

# Emergent Best Practices in National Risk Assessment Practices and Process

Douglas Hales  
D Hales Consulting Inc.

Prepared By:  
D Hales Consulting Inc.  
5561 Pettapiece Crescent  
Manotick, Ontario  
K4M 1C5

Contract Number: SEMEX-PHAC-10-391-35-15  
Project Number: CSSP-TI-2016-2236

Technical Authorities:  
James Scala, Manager, Exercise Program, 613-898-6240  
Centre for Emergency Preparedness and Response, Public Health Agency of Canada

Shaye K. Friesen, Risk Analyst, 613-992-0076  
DRDC – Centre for Security Science

**Disclaimer:** The scientific or technical validity of this Contract Report is entirely the responsibility of the Contractor and the contents do not necessarily have the approval or endorsement of the Department of National Defence of Canada.

Contract Report  
DRDC-RDDC-2016-C325  
November 2016

© Her Majesty the Queen in Right of Canada, as represented by the Minister of National Defence, 2016

© Sa Majesté la Reine (en droit du Canada), telle que représentée par le ministre de la Défense nationale, 2016

## Abstract

---

This study is being published by Defence Research and Development Canada's Centre for Security Science (DRDC CSS) as a reference document and artefact to support the Public Health Agency of Canada (PHAC) and other key stakeholders in developing the methodology for the National Risk Profile (NRP) project (CSSP-TI-2016-2236). This report identifies emergent best practices as part of a broad review and renewal of the Health Portfolio (Health Canada and the Public Health Agency of Canada) risk and capability assessment methodology. The observations and recommendations derived from an analysis of how other nations develop national risk profiles focus on the HP but have broader implications and lessons for the NRP project.

## Significance to defence and security

---

Increasing interdependence, a broadening range of threats, accelerating decision cycles and public expectations have prompted many nations to conduct national threat assessments and to publish national risk profiles. The Health Portfolio has recognized the need for refresh its existing emergency risk methodology. In addition to legislated and policy commitments, a formalized and extended risk and capability assessment methodology offers significant benefits. It can:

- Identify and order health related threats;
- Distinguish the capabilities the Health Portfolio requires to respond to these threats;
- Assess existing and programed capabilities to determine performance metrics and discern strengths and shortfalls; and
- Provide sufficient analysis to support decision making and inform investment prioritization.

The Health Portfolio Risk Assessment Task Force agreed on an ambitious work plan which included, as a first step, conduct of an environment survey of national approaches to risk assessment and review of Public Safety Canada's All Hazard Risk Assessment (AHRA) – with a view to informing a Health Portfolio Risk and Capability Assessments.

# Table of Contents

Abstract .....	i
Significance to defence and security .....	i
Table of Contents .....	ii
List of Figures and Tables .....	iv
1. Introduction .....	5
Objective .....	5
Approach.....	5
2. Risk Management.....	6
Benefits .....	6
Principles.....	7
Governance.....	7
Discussion .....	9
Start Up 9 .....	9
Frequency.....	9
Time Horizon.....	9
Sponsorship, Oversight and Approval.....	9
Take Aways.....	9
3. Conduct .....	10
The Risk Assessment Process.....	11
Guides .....	14
All Hazards Approach.....	14
Process .....	14
Stakeholder/Community Engagement .....	15
Take Aways.....	16
4. Risk Assessment .....	17
Risk Identification.....	17
Risk Taxonomy .....	17
Risk Analysis .....	18
Likelihood .....	20
Impact .....	22
Risk Scenarios .....	22
Handling Uncertainty .....	24
Risk Evaluation.....	26
Take Aways and Challenges.....	26
Products and Presentation .....	27
Take Aways and Challenges.....	39
5. Country Case Studies.....	40
The United States.....	40
The Canadian All Hazard Risk Approach.....	42

2011 Health Portfolio Risk Assessment .....	46
Risk Treatment.....	48
Capability Based Planning .....	50
<i>Exercise Perseverance (June 2013)</i> .....	51
6. Conclusion – Summary of Key Findings.....	54
General.....	57
Governance.....	57
Conduct .....	57
Risk Analysis/Risk Evaluation .....	58
Risk Treatment.....	59
7. Bibliography .....	60
8. Annex A. RAND Conceptual Models .....	63
9. Acronyms and Abbreviations .....	65

## List of Figures and Tables

---

Figure 1 Problem Spectrum .....	10
Figure 2 ISO Risk Management Process.....	15
Figure 3 Australian Community Engagement Model.....	16
Figure 4 Laos – Susceptibility to Dengue Fever.....	21
Figure 5- Example of Threat Scale.....	23
Figure 6 Norway – Probability Assessment by Scenario.....	29
Figure 7 Danish Radar Plot .....	30
Figure 8 Norwegian Risk Matrix.....	31
Figure 9 Estonia Risk Matrix .....	32
Figure 10 UK Risk Likelihoods – Malicious Risks & Other Risks.....	33
Figure 11 Dutch Risk Matrix .....	34
Figure 12 Netherlands – Upper and Lower Limits of Likelihood.....	35
Figure 13 Netherlands – Upper and Lower Limits of Consequences.....	35
Figure 14 Netherlands Risk Ratings by Impact Criteria .....	36
Figure 15 Norwegian Risk Ratings by Impact Category .....	37
Figure 16 AHRA – Representation of Uncertainty.....	38
Figure 17 Capability Assessment Management System Dashboard .....	38
Figure 18 Canadian All Hazards Risk Approach .....	42
Figure 19 AHRA Business Cycle.....	43
Figure 20 AHRA Risk Taxonomy.....	44
Figure 21 AHRA Impact Criteria .....	45
Figure 22 Norwegian “Bow Tie” Model.....	48
Figure 23 Netherlands National Safety & Security Strategy.....	50
Figure 24 RAND Propensity for Terrorism Conceptual Model.....	63
Figure 25 RAND Conceptual Terrorist Threat Model.....	64

# 1. Introduction

---

This study is being published by Defence Research and Development Canada's Centre for Security Science (DRDC CSS) as a referential document and artefact to support the Public Health Agency of Canada (PHAC) and other key stakeholders as part of the National Risk Profile (NRP) project (CSSP-TI-2016-2236). It identifies emergent best practices as part of a broad review and renewal of the Health Portfolio (Health Canada and the Public Health Agency of Canada) risk and capability assessment methodology. The observations and recommendations derived from an analysis of how other nations develop national risk profiles focus on the HP but have broader implications.

## Objective

The objective of this report is to:

- Review the findings of an environment scan survey of national risk assessment methodologies;
- Relate these to the All Hazard Risk assessment Approach (AHRA) developed by Public Safety Canada (PS) and DRDC's Centre for Security Science (CSS); and
- Recommend process and practices to support refreshment of the Health Portfolio risk assessment methodology and development of a capability assessment methodology.

## Approach

Open source research was conducted into current risk assessment approaches adopted by allies - Australia, the United Kingdom (UK) and the United States (US) and a number of members of the European Union (EU). Criteria were identified and compared. In many cases best practices are discernible. This report summarizes the results of a (compressed) environmental scan, compares these to the existing All Hazards Risk Assessment (AHRA) and identifies issues to inform a Health Portfolio risk and capability assessment methodology.

## 2. Risk Management

---

The International Organization for Standards (ISO) publishes a family of standards relating to risk management, notably

- ISO 31000.2009 Principles and Guidelines on Implementation;
- ISO/IEC 31010.2009 Risk Management – Risk Assessment Techniques; and
- ISO Guide 73.2009 Risk Management Vocabulary.

These provide an accepted lexicon, established principles and a generic process model which serves as a departure point for most national risk assessments.

The word risk generally connotes the notion of loss, injury or hazard. The ISO Guide links risk to objectives defining risk as the “effect of uncertainty on objectives”. Treasury Board has endorsed this definition of risk, and the Government of Canada’s *Guide to Integrated Risk Management* notes that risk management is an integral component of corporate management which involves “a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues.”<sup>1</sup>

A risk management framework is considered “a set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing, and continually improving risk management throughout the organization”.<sup>2</sup> Risk assessment is a subset of risk management and, first and foremost, a decision-support aid.

