to support emergency management planning in the federal domain. A standardized methodology is pursued in order to leverage the expertise of individual federal departments, share this expertise and knowledge across a community of practice, and generate a whole-of-government view of risks. Methods that attempt to build shared understanding of risks across organizations may be useful to multi-agency problems beyond the Canadian national context.

INTRODUCTION

Building a holistic, cross-government all-hazards risk assessment which aims to capture threats of all "stripes" and assess the associated public safety and security risk is a challenging task. Some of the challenges include the constantly evolving nature of man-made threats, the shifting patterns in threats derived from natural hazards, and increasingly complex ways even simple threats can lead to societal disruption, because they act on an increasingly interconnected and complex society.

While the approach described herein considers the Canadian risk picture, it has become more and more difficult to dissociate threats at home from the international threat environment. World Economic Forum's recently published Global Risks 2012 [100] is very revealing in terms of how current and emerging risks transcend national boundaries and challenge the traditional emergency-driven risk management. The challenge is to come up with novel approaches that incorporate the global context, and make a conscious effort to link national risk concerns with

[11] Paper presented at: Cornwallis Group Workshop 2012 Analysis of Trafficking and Transnational Threats West Point, New York, 1-5 April 2012

global issues. This is a necessary step towards improving collaborative efforts, to the benefit of more resilient communities within our nations, and aiming to build a resilient global community. The safety and security landscape is changing constantly, in Canada as elsewhere, either slowly eroded by less violent but constantly mounting pressures (the emergence of new diseases and the possibility of new pandemics; the exacerbation of weather events by global warming; unforeseen effects of emerging technologies; the asymmetric distribution of wealth and resources leading to increased demographic pressures; the increased complexity of our infrastructures stressing control mechanisms closer and closer to the breaking point; and, not in the least, the greater and greater expectation of protection by the population from its government), or "shaken" violently by "quake-like" events, such as the terrorist attacks of September 11, 2001. The defence landscape has changed significantly as well, following the end of the Cold War, in response to the shifting geopolitical landscape and the continuous blurring of the boundary between defence and security concerns.

These examples underscore both the need for a robust, all-hazards approach to public safety and security, and the challenges associated with undertaking such an approach.

TOWARDS A CANADIAN HOLISTIC RISK PICTURE

In Canada, all levels of Government – federal, provincial/territorial and municipal – share the responsibility to protect Canadians and Canadian society. Within each jurisdiction, the governments' public safety and security functions are shared among many departments and agencies. Hence, preparedness at the national level depends on synchronized efforts among many partners. For practical reasons, any attempt to formalize an overarching risk model needs to respect existing structures for ownership and responsibility in managing risks. As an example, in Canada, public safety and security functions are shared horizontally, within one jurisdiction, among several departments and agencies, and they cross jurisdictional boundaries based on severity of consequences of the event. This adds to the complexity of planning and managing even single emergencies that escalate across jurisdictions and organizational boundaries. The added challenge of an all-hazards planning comes from the lack of a coherent picture on the relative severity of the risks associated with various threats and hazards.

Organizational background

The Centre for Security Science (CSS) has made it its mission to generate and support scientific activities aimed at improving public security across the whole of government, and making a contribution internationally. CSS is organized as an extensive network of national and international Science and Technology (S&T) partners and public security communities, which includes both "producers" and "users" of S&T products and services, risk analysis being one of them. Within CSS, a Risk Portfolio has been established in response to growing interest in the risk field from across government and defence. The vision is to develop a risk resource centre to support the community with threat, vulnerability and risk assessments, gap analysis, foresight and future security visioning and other related activities and products. The author, a member of the CSS Operations Research (OR) team, has conducted research work on risk assessment methodologies and models, work that constitutes an important contribution to this enhanced risk "toolbox" housed within the CSS Risk Portfolio.

One of the initiatives where the Centre saw an opportunity to contribute was the development of an All Hazards Risk Assessment (AHRA) methodology, in close partnership with Public Safety Canada, the federal department with jurisdiction over coordinating federal public safety and security functions. The purpose of the AHRA is to enable federal institutions to perform risk assessments consistently, and to formalize a structure for combining departmental risk assessments to create a whole-of-government risk picture to support emergency management planning in federal institutions.

Given its mandate and the project's importance, CSS supported the AHRA initiative, as one that has the potential of benefiting the entire safety and security community. Although this initiative is focussed for now on the federal level of government, the Centre's position as a "network hub" provides it with a unique opportunity to bank on the variety of expertise available within the spectrum of partner organizations, and to advocate for models and tools that ensure interoperability with efforts at the local, regional, provincial/territorial, as well as the national and international level. Public Safety Canada is leading the collaborative AHRA project and provides the policy cover, while CSS provides technical support to developing the supporting methodology, which includes support to scenario development, risk analysis and evaluation, as well as effective presentation of the overall results. The author contributed significantly to the development of metrics and methods for risk analysis (likelihood and impact assessment) and risk evaluation, and generated the graphical depiction of the overall results for presentation to decision makers.

The Federal All-Hazards Risk Assessment

The Federal All-Hazards Risk Assessment (AHRA) aims to develop a mechanism for a comparative assessment and rating of risk events derived from all hazards (regardless of the source, whether malicious or non-malicious) that are significant enough to warrant federal interest, in order to support emergency management planning in the federal domain. The all hazards risk picture generated with the AHRA methodology initiative has the potential to inform decision-making at all levels.

Amongst the intended outcomes of the AHRA process, an important one is to generate a shared understanding of risks, their likelihood and potential consequences. Each federal institution has its own strategic and operational objectives, with each being exposed to its own unique set of risks, and each having its own information and resource limitations. The AHRA addresses the interconnected nature of Canada's risk environment by providing a means to produce a collective judgment of risks that may be of concern to more than one federal institutions. A standardized methodology is pursued in order to leverage the expertise of individual departments, share this expertise and knowledge across a community of practice, and generate a whole-of-government view of risks. The relative ordering of risk events based on their ratings and the process for assessing them will be used as a starting point for emergency management planning at the federal level, and to inform future actions and initiatives. This shared assessment of risks necessarily takes a high level view; however departments may continue to conduct more focused assessments of risks which fall within their immediate problem space, according to their mandate and responsibilities or interests, and as legislated in Canada by the Emergency Management Act and other relevant legislation and policies.