Growing attention is being devoted to risk assessment. A complex and continuing volatile environment and increasing public expectations and decreasing public confidence in core institutions have contributed to increasing emphasis being placed on adoption of all hazards approach and a more open and well-structured risk assessment process to inform investment decisions and contingency/continuity plans on both national and enterprise levels. Many risks are shared – a reflection of interdependencies – and treatment involves coordination across all levels of government and between public and private stakeholders. A common appreciation of threats facilitates communication and fosters collaboration.

### Benefits

The benefits of establishing a risk assessment process are well accepted. The nations surveyed developed risk assessment methodologies to promote transparency and encourage “common terminology and shared understanding of concepts”<sup>3</sup>.

Australia’s objectives are representative and include to:

- Enable consistent and rigorous emergency-related risk assessments;
- Increase the consistency and comparability of risk assessments; and
- Improve the national evidence- base on emergency-related risks.<sup>4</sup>

By ensuring that risks are compared on a consistent basis, assessments may be used to inform broader (enterprise-wide) priorities and investment decisions and plans; the UK “assesses and prioritises risks to allow a proportionate allocation of resources by assessing their relative likelihood/plausibility and impact”.<sup>5</sup> These benefits are equally applicable on a portfolio level. Risk assessment can contribute to raising a collective awareness of challenges to shared objectives and to aligning mitigation strategies and prevention and preparation programs.

---

<sup>1</sup> Government of Canada, Guide to Integrated Risk Management, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggirpr-eng.asp> accessed 25 January 2016. The US Department of Homeland Security (DHS) defines risks as “the potential for an unwanted outcome resulting from an accident, event, or occurrence, as determined by its likelihood and the associated consequences”. DHS Risk Lexicon, September 2008, [https://www.dhs.gov/xlibrary/assets/dhs\\_risk\\_lexicon.pdf](https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf) accessed 25 January 2016.

<sup>2</sup> International Organization for Standardization. ISO Guide 73.2009 Risk Management – Vocabulary, 15 November 2009 Section 2.1.1 , <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> accessed 20 April 2016.

<sup>3</sup> European Commission, Staff Working Paper: Risk Assessment and Mapping Guidelines for Disaster Management, Brussels, 2010,

<sup>4</sup> Australian Government. National Emergency Assessment Guidelines (Handbook 10), Second Edition, 2015, page 3.

<sup>5</sup> Organization for Economic Co-operation and Development. National Risk Assessment – Profiles of Selected OECD Countries, 2 December 2015, page 92.



## Principles

Notwithstanding that risk management “should be tailored and responsive to the organization's external and internal context including its mandate, priorities, organizational risk culture, risk management capacity, and partner and stakeholder interests”<sup>6</sup>, a number of overarching principles can be identified. Specifically, a risk assessment process should be:

- Tailored and responsive to an organization’s mandate, culture and capacity;
- Systematic in order to afford an enterprise perspective and identify trade space;
- Inclusive to provide all key stakeholders an opportunity to contribute and share “ownership”;
- Traceable (transparent) in order to facilitate auditing and assure confidence;
- Embedded in corporate management processes and decision cycles.

## Governance

A comparison of governance approaches was conducted, and an overview is provided below (Table 1).

---

<sup>6</sup> Government of Canada, Guide to Integrated Risk Management, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggir-pr-eng.asp> accessed 25 January 2016.

	Frequency	Horizon	Oversight	Approval
<b>Australia</b>	Started 2011			
<b>European Union</b>	N/A	1 - 5 years		
<b>Denmark</b>	First cycle completed in 2013	5 years	National Operational Staff - a virtual organization with representation from the Danish Emergency Management Agency,	Endorsed by Minister for Defence (lead Minister)
<b>Estonia</b>	A national risk process has existed since 2003. <i>Emergency Act</i> is being reviewed		Ministry of the Interior	
<b>Finland</b>	First National Risk Assessment completed fall 2015			Final endorsement at Ministerial level
<b>Hungary</b>	Pilot 2011. First cycle completed July 2014	short term (5 years) and longer term (20-25 years)	Ministry of the Interior	
<b>Netherlands</b>	Annual - reversion to 4 year cycle starting in 2016 proposed to Parliament	5 years	National Steering Committee	
<b>Norway</b>	First cycle 2012, 2nd edition 2013	1 year (this is recognized to pose challenges)		Submitted to parliament, distributed to stakeholders & published online
<b>Poland</b>	First cycle 2011	2 years	Gov't Centre for Security (attached to the Prime Minister's Office)	Approved by the Council of Minister
<b>Sweden</b>	First cycle 2012, latest 2014	5 years	Swedish Civil Contingencies Agency as mandated by Cabinet Reported submitted to Cabinet	
<b>United Kingdom</b>	Annually since 2004  The risk review process takes about 9 months	5 years		Overseen by the Cabinet Office Civil Contingencies Secretariat (CCS)
<b>US</b>	First 2010, 2nd 2014 - Quadrennial Reviews of Homeland Security mandated by Congress)	4 years		Quadrennial Report signed by Secretary of DHS, submitted to Congress
<b>All Hazard Risk Assessment</b>	Annual - tied to fiscal cycle/business cycle (trialled 2010-2013)	1- 5 years plus 5-25 years	Public Safety - Interdepartmental Risk Assessment Working Group	

*Table 1: Comparison of Governance*

## Discussion

### Start Up

Countries have only recently started conducting formal national risk assessments and publishing national risk profiles. While there is no formally accepted definition of a national risk profile, there appears to be an emergent consensus that national risk assessment is a process; national risk profile is a product. The latter should provide an overview of the threat environment and assessment methodology and describe in some detail what are considered to be the most serious risks the nation concerned faces. It should identify exposure and vulnerability and the associated risks to national interests - typically defined in terms of potential effects on people, property, and critical facilities and services. Importantly national risk profiles provide a venue for capturing and sharing assumptions for use by stakeholders charged with preparedness. In practice, few countries have completed many cycles i.e. the methodology is still maturing and could be considered in most cases a “work in progress”.

### Frequency

Most countries follow a 4-5 year cycle for refreshing national risk profiles; the exceptions being Poland which operates on a 2 year cycle and Norway and UK which operate on 1 year cycles. The Dutch have operated on an annual cycle but found this to be labour intensive and have proposed reversion to a 4 year cycle.

### Time Horizon

Most countries operate on a 5 year planning horizon. It is deemed important to be forward leaning and looking. As risk assessments are to be used to support planning and risk treatment, this recognizes that it takes time to build capabilities; hence, the risk horizon should be extended beyond today and the most immediate/eminent challenges. In most cases, there is a separate process for addressing urgent operational priorities. Trying to anticipate threats too far into the future brings with it other challenges. “The further into the future forecasts go, the more data deprived we are”<sup>7</sup> and the more speculative the assessments become.

### Sponsorship, Oversight and Approval

Not surprisingly national risk assessments are government-led. In some cases (e.g. Poland, Sweden, UK) the process is overseen by a central agency (e.g. cabinet secretariat) and the assessment presented to the executive for review and approval. In other cases, a lead department (e.g. Ministry of the Interior), and in the Netherland’s case a National Steering Committee which draws support from private and academic sectors (a Network of Analysts for National Security), is assigned responsibility for conducting the national risk assessment. High level oversight ensures adequate visibility, import and administrative is accorded risk assessment.

### Take Aways

A number of key “take aways” can be identified:

- A 5 year time horizon represents “best practice”;
- An annual cycle is ambitious and would necessitate a standing cadre of support staff. Consideration should be given to linking a Health Portfolio risk assessment to longer term (4 year) strategic planning cycle. This could be related to electoral cycles (e.g. the US Quadrennial Review), current national audit cycles or an internal strategic business cycle; and
- “Best practices” indicate that to embed risk assessment in corporate processes, responsibilities and roles should be clarified including assessment approval authority. High level oversight ensures adequate visibility, import and administrative support is accorded risk assessment.

---

<sup>7</sup> Technology Mapping; Technology Road-Mapping; Expert Technical Panels, etc.” (AHRA) Technology Mapping; Technology Road-Mapping; Expert Technical Panels, etc.” (AHRA) *Foresight* activities and techniques are focused on the longer terms and employ systematic thinking to generate a range of possible futures.

### 3. Conduct

Anticipating the future is not for the faint of heart. The NATO Code of Best Practices for Judgement-Based Analysis in Defence Decision Making distinguishes three classes of situations (Figure 1):

- In the case of *puzzles*, the issue is clear, what needs to be achieved is clear and the way in which this should be done (i.e. the model to be set up and the method to be applied) is also clear. Even in the case where these elements are not immediately clear, an agreement on their definition can be easily reached. Achieving a solution to a ‘puzzle’ may still be complicated but knowing how to build the model and which method to apply is a matter of education and expertise. The quality of the solution (e.g. its optimality) is usually testable.
- *Problems* denote situations where the issue may be more or less clear and structured and what needs to be achieved is (partially) clear as well. However it is not clear at the outset in what way a solution to a problem should be designed. Typically more than one perspective is relevant and a single overall optimum solution will be found. Analysis will require creativity in addition to education and experience and is likely to identify a ‘most preferred’ or ‘satisficing’<sup>1</sup> solution or set of options.
- ‘*Messes*’ or: ‘Wicked Problems’<sup>2</sup> describe complex – seemingly intractable situations defined by indeterminate and changing relationships. There may be some disagreement over cause, priority and remedy. Issues often bridge organizations and decision makers are faced with a moving target. Messes are inherently ill-structured and often the best that can be expected is to identify direction rather than destination; they are not so much solved as managed.<sup>8</sup>

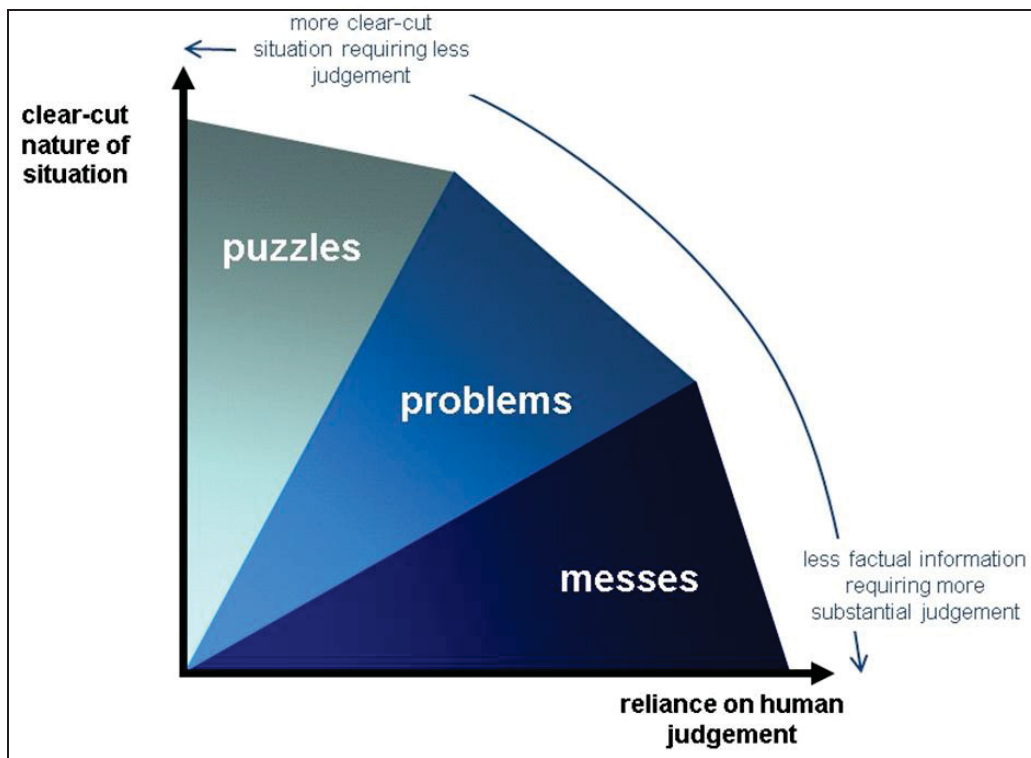


Figure 1 Problem Spectrum

National level risk assessment could best be described as a *mess* and all countries surveyed have recognized the requirement for eliciting subject matter expertise and exploiting judgment-based analysis. Multi-criteria decision analysis (MCDA) has been adopted as best practice to structure *wicked problems* and conduct national risk assessments. MCDA acknowledges that there is more than one criterion, facilitates sensitivity analysis and has proven extremely useful in

<sup>8</sup> NATO Guide for Judgement-Based Operational Analysis in Defence Decision Making, RTO-TR-SAS-087, Analyst-Oriented Volume, June 2012, page 2-2.

preference-ordering alternatives; in this case, sorting and prioritizing risks. It has been incorporated as an integrate component of risk assessment “best practices”.

Expert judgement is used to minimize and characterize uncertainty. Elicitation involves extracting knowledge and judgement and formulating this information in terms of probability. Group elicitation and synthesis has obvious advantages. Collation of assessment from multiple perspectives and subject matter experts’ judgement can be used to reduce variation and shape advice. Aggregation methods fall into two general categories: behavioural and mathematical. In behavioural aggregation, interaction is created between the groups of experts and group consensus is realized (i.e. a single probability distribution). Behavioural aggregation relies on the experts themselves to produce a consensual advice. “In mathematical aggregation, a single distribution is elicited from each expert individually and independently of the others and then the resulting distributions are mathematically combined into a single distribution”.<sup>9</sup> The resultant calculated judgment also can be seen as representing consensus.

Significantly, it has been determined that group elicitation can outperform their best individual member if three conditions are satisfied:

- Impartial facilitation which recognizes expertise, encourages participation and integration of feedback and is, at the same time, aware of and responsive to the potential for biases in the group interaction;
- A well designed protocol involving careful structuring and decomposition of the elicitation task; and
- Continuous feedback (via computer technology) presenting the implications of experts’ judgements.<sup>10</sup>

## The Risk Assessment Process

The next section describes and contrasts national risk assessment processes. A tabular summary is provided below (Table 2).

---

<sup>9</sup> Kevin Leung and Simona Verga. Expert Judgement in Risk Assessment, DRDC Centre for Operational Research & Analysis, TM 2007-57, December 2007. Page iv, <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc88/p529083.pdf> accessed 14 March 2016.

<sup>10</sup> P. Reagan-Cirincione. Improving the Accuracy of Group Judgement: A Process Intervention Combining Group Facilitation, Social Judgement Analysis and Information Technology. *Organizational Behaviour and Human Decision Processes*, 58, 1994, pages 246-270 cited in Kevin Leung and Simona Verga, op. cit. page 20.