MULTI-ORGANIZATIONAL CHALLENGES TO PUBLIC SAFETY AND SECURITY RISK ASSESSMENT AND MANAGEMENT

Risk is an intellectual construct, contingent on the belief that human intervention can influence the outcome of future events, as long as an effort is made to anticipate these events. Oftentimes risk has a negative connotation and is associated with the possibility of future harm or loss [101]. In simple terms, risks are about events that, when triggered, cause problems. Most commonly, risks are discussed in the context of effects of uncertainty on an enterprise's objectives. Because risks refer to potential problems in the future, often there is a great deal of uncertainty with regard to how and to what degree such events may be realized. If the enterprise's interests are potentially affected, processes are set up to manage the uncertainty and strategies are developed to minimize the effect of such future events on desired outcomes. *Risk management* is the structured approach to set up such processes and develop such strategies [102]. Although the details of the risk management approach vary widely across risk domains/organizations, the following steps identified in ISO/FDIS 31000, "Risk Management – Principles and Guidelines" [103] are commonly followed:

1. Risk identification: The process of finding, recognizing, and describing risks.

2. Risk analysis: The process of understanding the nature and level of risk (in terms of its impacts and likelihood).

3. Risk evaluation: The process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

4. Risk treatment planning: The process of identifying and recommending risk control (or risk treatment) options.

The outputs of these four steps should provide decision-makers with an improved understanding of the relevant risks (likelihood, impacts) that could affect the enterprise's objectives, indicators of the effectiveness of risk treatment measures already in place, the potential effectiveness of additional risk treatment measures as well as an appreciation of the inherent uncertainties in all key aspects of the risk assessment process. Generally, risk management is a part of decision making and hence an integral part of organizational planning processes.

One difficulty with existing risk management models is that they are usually designed for single organizations. They can be difficult to extend to a collective of organizations, such as the multitude of public, private and voluntary organizations that have a role in public safety and security. In the context of public safety and security, one must consider carefully what constitutes the "enterprise", and what is the role of risk assessment in informing collective planning processes to manage risks to society that arise from all hazards. Effective risk management of societal risks must, therefore, also address the multi-organizational planning context of public safety and security. The challenge this poses to the overall risk management paradigm is two-fold:

1. The risk domain is distributed amongst multiple organizations; as such, the assessment requires “assembling” expertise and knowledge across the risk practitioner community.
2. Decision making and planning processes that include risk control and risk treatment options, which complete the overall activity of risk management, are also distributed across various organizations, with their own levels of risk managers and decision makers.

Given the complexities surrounding the multi-organizational structure of the public safety and security domain, it is important to delimitate the scope and role of the AHRA process within overall activities of risk management.

The AHRA process and methodology are focused primarily on the assessment component of the overall risk management paradigm. The hazard risk domain is covered by the AHRA methodology. However, the strategic risk domain (e.g., political risks, reputational risks) and the operational risk domain (e.g., day-to-day issues confronting the institution) are not, although these aspects may be considered and factored in assigning impact ratings. Figure 1 highlights the role of the AHRA process within the overall process of emergency management, which happens government-wide and involves intra- and inter-departmental activities.

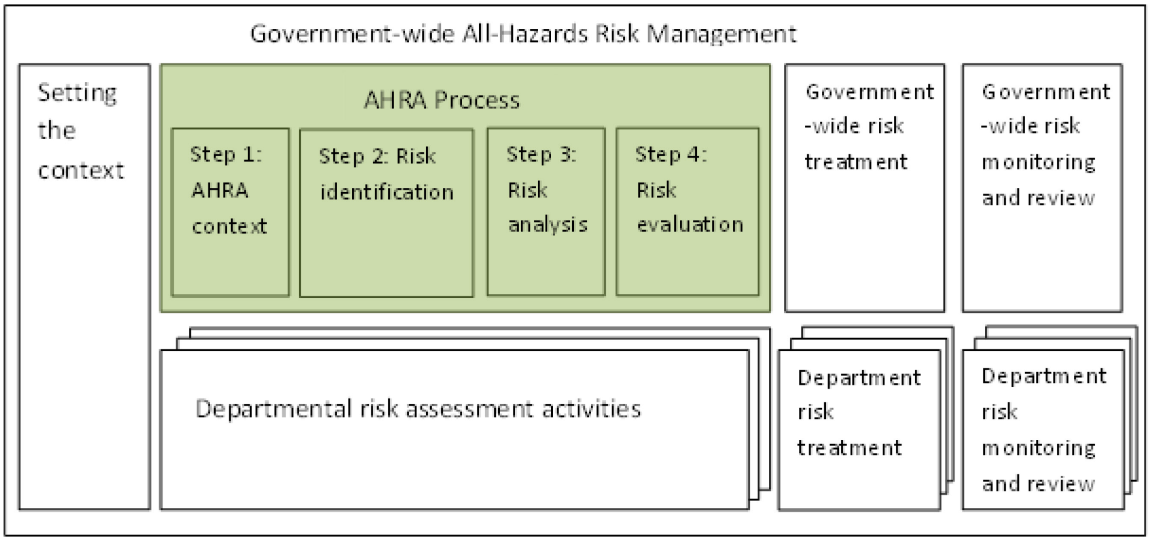

Government-wide All-Hazards Risk Management
Setting the context
AHRA Process
Step 1: AHRA context
Step 2: Risk identification
Step 3: Risk analysis
Step 4: Risk evaluation
Government-wide risk treatment
Government-wide risk monitoring and review
Departmental risk assessment activities
Department risk treatment
Department risk monitoring and review

Figure 9: Government-Wide All-Hazards Risk Management

SCOPING AND STRUCTURING THE ALL-HAZARDS RISK DOMAIN

Risks are events or circumstances that, if they materialize, could negatively affect the achievement of objectives. In the context of the AHRA, the objective is tonsure that Canadians are protected from the gamut of threats and hazards that can become a risk to their safety and security; to that end, the goal of AHRA is to produce a whole of government all-hazards risk picture that can potentially inform strategies to minimize the effects on society.

In order to make the entire process more manageable, a risk taxonomy was developed [104], which breaks down all-hazards risk by types of threats and hazards of significant potential impact within the field of view of the Federal Government. The most current version of the AHRA taxonomy is shown in Figure 7 below.