Table 2 Comparison of Risk Assessment Processes

	Guidelines	All Hazards Approach	Process	Staffing/Stakeholder Engagement
<b>Australia</b>	National Emergency Risk Assessment Guidelines		Follows ISO model (5 processes) 1. Establish the Context 2. Risk Identification 3. Risk Analysis 4. Risk Evaluation 5. Risk Treatment	First Principle: Communication & consultation with external and internal stakeholder should take place during all phases of the risk management process
<b>European Union</b>	Commission Staff Working Paper + Council Decisions on Risk Assessment and Mapping Guidelines for Disaster Management	Yes	1. Establish context 2. Identify risk 3. Analyze risks 4. Evaluate risks 5. Treat risks	N/A
<b>Denmark</b>	Risk and Vulnerability Analysis (2006) available on-line plus scenario bank	Yes	5 Phases - DEMA identified <i>incident types</i> , DEMA identified analysis criteria, DEMA drafted reports on <i>incident types</i> , OGDs consulted, draft National risk Profile submitted for sign off	Internal & external stakeholder groups(60 organizations) assist formulation e.g. Danish Energy Authority, National IT/Telecom Agency
<b>Estonia</b>		"Restricted AHRA" - does not include terrorism or war  Hazards outside Estonia included if there is a potential for harm to Estonians citizens	1. Define the type of emergency to be assessed  2. Identify the risks through use of scenarios  3. Analyze the probability and impact 4. Evaluate the risks (very high, high, medium, low) 5. Identify risk reduction measures	Crisis Committee serves as a national resiliency forum Expanded (private) engagement under consideration
<b>Finland</b>	Guidance developed to support regional assessments	Yes	Bottom-up. 1. Preparation of "risk cards" (risk identification) by ministries 2. Analysis by working groups (reasonable worst case scenarios)	Multi-stakeholder working groups

<b>Hungary</b>			Three Stages 1. Definition of Societal Values 2. Identification of Threats & Risks 3. Execution of Risk Analysis (using risk scenarios - triggering events, processes, failures)	Ad Hoc Group of Experts supported by 3 subgroups (Natural Disaster, Major Man-Made Disaster & s, Intentional Incidents) - SMEs from ministries, public authorities and research institutions Need for permanent machinery and "sustained collaboration of experts "noted
<b>Netherlands</b>	<i>Working with scenarios, risk assessment and capabilities in the National Safety and Security Strategy of the Netherlands</i>	Yes	Based on elaboration of risk themes - identification and exploration of risks through scenarios which include whether scenario is worst/less probable or probable/less harmful + generic or geographically specific Impact on Critical Infrastructure (products & Services) considered	Network of Analysts for National Security Names of National Safety and Steering Group published
<b>Norway</b>			4 steps 1. Definition of societal values 2. Risk & threat identification and selection 3. Risk analysis of selected scenarios 4. Consolidation and establishment of a risk matrix	15-20 SMEs participate in a scenario development workshops Smaller reference group (5-6) meet 3-4 times a year to discuss methodology, choice of scenarios
<b>Poland</b>		Yes (Risk Analysis includes terrorism, cyber-attacks and riots/public disorder)	"Fragmentary Reports" consolidated by GCS and distributed for review/comment 17 scenarios in 2013	<b>Risk assessment of terrorist acts coordinated by the Internal Security Agency</b>  National Risk Assessment conducted by ministries/agencies and regional authorities. Private sector SMEs participate in CI assessment  The intent is to engage the widest possible spectrum of experts at the regional level in development as risk scenarios
<b>Sweden</b>	Included in the National Risk Assessment		6 steps 1. Specify what should be protected 2. Risk identification, identification of adverse events 3. Selection of events (risks) for analysis 4. Scenario development of selected adverse events 5. Analysis of scenarios (impact, likelihood & uncertainty assessments) 6. Synthesis and evaluation of risks	SME workshops - wide range of stakeholders Validation through in-depth interviews and research  Reviewed within government  Final result distributed to civil protection stakeholders
<b>United Kingdom</b>			Conducted within government	
<b>US</b>	Yes (Threat & Hazard Identification and Risk Assessment Guide)		4 Steps 1. Identify the Threats and Hazards of Concern 2. Give the Threats and Hazards Context 3. Establish Capability Targets 4. Apply the results	
<b>All Hazan Risk Assessment</b>	All Hazards Risk Assessment Methodology Guidelines 2012-2103	Yes	5 Steps 1. Setting the Context 2. Risk Identification 3. Risk Analysis 4. Risk Evaluation 5. Risk Treatment	Workshops

## Guides

To ensure broad, communal acceptance, it is important to work from an agreed lexicon, process and evaluation criteria. Most countries publish Guides to direct national assessment and inform subordinate assessments. These Guides outline processes, establish valuation criteria and provide templates. The intent is to inform both the national and complementary regional risk assessments

## All Hazards Approach

Most nations have adopted all hazards approach to facilitate synthesis. Some nations restrict assessments to domestic risks; a few consider risks to nationals outside the country's borders.

## Process

The methodology is defined in terms of a staged process model. The activities derive (almost without exception) from the steps identified in ISO 31000:

- **Setting the Context** – The process of establishing the scope i.e. articulating an institution's objectives and defining its external and internal parameter to be taken into consideration when managing risks.
- **Risk Identification** – The process of finding, recognizing, and recording risks.
- **Risk Analysis** – The process of understanding the nature and level of risk, in terms of its impacts and likelihood. Risk Analysis includes determining (estimating) the potential consequences and probabilities relating to identified risks.
- **Risk Evaluation** – The process of comparing the results of Risk Analysis with risk criteria to determine whether a risk and/or its magnitude are acceptable or tolerable.
- **Risk Treatment** – The process of identifying and recommending risk control or Risk Treatment options.

Risk assessment is the process of **risk identification, risk analysis and risk evaluation** and the purpose of risk assessment is to provide evidence-based findings to inform risk treatment options analysis and investment decisions.



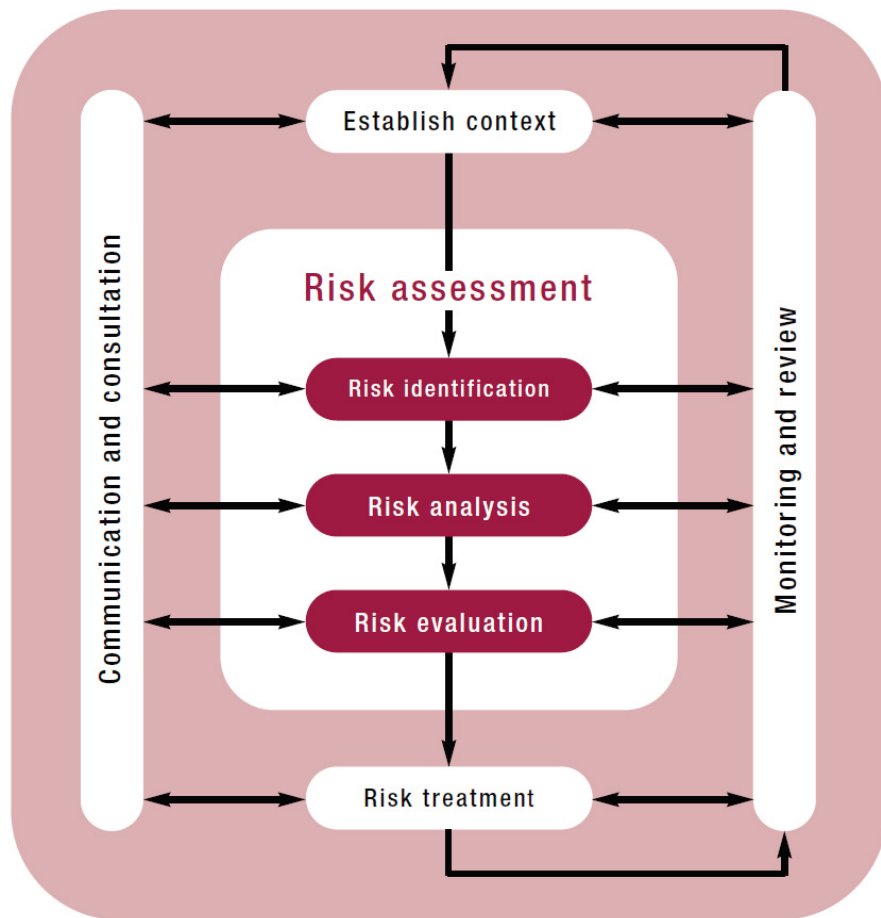


Figure 2 ISO Risk Management Process<sup>11</sup>

## Stakeholder/Community Engagement

There is broad agreement on the need to include stakeholder and engage external partners. This ensures differing perspectives are acknowledged and advantage taken of the collective expertise. It also helps to ensure that assessments are credible and accepted within communities of interest. The Australian Community Engagement Model (Figure 3) captures these benefits.

<sup>11</sup> Association of Insurance and Risk Managers, The Public Risk Management Association and The Institute of Risk Management. A Structure Approach to Enterprise Risk Management (ERM) and the Requirements of ISOP 31000, page 9, [http://www.airmic.com/sites/default/files/ERM\\_ISO-31000\\_guide.pdf](http://www.airmic.com/sites/default/files/ERM_ISO-31000_guide.pdf) accessed 22 December 2015.



Figure 3 Australian Community Engagement Model<sup>12</sup>

There is less consensus on how and when to engage external stakeholders. Some nations solicit suggestions from all stakeholders as part of the *Risk Identification* process; others rely solely on internal expertise. Some also use Subject Matter Experts (SMEs) to cull and assist in developing risk scenarios, others develop risk scenarios internally. The advantage of broader and earlier consultation obviously comes at a cost. Virtually all countries rely on external expertise to assist in *Risk Assessment* and *Risk Evaluation*.

## Take Aways

“Best practices” suggest that:

- A national Risk Assessment Guide should be approved and published. In the absence of a revised and Government approved AHRA or substitute, the Health Portfolio may wish to consider developed – ideally collaboratively- and publishing Health Portfolio Risk/Capability Assessment Guide to complement and extend the existing AHRA to direct internal risk assessment and inform external (partners’) risk assessments;
- The ISO process model should be adopted; and
- Provision should be made for engaging internal and external stakeholders in the risk assessment processes.

<sup>12</sup> Australian Government. National Emergency Assessment Guidelines Practice Guide (Handbook 11), 2015, page 13, <https://www.ag.gov.au/EmergencyManagement/Tools-and-resources/Publications/Documents/Handbook-series/NERAG-Handbook11.pdf> accessed 22 December 2015.

## 4. Risk Assessment

---

### Risk Identification

The survey suggests that approaches to risk identification vary. Most include a bottom-up survey of experts, brainstorming workshops, interviews i.e. a nomination process. As mentioned, in some countries, this involves broad consultation and engaging external stakeholders; in others e.g. the AHRA, this has traditionally involved only key federal departments.

Risk themes emerge and these, in turn, must be grouped and catalogued.

### Risk Taxonomy

A Risk Taxonomy provides a common characterization scheme ensuring that all types of risk have been considered and facilitating aggregation.

- “By providing a comprehensive set of risk categories, it encourages those involved in risk identification to consider all types of risks that could affect the organization's objectives.
- By providing a common set of risk categories, it facilitates the aggregation of risks from across the organization.
- By providing a stable set of risk categories, it facilitates comparative analysis of an organization's risks over time.”<sup>13</sup>

The Treasury Board Risk Framework list of potential risks focuses on organizational and program risks (e.g. Business Processes, Capital Infrastructure, Communications, Conflict of Interest, Financial Management, etc.). All hazards risk taxonomies focus on national existential risks (public safety and security).

Most nations have adopted an all hazard risk approach which facilitates comparative analysis. Typically the taxonomy is based on triggering events<sup>14</sup> and distinguishes between hazards - non-malicious (natural disasters and accidents) - and threats - malicious agents. This distinction is useful and situates assessment i.e. the likelihood of hazards can be estimated through empirical/historical research or deterministic models. The likelihood of threats is, in part, a function of subjective assessment of capability and human intent. This may involve Intelligence assessments raising information sharing issues.

---

<sup>13</sup> Government of Canada. Guide to Risk Taxonomies, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/grt-gtr/grt-gtrtb-eng.asp> accessed 25 January 2016.

<sup>14</sup> Treasury Board defines a risk event as a situation with the potential to affect the achievement of an organization's objectives. Government of Canada. Guide to Risk Taxonomies, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/grt-gtr/grt-gtrtb-eng.asp> accessed 25 January 2016.

Table 3 Comparison of Risk Taxonomies

	Threat Taxonomy
<b>Australia</b>	
<b>European Union</b>	
<b>Denmark</b>	Natural & Man-made Incidents (Extreme Weather, Serious Contagious Disease, Accidents, Security Threats)
<b>Estonia</b>	
<b>Finland</b>	
<b>Hungary</b>	Natural Incidents, Major Accidents, Intentional Incidents
<b>Netherlands</b>	Non-wifful Scenario Wifful Scenarios
<b>Norway</b>	Natural Events Major Accidents Malicious Acts
<b>Poland</b>	1. Natural Disasters 2. Malicious Acts 3. Defence and Military Issues
<b>Sweden</b>	
<b>United Kingdom</b>	
<b>US</b>	1. Natural Hazards 2. Technological. Accidental hazards 3. Human-caused threats/hazards
<b>All Hazard Risk Assessment</b>	Adaptive/Malicious (Criminal, Foreign State) Non Malicious (Unintentional, Natural, Health, Emerging Phenomena)

## Risk Analysis

Risk analysis is conducted to assess the level of risk a hazard/risk poses. It involves assessments of both likelihood and impact.

ISO 31000 recommends that risks be seen as the combination of the consequences of an event and the associated likelihood of its occurrence. National risk assessments defined in terms of dimensional impacts. Most nations use scales to facilitate assessments.

Table 4 Evaluation Criteria

	Probability Criteria	Impact Criteria (Indicators)
Australia	6 point scale - Extremely Rare, Very Rare, Rare, Unlikely, Likely, Almost Certain Based in part on average recurrence rates/annual exceedance probability	<ol style="list-style-type: none"> <li>1. Death of, or injury or illness to people</li> <li>2. Loss in economic activity and/or asset value and/or negative effect on important industries in the economy</li> <li>3. Loss of species and/or landscapes and/or environmental values in the environment</li> <li>4. Loss or destruction of community well being, and/or loss or destruction of culturally important objects and activities in the social setting</li> <li>5. Inability of governing bodies to deliver their core functions.</li> </ol>
European Union		Human impact
		Economic & Environmental Impacts
		Political & Social Impacts
Denmark	Does not attempt to put a value on likelihood	<ol style="list-style-type: none"> <li>1. Harm to life, health&amp; well-being</li> <li>2. Harm to property &amp; the economy</li> <li>3. Harm to the environmental</li> <li>4. Availability of critical societal functions</li> </ol>
Estonia	5 point, logarithmic scale (Very Low, Low, Medium, High, Very High)	5 point (A-E) scale, 4 criteria <ol style="list-style-type: none"> <li>1. Human Life and health</li> <li>3. Asset damage</li> <li>4. Natural Environment</li> <li>5. Vital Service</li> </ol>
Finland	5 point Richter scale (Very Low, Low, Average, Significant, Catastrophic) - only applied to "Tier 2" risks. All "Tier 1" risks considered plausible/equally likely	5 criteria <ol style="list-style-type: none"> <li>1. Human Impact</li> <li>2. Economic impact</li> <li>3. Environmental impact</li> <li>4. Impact on Critical Infrastructure</li> <li>5. Impact on vital functions</li> </ol>
Hungary	5 point Richter scale - Very Unlikely, Unlikely, Possible, Likely, Very Likely	5 societal vales/8 impact criteria <ol style="list-style-type: none"> <li>1. Human Life &amp; Health (a. Deaths,b. Illness &amp; Injuries)</li> <li>2. Nature/Environment (Long term damage to nature and the environment)</li> <li>3. Finance/Economy (Financial and Material Loss)</li> <li>4. Stability of Society (a. Social Unrest), b. Disturbance to Daily Life)</li> <li>5. Ability to Govern and Territorial Control (Weakened National ability to Govern, b. Weakened Control of Territory)</li> </ol>
Netherlands	5 point logarithmic scale - Highly unlikely, Unlikely, Likely to a certain extent, Likely, Highly Likely	5 Point Richter Scale based on descriptive impact indicators <ol style="list-style-type: none"> <li>1. Territorial Security (a. Encroachment of territory, b. Infringement of International Standing)</li> <li>2. Economic Security (Cost and Impairment of the Economy)</li> <li>3. Ecological Security (Long-term Impact on Nature and the Environment)</li> <li>4. Physical Safety (a. Fatalies, b. Injuries, c. Physical Suffering)</li> <li>5. Social and Political Stability (a. Disruption of Everyday Life, b. Violation of the Democratic System, c. Social Psychological Impact and Social Unrest)</li> </ol>
Norway	5 point Richter (Very Low, Low, XXX, High, Very High) with supporting logarithmic scale <b>No probability assessments conducted for malicious acts.</b>	8 criteria based on 5 " societal assets" point scale <ol style="list-style-type: none"> <li>1. Life &amp; Health (a. death,b. Injuries)</li> <li>2. Nature &amp; the Environment (Long term damage to nature and the environment)</li> <li>3. Economy (Financial and material losses)</li> <li>4. Societal Stability (a. Social Unrest, b. Impact on daily life)</li> <li>5. Capacity to govern and maintain territorial control (a. Weakened national capacity to govern, b. weakened territorial control)</li> </ol>
Poland	5 point word ladder - Very Rare, Rare, Possible, Likely, Very Likely	5 point scale (Irrelevant, Small, Medium, Large, Disastrous), 3 criteria rated - human, economic & environmental impact <ol style="list-style-type: none"> <li>1. Human Impact (Fatalities, Hospitalizations, Evacuations, Impact on daily life)</li> <li>2. Economic/Property/Infrastructure Impacts</li> <li>3. Critical Infrastructure Impacts</li> <li>4. Environmental Impacts</li> </ol>