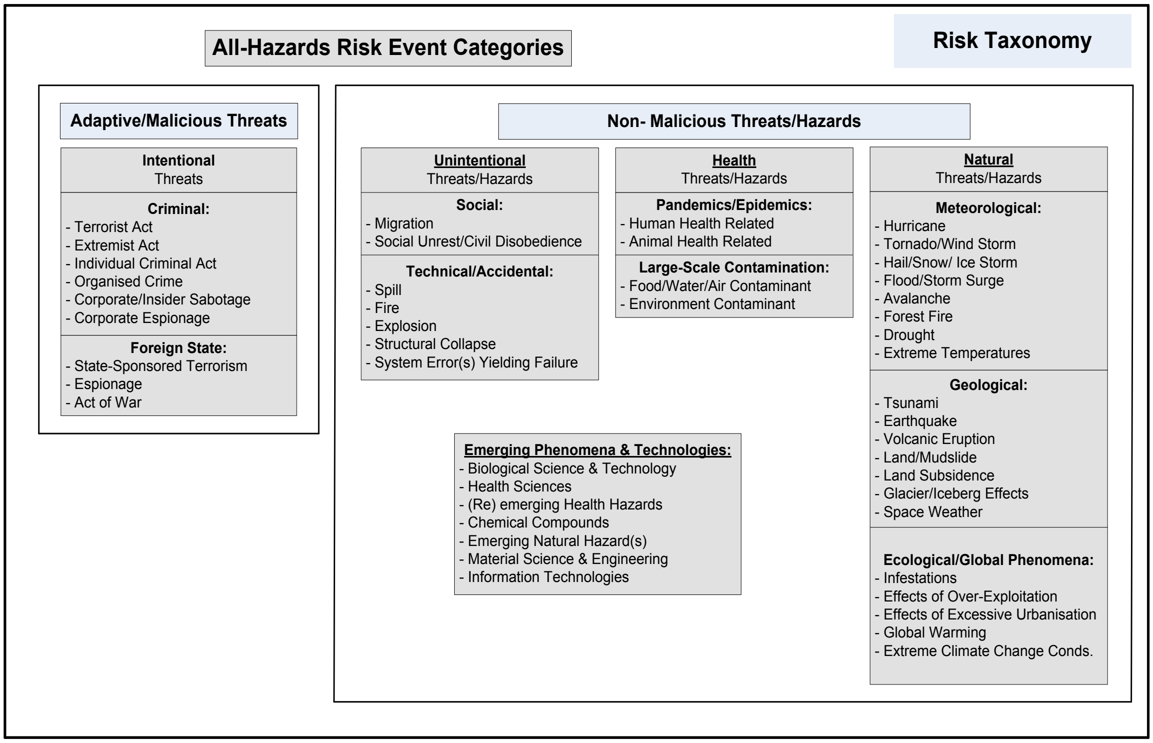

All-Hazards Risk Event Categories
Risk Taxonomy
Adaptive/Malicious Threats
Intentional Threats
Criminal:
- Terrorist Act
- Extremist Act
- Individual Criminal Act
- Organised Crime
- Corporate/Insider Sabotage
- Corporate Espionage
Foreign State:
- State-Sponsored Terrorism
- Espionage
- Act of War
Non- Malicious Threats/Hazards
Unintentional Threats/Hazards
Social:
- Migration
- Social Unrest/Civil Disobedience
Technical/Accidental:
- Spill
- Fire
- Explosion
- Structural Collapse
- System Error(s) Yielding Failure
Health Threats/Hazards
Pandemics/Epidemics:
- Human Health Related
- Animal Health Related
Large-Scale Contamination:
- Food/Water/Air Contaminant
- Environment Contaminant
Natural Threats/Hazards
Meteorological:
- Hurricane
- Tornado/Wind Storm
- Hail/Snow/ Ice Storm
- Flood/Storm Surge
- Avalanche
- Forest Fire
- Drought
- Extreme Temperatures
Geological:
- Tsunami
- Earthquake
- Volcanic Eruption
- Land/Mudslide
- Land Subsidence
- Glacier/Iceberg Effects
- Space Weather
Ecological/Global Phenomena:
- Infestations
- Effects of Over-Exploitation
- Effects of Excessive Urbanisation
- Global Warming
- Extreme Climate Change Conds.
Emerging Phenomena & Technologies:
- Biological Science & Technology
- Health Sciences
- (Re) emerging Health Hazards
- Chemical Compounds
- Emerging Natural Hazard(s)
- Material Science & Engineering
- Information Technologies

Figure 10 All-Hazards Risk Taxonomy

An effective taxonomy has three key attributes: it provides a classification scheme; it is semantic; and it can be used as a map to navigate the domain [105]. The proposed scheme has been designed with those key attributes in mind. The All Hazards Risk Taxonomy defines the risk domain in which there are two major classes; the Malicious/Adaptive and the Non-Malicious/Non-Adaptive. Malicious threats are intentional and originate from threat actors like terrorists, organized crime actors, or foreign states. Non-malicious threats include unintentional man-made, health, and natural disasters, and cross-cutting risks such as those related to emerging technologies or climate change. To aid the tackling of so vast a domain, the AHRA taxonomy partitions threats/hazards into logical categories, and provides a "blueprint" for further analytical and methodological development. The AHRA taxonomy was developed together with a risk lexicon [106], which can help the collaborative effort by establishing a common terminology and ensure mutual understanding. Both initiatives benefited from input from the project partners, representing many federal organizations with national security, public safety and emergency management objectives. The AHRA taxonomy helps structure the vast problem space, while capturing its breath and complexity.

THE AHRA CONTEXT AND RISK IDENTIFICATION

Invariably, risk assessment starts with risk identification. An important prerequisite to risk identification is establishing the context. This implies selecting the domain of interest, establishing the identity and objectives of stakeholders, the scope of the process, and the basis upon which risks will be evaluated (i.e., assumptions, constraints).

The scope of the approach described in this paper is "all-hazards", which means that all types of hazards, as captured in the AHRA taxonomy, are considered as sources of risks, although not all may be retained for further assessment and evaluation. For the federal AHRA project, the focus is on emergencies that are likely to require federal involvement.

Also, in order to employ a common time frame for analysis, the AHRA considers events that are possible within the next five years. This does not exclude rare events, which might have low (but not zero) probability of happening in the next five years. An example would be the disruption of satellite communications by solar storms; although rare, this could occur at any time within the next five years. However, within the current scope of the approach, potential events that are not considered in the AHRA are those that cannot realistically be expected to occur within the next five years. This may be because the conditions that can generate the risk may require more time to emerge as threats (examples include: new technologies, whose effects on human health and environment have not been tested; an asteroid impact, assuming that it is known that there are no asteroids in sufficient proximity in this time frame; etc.).

The federal AHRA project has annual cycles. Each year, federal organizations are asked to bring forward their top threats and hazards. An Interdepartmental Risk Assessment Working Group is mandated to select those threats and hazards that will be retained for further assessment. For example, the federal AHRA project has gone through two cycles (the second cycle is under way): during the first, pilot cycle (2010-2011), 16 threats and hazards were retained, while for the current cycle (2011-2012), 12 threats and hazards were retained, as shown in Table 1 below.