	5 point Richter scale - Very Low, Low, Medium, High, Very High with logarithmic guide	5 "National Protection" Values/Criteria rated. (Indicators in brackets). Rated using 5 point Richter scale (Minimal, Minor, Average, Significant, Very Significant) with logarithmic guide 1. Society's Functionality (Disruption to everyday life) 2. Human Like and Health (Fatalities, Severely injured/ill, Lack of fulfillment of basic needs, evacuations) 3. Economic Values and the Environment (economic impact, impact on nature and the environment) 4. Democracy , Rule of Law and Human Rights & Freedoms (Social unrest, lack of confidence in/control over public institutions, impact on political decisions, impact on international reputation) 5. National Sovereignty (territorial control)
<b>Sweden</b>		
<b>United Kingdom</b>	5 point Richter scale (logarithmic)	Human Impact Economic Impact Disruption of Essential Services/Social Services Environment Psychological
<b>US</b>		6 criteria 1. Loss of Life 2. Injuries and Illnesses 3. Direct Economic Costs 4. Social Displacement 5. Psychological Stress 6 Environmental impact
<b>All Hazard Risk Assessment</b>		6 Criteria assessed using a 10 logarithmic Richter scale i.e. 1- 5 with 0.5 intervals 1. People (DALY) 2. Economy (direct & indirect) 3. Environment 4. Territorial Security 5. Canada's Reputation & Influence 6. Social and Psych-Social

People have a preference for communicating uncertainty using words. “Linguistic probabilities provide greater elasticity of meaning than numerical probabilities. Not only do words free creative expression and lend themselves to the narrative structure of intelligence reporting, they can also ease the short-term accountability pressures on analysts or other expert assessors.”<sup>15</sup> Directionality also may introduce interpretative biases. “If a term has negative directionality (e.g., unlikely), then strengthening it will convey even a lower probability of occurrence (e.g., very unlikely). Conversely, a term with positive directionality (e.g., likely) will convey a higher probability of occurrence when strengthened (e.g., very likely)... Directionality conveys information to receivers about a speaker’s recommendations, preferences, or beliefs.”<sup>16</sup> Consequently many Intelligence Services have tried to establish ordinate scales to standardize use of probability scales. Research into consumers’ perspectives underscores the importance of a communication standards.

Most national risk assessment methodologies – “best practices” - provide for scores and descriptions to reduce miscommunication a simple word ladder might introduce.

## Likelihood

“Likelihood is an estimate of the chance of an event or an incident happening, whether defined, measured or determined objectively or subjectively ... Likelihood can be assessed quantitatively using deterministic methods (models and simulations) or probabilistic methods (calculating probabilities from historical data or proxy indicators).<sup>17</sup>

As a prelude or sometimes as part of the national risk assessment process, some countries include baseline information in the form of atlases depicting hazard-prone areas based on topography and/or historic records of disaster. Examples

<sup>15</sup> David Mandel. Accuracy of Intelligence Forecasts From the Intelligence Consumer’s Perspective, DRDC-RDDC 2015-PO92, page 3, [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390_A1b.pdf) accessed 28 March 2016.

<sup>16</sup> David Mandel. Accuracy of Intelligence Forecasts From the Intelligence Consumer’s Perspective, DRDC-RDDC 2015-PO92, page 3, [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390_A1b.pdf) accessed 28 March 2016.

<sup>17</sup> Public Safety Canada, All Hazards Risk Assessment: Methodology Guidelines 2012-2013, 2012, page 22 <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-sssmnt/index-eng.aspx> accessed 23 April 2015.

include maps depicting fault lines and regions where earthquakes are more likely to occur, flood plain maps illustrating areas vulnerable to floods, and charts depicting historic weather patterns precipitation where severe weather storms or drought are more likely to occur. Overlaying population distribution and critical infrastructure (e.g. electrical generation facilities, transportation hubs) facilitates impact assessments. The Laotian national risk profile includes maps illustrating disease patterns (Figure 4). Such maps help situate scenarios.