The AHRA is a scenario-based approach. The advantage of such an approach is that scenarios can provide context and specificity to identified sources of risk. The challenge is ensuring that the risk space is appropriately characterized. In developing the set of scenarios one should aim for an "importance sampling" of the risk domain. On the one hand, this means developing a set of scenarios large enough to ensure that drivers for capabilities are adequately captured. On the other hand, the set of scenarios should be reduced to a number that is realistic, in terms of required stakeholder and expert engagement, and in terms of what can be achieved during the assessment process. In other words, one should strive to cover the entire all-hazards risk space, albeit sparsely, to enable a parametric analysis of the whole domain [107], rather than concentrate a disproportionately large number of scenarios on a few narrow risk intervals.

Given the goal of the AHRA project of emphasizing the interconnected nature of Canada's risk environment, each of the proposed scenarios must present a level of complexity that places it beyond the sole responsibility of one federal organization. Each scenario is a collaborative effort, with multiple institutions involved in its development. The desired output of the scenario development exercise is a realistic set of incident scenarios that reflect serious, plausible threats and hazards that federal organizations with an emergency management mandate must be prepared to address. However, because of the challenges associated with setting up a complex process such as the AHRA, as well as those associated with ensuring the availability of the interdisciplinary expertise required during the assessment process, the number of scenarios developed and assessed was kept at 10 per year, at least for the first two AHRA cycles, as illustrated in Table 2.Generally, new scenarios are sought each year, to build a comprehensive set of scenarios over time.

Table 10: Threats and hazards identified during the first two federal AHRA cycles

List of Threats &Hazards (Unrated)	
2010-2011:	**2011-2012:**
• Terrorism • Foreign interference/espionage (cyber) • Breach of information • Explosions • Oil incident • Accidental and/or intentional chemical event • Aircraft disasters • Marine disasters • Rail disasters • Pandemic (e.g. pandemic influenza) • Emerging respiratory infectious disease outbreak • Foodborne infectious disease outbreak • Zoonotic infectious disease outbreak • Non-zoonotic animal disease • Floods • Hurricanes	• Cyber attack • Terrorism • Influx of Illegal Migrants • Radiological or Nuclear Accident • Marine pollutants/Accidental Chemical Event • Earthquakes • Floods • Hurricanes • Pandemic • Foodborne Outbreak • Extreme Weather • Extreme Space Weather

For some hazards, a single narrative scenario may be found insufficient to characterize the continuum of associated risk. A more complete assessment would consider the continuum in the magnitude and likelihood of triggering events and variation in the consequences associated with different contexts (locations, weather conditions, economic cycles, day versus night events, etc.). At the same time, the efforts required of a full risk assessment are not practical for the purposes of the AHRA process, particularly in the first few cycles. The possibility of developing composite scenarios with variants has been considered, in order to find the right balance between the reduced number of scenarios that are considered practical in terms of being able to address in a collaborative project, and the more complete view of risk that may ultimately be required to properly inform priority-setting and emergency planning. A composite scenario is in fact a set of related scenarios of varying magnitudes, representing potential realizations on the continuum of risk generated by the same particular hazard, and chosen in such a way to best characterize that continuum for emergency planning purposes.

Table 11: Scenarios developed during the first two federal AHRA cycles

List of event scenarios	
2010-2011:	**2011-2012:**
Health: • Emerging zoonotic respiratory pathogen outbreak • Listeriosis outbreak • Foot-and-mouth disease outbreak **Natural:** • Hurricanes • Flood **Unintentional:** • Marine oil spill **Malicious:** • Aircraft disaster (cargo) • Aircraft disaster (passenger) • Chemical release incident • Cyber incident	**Health:** • Pandemic human disease • Foodborne outbreak **Natural:** • Earthquake • Hurricane • Ice storm **Unintentional:** • Nuclear accident/ technical failure • Marine pollutants – accidental chemical event **Unintentional Social/ Intentional Criminal** • Influx of Illegal migrants **Malicious:** • Cyber attack • Terrorism event

RISK ANALYSIS

Once a risk has been identified, it must be analyzed, which means understanding the nature and level of risk, usually in terms of likelihood and impacts or consequences. “Likelihood” refers to the risk event’s chance of occurrence, and “consequences” measure the severity and extent of the risk event’s effects. A challenge facing an “all-hazards” methodology is defining and finding good measures for “Likelihood” and “Consequences” consistently across risks of very different nature.

The AHRA methodology proposes to investigate the consequences of a risk event, as described by a scenario, along a number of dimensions, chosen to capture the spectrum of risk interests of the federal government. There are six impact categories, each designed to cover a significant segment to federal emergency management institutions. Public Safety Canada consolidated a list of impact dimensions, together with relevant criteria to be considered within each impact category, by consultation with the federal emergency community. The author’s role was to develop metrics for risk analysis (likelihood and impact assessment), and to ensure that the approach was as robust and consistent as possible.

Overall, the scoring approach is an “order of magnitude” approach. The scoring method uses a logarithmic (half-log-10) scoring scale, and attempts to apply it consistently across the impact categories, at least to a practical extent. A logarithmic scale is appropriate to allow for the extent of variability and uncertainty associated with a large problem space. It is also appropriate for the purposes of maintaining an underlying mathematical linkage between the simplified scoring approach used for the collaborative work and a full quantitative risk, which might exist and be used by expert analysts in more focused risk areas across the many departments. In other words, the approach is fundamentally (mathematically) compatible with more formal quantitative risk assessment approaches, but does not presume that they exist. Maintaining a mathematically rigorous underlying structure for the simplified scoring approach allows for the current “working” version to be enhanced over subsequent phases, in order to increase the level of compatibility with more formal methods, without need to lose compatibility with previous generations of work.

RISK ANALYSIS – IMPACTS

The six impact categories in the AHRA are: People, Economy, Environment, Territorial Security, Canada’s Reputation and Influence, and Societal and Psycho-Social effects. In theory, the six categories were chosen to cover “orthogonal” dimensions in the consequence space; in practice, there were many cases were the effects cannot be clearly split in independent components, which created a challenge in terms of avoiding double-counting of effects. For example, the “environment” impact category is intended to capture unique effects on natural environmental assets; in practice, environmental effects are often tangled up with costs associated with the loss or degradation of those environmental assets, which can be counted as an economic impact. In such cases, the “orthogonality” requirement was enforced during the assessment process, by asking participants to decide which category provides the best fit, and only include those effects once.

People

The first impact category is the “People” category, which captures the impact following a given risk event in terms of fatality, injury, and disease. To account for non-fatal health effects, alongside fatal ones, a composite measure of human health impact was employed, by estimating the proportion of indirect deaths caused by the scenario, which may be thought of as fatality-equivalents. They can be the result of physical injuries, chronic illness, mental illness and being displaced (or lacking basic necessities of life).Fatality-equivalents may also be inferred by defining the relative severity of the injury, illness or displacement and duration of these effects, using metrics such as the Disability-Adjusted Life Years (DALY) lost, which provide quantitative means for taking into account the burden imposed by premature mortality and morbidity on populations [108]. The severity scale ranges between 0 (perfect health) and 1 (death). The duration of the injury is represented in years. For the AHRA project, relative severity is defined as mild, moderate and severe, while the duration includes the options of short term, long term and permanent. A short term injury/illness is defined as being less than four weeks, while a long term injury greater than four weeks. Permanent injuries/illnesses are present for the remainder of the person's life which is assumed to be 40 years for the average adult.

The DALY measure is also used to measure the impact of fatalities. The severity of a fatality is always equal to 1, while an estimate of the number of years of life expectancy at the time of death is the appropriate measure of duration. An adult fatality, on average, can be assigned a score of approximately 40 (for 40 years of lost life). This provides a way to calculate the number of fatality equivalents from DALYs.

Once the total number of fatality equivalents has been tallied up for a given risk event, the following table shows the conversion into an impact rating on a scale from 0 to 5.

Table 12: Rating table for the "People" impact category

Impact Score	**Fatality-Equivalents**
No Impact	No Impact
0	1
0.5	3
1	10
1.5	30
2	100
2.5	300
3	1,000
3.5	3,000
4	10,000
4.5	30,000
5	100,000

Economy

The second impact category is the "Economy" category. This category captures the dollar value following damage(s) or loss to economically productive assets and disruptions to the normal functioning of the Canadian economic system, following a risk event. This economic loss is broken down into:

- Direct loss, which accounts for the immediate economic damage generated by the disaster, measured in repair or replacement costs for physical assets (buildings, infrastructures, equipment etc.)

- Indirect loss (flow losses), measured in costs associated with the disruption of flows of goods and services, due to damages or disruption to productive assets and economic infrastructure, relative to the duration of the disruption.

When identifying contributions to the economic loss, the assessment should ensure that no double-counting takes place, and certain built-in mechanisms and behavioural changes (e.g. consumer-demand shift, substitution of inputs and/or reallocation of resources, etc.) should be considered, which can mitigate to a certain extent the losses. Taking all identified "positive-" and "negative-costs" into account, all costs are added, and the rating for this category is based on the final dollar figure, as illustrated in Table 4 below.

Table 13: Rating table for the "Economy" impact category

Impact Score	**Total Economic Loss**
No Impact	No impact
0	$10M
0.5	$30M
1	$100M
1.5	$300M
2	$1B
2.5	$3B
3	$10B
3.5	$30B
4	$100B
4.5	$300B
5	$1,000B

Macroeconomic studies provide a complementary way to assess the repercussions of direct and indirect economic losses. For instance, estimates of macroeconomic effects would take into account that some indirect effects could be exacerbated or mitigated in the aggregate by changes in prices or flexibility in the production process (e.g. through reallocations in spending/production across sectors or through the mobilization of production factors if production is not at full capacity). Estimates of high-order impacts require the use of more sophisticated economic models.

It must be noted that for the "people" as well as the "economy" category, in order to minimize round-off errors, the actual numbers in units chosen for the category (fatality equivalents, and dollars, respectively) are elicited during the assessment process; the ratings derived from those numbers are only used during the later stages in the process, when all the assessments are "assembled" into an overall measure of risk for each risk event considered, as described by the corresponding scenario.

The remaining impact categories, however, are less quantifiable; the next few paragraphs describe briefly the qualitative approaches to assessing the "Environment" category, "Territorial security", "Society and psycho-social" effects, and "Canada's reputation and influence". For each of these categories, a 0 to 5 rating scale was developed based on sets of qualitative criteria to be considered within each category, as identified by the federal community (although the same order of magnitude approach was followed in the more quantifiable aspects of impact for some categories). A more detailed description of the rating methods for these categories can be found in [109].

Environment

The "Environment" category rating scale focuses on environmental damage caused by a risk event. In the context of the AHRA, environmental damage refers to non-economic aspects associated with the loss of environmental assets or environmental quality. This category will exclude assessing economic aspects created by such loss, as they are better captured under the "Economy", in order to avoid double counting. The Environment impact category relates to the preservation of specific components of the environment pertaining to air, water and soil ecosystems, including fauna and flora. The rating of this category considers four elements that characterize the size and severity of environmental damage from a risk event or an emergency: the magnitude of an environmental response required (local, regional, multi-jurisdictional, general, specialized, etc.); the geographical extent of the damage; the magnitude of damage based on adverse effects to different components of the environment; and the duration of the damage including the level of recovery efforts.

Territorial Security

The "Territorial security" category is intended to capture the impact of a risk event on the Government's ability to maintain safety and security functions within all of its territory. This dimension captures conditions in which there is a loss or disruption in the Government's ability to secure its territory or its borders, and to secure the safety of citizens. Challenges can come from abroad (e.g. terrorist attacks, challenges to Arctic sovereignty) or from natural disasters (e.g. hurricanes, earthquakes, infectious diseases).

For this category, the rating is determined by the area affected, with factors including the duration of disruption and population density.

Canada's Reputation and Influence

"Canada's reputation and influence" category captures shifts in views towards Canada by foreign governments, international actors and populations following a risk event in Canada or involving Canadians abroad. The rating is based on qualitative descriptions of a non-exhaustive list of situations that can demonstrate effects on Canada's international position. Examples include: damage or loss of control over Canada's embassies, suspension of international agreements, protests against Canada, imposition of travel restrictions to Canada, deterioration of bilateral political relations, etc.

Society and Psycho-Social

The “Society and psycho-social” category measures the extent of disruption to normal societal function following a risk event leading to sustained adverse behaviour change in the population. Societal and psycho-social effects might be rooted in people’s understanding and perception of the incident as well as their sense of control over the outcome, which may lead to changes in their individual pattern of behaviour over the short or long term, and may even lead to social actions, such as protests, civil disturbances or vandalism.

The rating of this category is based on a qualitative assessment that focuses on two criteria: public outrage and public anxiety. The descriptors for each of these criteria consider the number of people affected, the nature and severity of disruption, and the possibility of short to long-term psycho-social effects in the population.