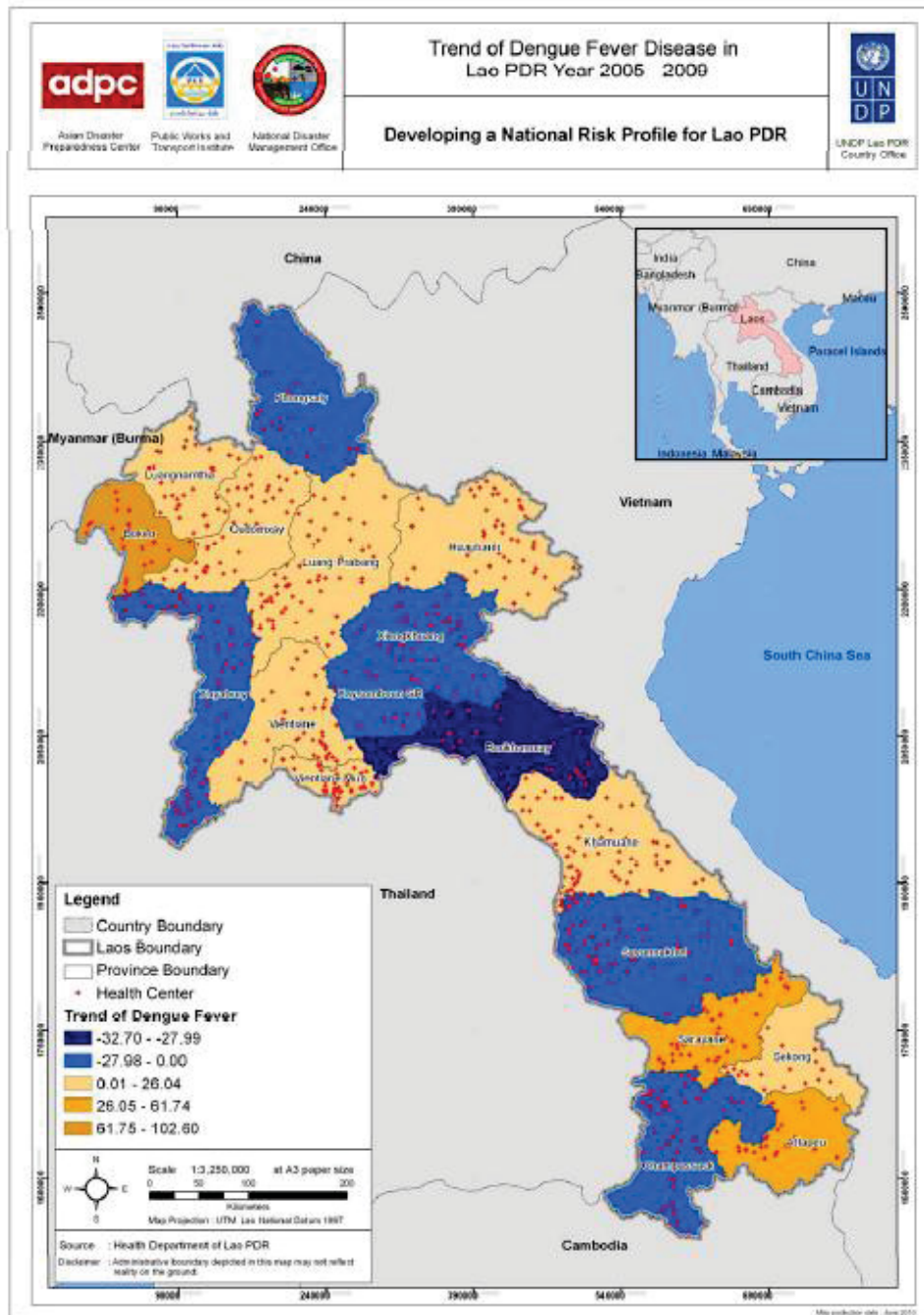


Figure 4 Laos – Susceptibility to Dengue Fever<sup>18</sup>

All countries tend to use a 5 point Richter scale with and qualitative descriptors, and most have associated quantitative guides, to facilitate assessments. Combinations of historical data, trend analysis and/or simulations to project the

<sup>18</sup> Asian Disaster Preparedness Centre. Developing A National Risk Profile of Laos, Part 1: Hazard Assessment, November 2010, page 69, [http://www.adpc.net/igo/category/ID275/doc/2013-s-WNa61-ADPC-Final\\_Report\\_Part1.pdf](http://www.adpc.net/igo/category/ID275/doc/2013-s-WNa61-ADPC-Final_Report_Part1.pdf) accessed 24 April 1016

likelihood of occurrence are used to inform non-malicious risk assessments. As mentioned these are more appropriate for forecasting natural disasters and accidents than terrorist-related events. Intelligence judgments are used to inform estimates of malicious threats. Target vulnerability and agent capabilities and intent are often used to inform such estimates. This may restrict both the participation of SMEs - if they require security clearance to access supporting Intelligence estimates – the subsequent distribution of the consolidated risk profile within the community.

## Impact

The concept of Value-Focused Thinking (VFT) was developed by Ralph Keeney. He argued that people often focus first on identifying and comparing options rather than on articulating and prioritizing objectives. In VFT “values” (rating criteria) are determined before rather than after alternatives are identified. The key is to start with objectives. Some countries define national interests more narrowly than others i.e. some hazard/risk taxonomies provide for civil unrest and others for extraterritorial demands to protect nations outside the homeland. The Health Portfolio may wish to err on the expansive side in order to consider any unique risk posed/capabilities invoked an international deployment poses. A number of countries start by distinguishing national interest then derive impact criteria from these. Others simply identify and describe impact criteria using scales and word ladders to facilitate analysis of the multi-dimensional consequences of a hazard/threat event. Typically these include the following four to five dimensions

- People
- Economy
- Environment
- Critical Services
- Social

There is general agreement that, insofar as possible, impact analysis should rely on empirical evidence and experience. One of the most significant challenges is the ability to estimate the domino effects and cascading risk. One event may have sequential consequences. Impact varies over time e.g. longer term economic, environmental and/or health implications may need to be weighted and it is more challenging to estimate forthcoming rather than immediate impacts. Typically, likelihood and impact assessments are handled by leveraging and coordinating the subjective input of affected stakeholders and SMEs. A modified *Delphi* approach may be used. It is a well-established method for structuring knowledge elicitation and promoting convergence of opinion. A questionnaire is conducted, data collected and the resultants reviewed/discussed by participants and another iteration of rating conducted.

All countries provide hierarchies with accompanying narrative descriptions (word ladders) to assist raters. Logarithmic scales reflect orders of magnitude rather than equal steps and, given the large range, were deemed more appropriate than linear scales.<sup>19</sup>

## Risk Scenarios

Scenarios are used by all nations surveyed to illustrate identified hazards/threats. They provide the means to make explicit context and assumptions i.e. identify plausible conditions and cause-effect relationships and to define prevention, preparation, response and recovery requirements which invoke capability demands. They can be used to characterize the problem space, support the rehearsal of risk treatment options and facilitate the evaluation of new technology. There are a large number of factors resulting in near infinite number of possibilities which can be combined and sequenced to generate risk scenarios. Consequently all nations select a sample set to focus analysis and render the assessment process manageable. Scenario selection is important if the aim is to aggregate and provide a national/enterprise-wide depiction of risk. It is important to consider all appropriate hazards/risks.

There can also be wide divergence in scenario timelines and the scale and import of consequences. Common practice made explicit in UK direction is to base assessments on a “reasonable worst case”. This represents the northeast point on

---

<sup>19</sup> On a logarithmic scale, each mark on the scale is the previous tick mark *multiplied* by some number. Examples include the Richter scale for measuring the magnitude of earthquakes.



a likelihood/consequence frontier and is considered to offer a challenging manifestation of the hazard/risk.<sup>20</sup> The US Material Threat Assessment (MTA) has adopted similar approach developing “plausible, high consequence” scenarios to frame assessments.<sup>21</sup>

Information on which to base assessments may be absent, insufficient or unreliable. In many models range and randomness can be represented using distribution curves, although the norm in national risk assessments is to simplify and employ a level or range. An example is provided below (Figure 5).

Threat Levels		
Level or Tier	Nominal Score (Range)	Qualitative
1	1 (0–2)	<b>Very low:</b> not a threat or otherwise not worth follow-up action
2	3 (2–4)	<b>Low:</b> probably not a threat but merits modest follow-up action
3	5 (4–6)	<b>Medium:</b> merits follow-up actions to improve information
4	7 (6–8)	<b>High:</b> merits follow-up actions with expectation of likely surveillance, arrest, or interdiction
5	9 (8–10)	<b>Very High:</b> merits maximum response, with regular updates at top level and extensive alerts down the line

Figure 5- Example of Threat Scale

A “black swan” event is by definition an outlier falling “outside the realm of expectations, because nothing in the past can convincingly point to its possibility”<sup>22</sup>. They may be no precedents and black swans again by definition have an extreme impact. Given this unpredictability (unstructured randomness), black swans cannot be represented using probability distribution curves and it is generally concluded the only realistic preventative/preparedness course of action open is to foster robustness. No national risk assessments explicitly attempt to cater for black swans.

The scale and level of fidelity of scenarios varies. Aggregation is a fundamental challenge. Abstract scenarios can be used to explore representative hazards/threats. Geo-referenced scenarios can be used to inform contingency plans for specific regions/ municipalities. National scenarios represent hazards/threats which are sufficient large or severe enough to warrant intervention by a central/federal government.<sup>23</sup> Insufficient information is available to comment and compare the detail provided in national risk scenarios.

<sup>20</sup> U.K. Cabinet Office, National Risk Register of Civil Emergencies, 2013 edition, page 3, accessed 4 January 2016.

<sup>21</sup> MTA 2.0 Collaboration and Methodology presentation at the PHEMCE Stakeholders Workshop 6 January 2016.

<sup>22</sup> Nassim Nicholas Taleb. The Black Swan: the Impact of the Highly Improbable, Random House, New York, 2007, page Xvii.