RISK ANALYSIS – LIKELIHOOD

Whether it refers to a natural hazard or a malicious threat, likelihood assessment attempts to estimate the chance of an event occurring. The assessment method, however, is by necessity very different between the two major classes in the AHRA taxonomy:

- For non-malicious threats/hazards: Quantitative approach by which experts draw on historical data to determine the probability of a risk event as described in the scenario.
- For malicious threats: Through elicitation, experts provide qualitative judgment by considering overall capability (technical feasibility and enabling capabilities) and intent of the malicious actor(s) carrying out the threat.

Likelihood – non-malicious events

To provide estimates for the likelihood of non-malicious risk events, experts draw on historical data of comparable Canadian and international cases, as well as modeling and analysis. The likelihood estimate associated with the risk event as described by the scenario can be expressed by using the table below:

Table 14: Rating table for likelihood of non-malicious scenarios

Likelihood Score	Estimated frequency, once every X years, where X is:
0	100,000
0.5	30,000
1	10,000
1.5	3,000
2	1,000
2.5	300
3	100
3.5	30

4	10
4.5	3
5	1

As for the “people” as well as the “economy” category, in order to minimize round-off errors, the actual numerical estimates, expressed either as in the table above (i.e., one event every X number of years) or, alternatively, as annual probabilities or as the probability of the event happening in the next five years, are elicited during the assessment process; the ratings derived from those numbers are only used at the end, when estimating the overall risk for each risk event considered, as described by the scenario.

Likelihood –malicious events

For malicious scenarios, although records of past attacks are very useful, they cannot be the sole basis for estimating the likelihood of a possible future attack. What makes this category unique is the fact that malicious actors learn, both from past experiences and from advances in technology, as do security organizations trying to prevent them from carrying out attacks, and both sides continuously adapt and adjust their strategies and methods.

Estimating the likelihood of malicious scenarios is considerably different than for non-malicious ones, as these estimates must take into account the determined and adaptive nature of an intelligent adversary. Such an adversary will make a choice to carry out an attack based, on the one hand, on the statement they want to make, in accordance with the individual’s or the organization’s ideology. To capture this dimension, the current approach relies on the intelligence community to provide expert judgment on an individual’s or organization’s intent to carry out an attack, such as the one described in the scenario. On the other hand, the adversary’s choice of an attack is also based on considerations of whether mounting an attack is technically feasible, as well as whether the adversary has adequate organizational and support means to carry it out. Again, the current approach relies on judgment from domain experts to assess various components of the technical feasibility of a malicious attack scenario, and on the intelligence community to provide expert judgment on whether an individual or organization has sufficient capability to carry it out. The combined assessments of feasibility, capability, and intent are used to generate an overall assessment or composite judgment of likelihood. Figure 3 shows the components and steps involved in producing an estimate for the likelihood of a malicious scenario.

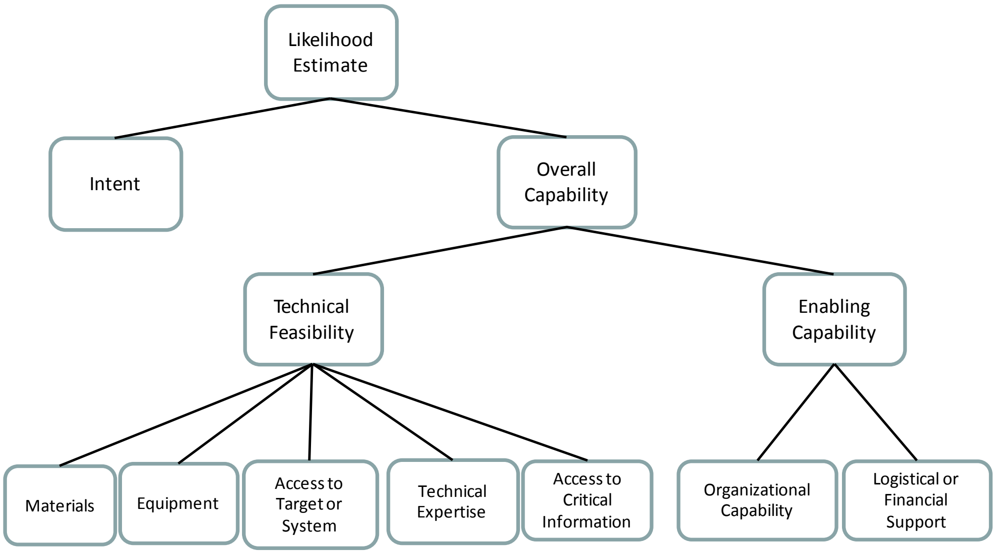


Figure 11: Malicious Likelihood – Components

The overall likelihood score is based on the principle of the "weakest link", meaning that the final rating is determined by selecting the lowest component rating, across all components. A successful adversarial attack cannot occur if one of the elements is absent, lacking or unobtainable; in other words, an attack is assessed as unlikely if the level for one element of the overall capability of the malicious actor(s) is below a necessary level to being materialized, or if there is a lack of intent to carry it out.

The final estimate is expressed on a rating scale of 0 to 5, similar to the rating scale of non-malicious scenarios. However, the two estimates are very different in nature, and there are no grounds for the assumption that an identical rating indicates an equally likely malicious scenario compared to a non-malicious one. A more detailed description of the rating method for likelihood of malicious scenarios can be found in [109].

RISK EVALUATION – COMPARING RISK SCENARIOS

The goal of the risk evaluation stage in the AHRA process is to bring diverse risks into the same high-level view. It generally comprises the following steps:

a. Determination of the risk magnitude (i.e. likelihood and consequences) for the risk.
b. Aggregation and consolidation of risk assessment results into a whole-of-government AHRA.
c. Production of selected AHRA communication products and graphical representations of results.

The determination of the overall magnitude of the risk associated with each scenario includes "aggregating" the impact assessments into a single measure of consequences, which, combined with the likelihood assessment, provided an estimate of risk for each scenario. Presented collectively, once the set of selected scenarios has reached "critical mass", in terms of proper representation of the risk space, these risk estimates will generate a picture of "all hazards" risk to the federal government, and can be used to inform federal emergency management planning.

As discussed in previous sections, for those impact categories more amenable to a quantitative assessment, an "order of magnitude" rating approach was employed, using a logarithmic scale with half scores; for example, for the "People" category, for 1 fatality, the risk score is $s_{I_P} = 0$, since 1=10^0, while 300 fatalities will produce a rating of $s_{I_P} = 2.5$, since 300=$10^{2.5}$.

Rolling up the impact categories into a single composite score requires strong societal value judgements. Establishing equivalency of ratings in different categories is necessarily subjective. For example, the rating scale for the "Economy" assumes a monetary equivalent of 10 million dollars for one fatality, or, in other words, a risk event causing an economic loss of about 10 million dollars is about the same magnitude as a risk event causing a fatality. Although the use of such conversion factors is a sensitive and controversial issue, they are commonly used by government agencies to optimize government decisions and make cost-effective changes to policies. In most cases, the monetary value is based on what the society is willing to pay in order to save a human life; a common measure used to determine such value is the Value of Statistical Life (VSL). The research literature on the topic of monetary valuation of human life is vast, with a great variability in the values obtained from different studies, particularly in the United States [110], [111]; the variability in methods and values may be the reason why federal agencies use different monetary valuations [112].

According to one study published in 2009 [111], which looked at 40 studies from 9 countries, the average value of VSLs stands $9.5 M and the median at $6.6 M, expressed in units of $US 2000; among the 40 studies, there were seven done in Canada, with an average VSL value of $9.2 M and a median of $4.0 M. In the US, one of the prolific academic contributors to the field (K. Viscusi, [113]) suggests that the value of $8.7 M (in $US 2011) is appropriate, while in 2004, the US Office of Management and Budget instructed federal agencies to use values between US$1 million and US$10 million per life lost [112].

Considering such evidence from academic research and government practice alike, and considering currency exchange rates over recent years, an equivalency factor of C$10 million per life lost was adopted for the AHRA.

Unfortunately, not much evidence was found in order to support equivalency of ratings with the remaining categories. During the rating workshops, the participants were prompted to examine whether a similar rating in a different category would indicate an event of similar magnitude. However, as it matures, AHRA would benefit from including dedicated "calibration workshops", where expert judgement is sought in order to establish such conversion factors and calibrate ratings across all impact categories.

Assuming equivalency of ratings has been established (i.e., impact categories have been calibrated), one can calculate a "Consequence Score"S_C:

$$S_C = \log\left(\frac{1}{6}\sum_{i=1}^{6} 10^{s_{I_i}}\right) \tag{1}$$

Non-malicious likelihood tables are formulated as “one event every 10^{5-S_L} years”, where S_L is the associated likelihood score. The rating scheme was designed to produce the highest rating, 5, for the highest frequency considered, which is once a year or more frequent: e.g., $1/10^{(5\text{-}5)}$

As noted in a previous section, malicious likelihood scores, based on qualitative judgments, are also expressed on a 0 – 5 scale; however, the two scales are not necessarily equivalent. A separate “calibration” exercise was conducted to place the malicious scenarios on the same likelihood scale as the non-malicious ones; however, the results for the malicious scenarios are classified, and they are not included in the current paper.

The joint presentation of both the likelihood and consequence dimensions on a scatter plot provides a graphical means for presenting a high level view of diverse risks. This graphical depiction can be used to compare similar events (e.g., possible variants of a hurricane scenario), or very diverse events (e.g., pandemic influenza versus marine oil spill). Figure 4 presents such a scatter plot, where the iso risk contours are given by:

$$S_R = S_C + S_L \tag{2}$$

It must be noted that the uncertainty “bubbles” around the risk estimate for each scenario come from elicitation of uncertainty around each of the estimates provided by experts during the elicitation process (i.e., uncertainty around the likelihood estimate, as well as around estimates for each of the impact categories). To come up with an uncertainty interval around the “aggregated” consequence measure, the author simply looked at the impact estimate driving the consequence measure (due to the “order of magnitude” approach) and used its associated uncertainty; although more sophisticated calculations can be used, it was deemed sufficient for providing a rough measure of uncertainty around the estimates. The “bubbles” are simply PowerPoint ellipses with the uncertainty intervals for likelihood and consequences, respectively, as minor and major axes. Having an illustration of uncertainty included on the graph, together with the point estimates for overall risk, was considered more important than improving the accuracy of the calculation for marginal improvements in uncertainty results. In the author’s opinion, the important point was that the uncertainty be presented as part of the overall risk picture, rather than strive for a level of accuracy in uncertainty calculations which would not be supported by the low accuracy in elicited uncertainty estimates. For validation of results, the author collaborated with experts in the AHRA Interdepartmental Working Group on Risk Evaluation and Visualization.

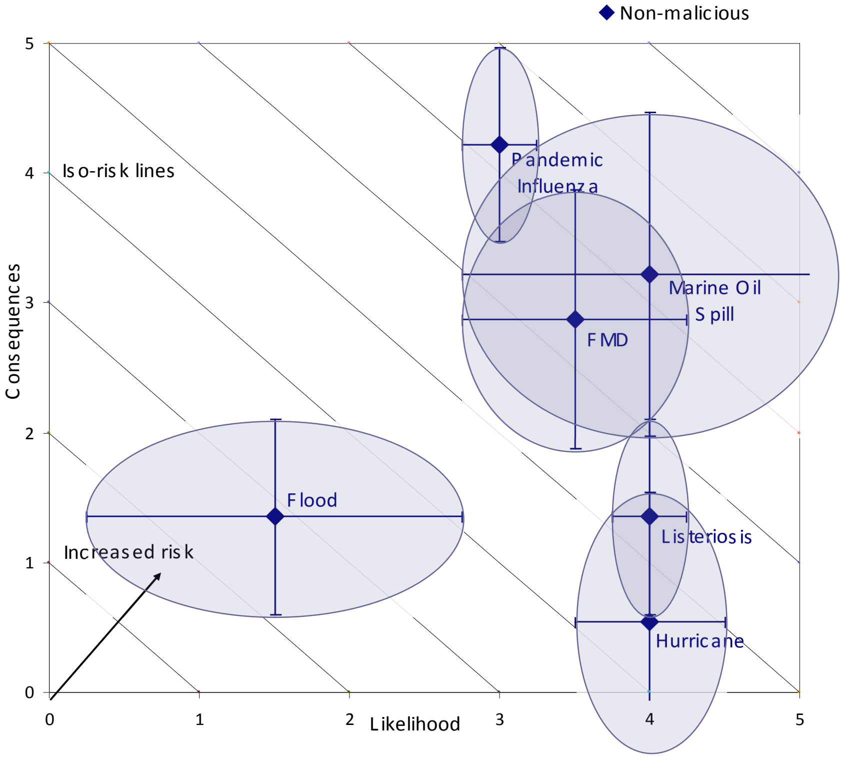


Figure 12 High level view of AHRA results for non-malicious scenarios

Summary

In summary, this paper started out by highlighting the complex and interconnected safety and security risk landscape, both from a global as well as Canadian prospective. Then, the paper argued for an increased need for collective planning processes to manage risks to society derived from "all-hazards", and discussed some of the challenges associated with such an endeavour. The biggest part of the paper was devoted to describing the Canadian Federal All-Hazards Risk Assessment, a collaborative effort within the Canadian Federal community aiming at developing a mechanism for a comparative assessment of risk events and to generate a picture of "all hazards" risk to the federal government, and to inform federal emergency management planning. The AHRA approach is scenario-based, where scenarios are used to provide context and specificity to identified sources of risk. A risk taxonomy is used to structure the complex and vast problem space, and to guide the scenario selection and development towards an appropriate sampling of the risk domain. Each scenario is assessed in terms of likelihood and consequences. Likelihood refers to the risk event's chance of occurrence; different methodologies are used for its estimation, depending on whether the scenario involves a malicious or a non-malicious threat/hazard. Consequences of a risk event, as described by a scenario, are investigated along a number of dimensions. The scoring approach is an "order of magnitude" approach, and attempts to apply consistently across the impact categories. For those impact categories more amenable to a quantitative assessment, the scoring method uses a logarithmic scoring scale. Some of the impact categories, however, are less quantifiable; and for those categories, the rating was based on sets of qualitative criteria identified by the federal community.

The impact assessments, “aggregated” into a single measure of consequences and combined with the likelihood assessment, determine the magnitude of the overall risk associated with each scenario. Presented collectively, once the set of selected scenarios has reached “critical mass” in terms of proper representation of the risk space, these risk estimates generate a picture of “all hazards” risk to the federal government, and can be used to inform federal emergency management planning. Most importantly, the approach described in this paper attempts to build shared understanding of risks across organizations, and may be useful to multi-agency problems beyond the Canadian national context.

References

[100] Global Risks 2012, World Economic Forum, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf.

[101] Rowe, W.D. (1977), An anatomy of Risk, Systems Engineering and Analysis Series (Chestnut, H., Ed.), John Wiley & Sons, 1977.

[102] Haimes, Y.Y., Risk Modeling, Assessment and Management, 2nd ed., Systems Engineering and Management Series (Sage, A.P., Ed.), John Wiley & Sons, Hoboken, New Jersey, 2004.

[103] International Organization for Standardization, "Risk management – Principles and guidelines on implementation", Draft International Standard ISO/DIS 31000, 2008.

[104] Verga, S.**,** "All-hazards risk framework – an architecture model", in S. Martorell, C. G. Soares and J. Barnet(Eds.), Safety, Reliability and Risk Analysis: Theory, Methods and Applications, vol. 1 (Proceedings of the European Safety and Reliability Conference, ESREL 2008, and 17th Society for Risk Analysis-Europe, Valencia, Spain), pp. 315-323, CRC Press/Balkema, Taylor and Francis Group, London, UK, 2008.

[105] Lambe, P., Organising Knowledge: Taxonomies, Knowledge and Organisational Effectiveness, Oxford: Chandos Publishing, 2007.

[106] Verga, S., "Intelligence Experts Group All-Hazards Risk Assessment Lexicon", DRDC CSS Note, DRDC-Centre for Security Science-N-2007-001, 2007.

[107] Davis, P.K., Analytic Architecture for Capabilities-Based Planning, Mission-System Analysis, and Transformation, RAND Monograph Report MR-1513-OSD, 2002.

[108] Mathers, C.D., Vos, T, Lopez, A.D., Salomon, J, and Ezzati, M (ed.), National Burden of Disease Studies: A Practical Guide, Edition 2.0, Global Program on Evidence for Health Policy, Geneva: World Health Organization, 2001.

[109] The All Hazards Risk Assessment Methodology Guidelines, 2011-2012, Public Safety Canada, Emergency Management Planning Unit, AHRA-ETR@ps-sp.gc.ca.

[110] Viscusi, W. Kip and Aldy, Joseph E., "The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World", *Journal of Risk and Uncertainty*, vol. 27, 2003, p. 5-76.

[111] Bellavance, F., Dionne, G.and Lebeau, M.,"The value of a statistical life: A meta-analysis with a mixed effects regressions model",*Journal of Health Economics*, 28: 444-464, 2009.

[112] Appelbaum, Binyamin, "As U.S. Agencies Put More Value on a Life, Businesses Fret", The New York Times, New York, NY, USA, 16 February 2011.

[113] Viscusi, W. Kip, “The Value of a statistical life,” Discussion Paper, n° 517, Harvard Law School, Cambridge, 2005.

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.)

The Federal All Hazards Risk Assessment Framework Body of Knowledge: Volume II : Supporting Material

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

Bayne, I.; Duncan, J.; Friesen, S.; Goudreau A.; Mills, B.

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

September 2013

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

90

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

14

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.)

Technical Note

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 CSS TN 2013-015

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.)

Public Safety (PS) Canada and Defence Research & Development Canada's (DRDC) Centre for Security Science (CSS) are in the process of investigating improvements to the federal All Hazards Risk Assessment (AHRA) methodology that would enable the federal government to develop a national picture of high priority risks and capabilities that mitigate those risks.

This report contains the statistical data and reference materials used to develop the Technical Report, The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume 1: Establishing an Information Baseline and Way Forward, DRDC CSS TR 2013-014.

The Technical Report (TR) is intended for participants in the federal AHRA initiative and for a wider audience involved in safety, security, societal resilience and emergency risk management. The report highlights lessons from the federal AHRA approach that would support multi-mandate and multi-jurisdictional risk assessments, and enable the development of a national risk assessment (NRA).

This Technical Note is reviewed and, if required, updated annually.

Sécurité publique Canada (SP) et le Centre des sciences de la sécurité de Recherche et développement pour la défense Canada (RDDC CSS) examinent actuellement les améliorations pouvant être apportées à la méthodologie d'évaluation tous risques (ETR) du gouvernement du Canada afin que ce dernier brosse un portait des principaux risques et des capacités atténuant ceux-ci à l'échelle nationale.

Ce rapport contient des données statistiques et des matériaux de référence utilisés pour élaborer le rapport technique, The Federal All Hazards Risk Assessment Framework Body of Knowledge Volume 1: Establishing an Information Baseline and Way Forward, DRDC CSS TR 2013-014.

Ce rapport technique (RT) est destiné aux gens participant à l'initiative fédérale d'ETR, de même qu'à un plus large public associé à la sûreté, la sécurité, la résilience sociétale et la gestion des risques en situation d'urgence. Le rapport souligne les leçons tirées de l'approche fédérale d'ETR pouvant soutenir des évaluations de risque touchant plusieurs mandats et compétences, et permettant l'élaboration d'une ENR.

Ce document est passé en revue et, si nécessaire, mis à jour annuellement

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.)

All Hazards; Risk Assessment; Risk Management; Planning; Emergency Management