<sup>23</sup> In Canada’s case these are spelled out to some degree in the *Emergency Management Act*. The *Emergencies Act* defines what constitutes a ‘national emergency’<sup>23</sup> and establishes procedures for declarations of a public welfare emergency and/or an international emergency. It stipulates when intervention by the Federal Government is warranted. It specifies, *for the purposes of this Act, a “national emergency” is an urgent and critical situation of a temporary nature that*

## Handling Uncertainty

Risk assessment is not a science. Analysis is informed by stakeholder and SME estimates. There is no consensus on “best practices” to handle uncertainty, but there is general acknowledgement of the requirement to explore uncertainty exploration i.e. document the variation or imprecision inherent in the results of the Risk Analysis, the collective deviation in assumptions and judgements. The intent, in part, is to clarify and characterize the fragility of the underlying value-judgments.

---

*(a) seriously endangers the lives, health or safety of Canadians and is of such proportions or nature as to exceed the capacity or authority of a province to deal with it, or*  
*(b) seriously threatens the ability of the Government of Canada to preserve the sovereignty, security and territorial integrity of Canada*  
*and that cannot be effectively dealt with under any other law of Canada.*

*An integrated Government of Canada response is required when:*

- *a province/territory requests federal support to deal with an emergency;*
- *an emergency affects multiple jurisdictions and/or government institutions and it requires a coordinated response;*
- *an emergency directly involves federal assets, services, employees, statutory authority or responsibilities, or it affects confidence in government; or*
- *an emergency affects other aspects of the national interest<sup>23</sup>*

Table 5 Handling Uncertainty

	Scenarios	Likelihood	Impact	Confidence	Presentation
Australia				Highest High Moderate Low Lowest	
European Union					
Denmark					
Estonia					
Finland					
Hungary					Three diagrams Basic - equal weight to impact criteria Uncertainty - Bounds for Likelihood and Impact Sensitivity - Defined weights for impact Criteria
Netherlands	Worst Case, Probable, Less Harmful	Forecast Lower Limit Upper Limit			Based on equal weighing of impact criteria Some sensitivity analysis conducted
Norway	A specific effort is made to specify assumptions	An uncertainty rating is captured for all estimates			
Poland					
Sweden	Scenarios assessed for uncertainty (reliability of supporting data, confidence in likelihood and impact scores)			High Medium Low	Impact scores assigned equal weight
United Kingdom	Generic risks				
US					
All Hazard Risk	Elevated Impact Variation, Nominal Scenario, Reduced			An confidence rating 5 point scale (a-e) is captured for each impact rating	

The use of scenarios helps in that it makes many if not most governing assumptions explicit. These are used to bound the risk assessment. Sensitivity analysis may be conducted to explore the effects of variations in specific assumptions and/or discrete parameters. The Netherlands categorizes scenarios in terms of Worst Case, Probable and Less Harmful making clear which case is being evaluated. As previous mentioned, many countries defer to credible injurious cases. As the UK notes, risk scenarios are intended “to represent orders of magnitude rather than precise measures “.<sup>24</sup>

Likelihood scales represent estimates of frequency and probably. In some cases ranges are provided to accompany scores; more often it is accepted that the ordinal rating represents an estimate. Impacts can vary and some countries have tried to provide scenario variants in order to capture this range of contextual assumption e.g. the Netherlands (Worst Case, Probable, Less Harmful) and the Canadian All Hazards Risk Approach (Elevated Impact Variation, Nominal Scenario, Reduced Impact Variation). More countries seemed to have – whether by explicit choice or implicit fall back) on credible, high consequence scenarios.

<sup>24</sup> Organization for Economic Co-operation and Development. National Risk Assessment – Profiles of Selected OECD Countries, 2 December 2015, page 97.

In some countries, the range of estimates is presented, often as an oval on a risk matrix diagram, to depict graphically – as vectors or elliptical bubbles - the variance among subject matter experts. It does not appear standard deviation is calculated or used. Prior reference has been made to *Delphi* methods whereby results are anonymized and distributed to stimulate discussion and promote convergence.

In many countries, assessors are asked to rate their level of confidence in the supporting data and in their likelihood and impact assessments. The criteria Australia uses to rate confidence is representative; it includes an assessment of the:

- “reliability, relevance and currency of the evidence used to support the consequence and likelihood assessments;
- use of appropriate expertise as part of the risk assessment process to assign the consequence and likelihood levels; and
- level of agreement between stakeholders”<sup>25</sup>.

Scales are provided to assist in directing confidence rates. Sweden, for example, invites assessors to rate their confidence – High, Medium or Low - in the reliability of the supporting data and resultant likelihood and impact assessment. Other countries e.g. Australia and the AHRA use 5 point scale. Confidence can, again, be represented on a risk matrix to convey assurance in the results. These provide consumers with some sense of the degree of reliance to be placed on the results.

In most cases the presentations depict aggregate and normalized scores with equal weighting assigned to impact criteria. Some countries conduct sensitivity analysis – adjusting impact criteria weights - and publish the results. A recent RAND report is instructive and suggests that equal weights offer a reasonable starting place; different weights should be used when one has specific domain knowledge.<sup>26</sup>

## Risk Evaluation

The Risk Evaluation process involves consolidation and comparison of the result of risk analysis. Use of a common set of criteria facilitates risk evaluation.

## Take Aways and Challenges

A number of key “take aways” can be identified:

- The ISO 31000 process model informs national risk assessment methodologies and should be used as the departure point for a Health Portfolio risk assessment methodology;
- Stakeholder engagement should be a key element in a Health Portfolio risk assessment methodology; most importantly in *Risk Analysis*;
- A Health Portfolio Risk Taxonomy – based on natural, accidental and malicious distinctions - should be developed. This will involve refreshing the 2011 extension of the AHRA Risk Methodology;
- Numerical scores and descriptions should be used to elaborate and establish communication standards to support consumers ;
- The (logarithmic) rating schema used nationally should suffice for assessing likelihood;
- Common impact criteria include people, the economy and the environment. In addition many also provide for assessment on critical service/societal stability;
- “Best practices” include use of representative, “reasonable worst case/plausible high consequence’ risk scenarios to capture assumptions and provide a contextual setting for analysis. Scenarios identified as high risks may be subject of a further, more detailed analysis;
- There is general acknowledgement of the need to recognize variance in assessments but no emergent “best practice” to draw upon. In some countries analysts are asked to record their confidence in their ratings.

Two key issues which present challenges can also be identified:

---

<sup>25</sup> Australian Government. National Emergency Assessment Guidelines (Handbook 11), Second Edition, 2015, page 42.

<sup>26</sup> Davis, Paul K., Walter L. Perry, John S. Hollywood, David Manheim. Uncertainty-Sensitive Heterogeneous Information Fusion, RAND, 2016, page 37, [http://www.rand.org/pubs/research\\_reports/RR1200.html](http://www.rand.org/pubs/research_reports/RR1200.html) accessed 21 April 2016

- In order to capitalize on selective SME crowdsourcing<sup>27</sup>
- The availability of – including access to sensitive/classified - data poses challenges. Health Portfolios SMEs may be in a position to advise on the feasibility of preparing, storing, transporting, release and persistence of a biological and/or chemical agent, and impact, but are likely not in a position to gauge the intent and capability of a terrorist organization/cell. There appear to be two commonly employed approaches;
  - Integrate SME judgement into Intelligence Assessments – distinctive from Risk Assessments;
  - Have Intelligence analysts participate in risk assessment workshops restricting attendance to SMEs with appropriate security clearances. This helps to ensure coherent and consistent analysis but in most cases restricts distribution of the aggregated evaluation.

## Products and Presentation

All countries acknowledge the importance of risk communication, and many countries publish the results. In most cases, the national risk assessment is approved and published and includes – sometimes as a separate document, more often as an integral part of the assessment - a catalogue of risk scenarios. Several countries, notably the U.K., publish both a classified (National Risk Assessment) and a complementary, unclassified document (National Risk Register of Civil Emergencies).

National risk assessments are used in part to raise public and community awareness highlighting in part the responsibility of individual citizens and to align plans. There is some variance in how much detail is provided. Some countries prefer to provide a detailed description and discussion of the risk posed; others prefer to limit the amount of detailed shared.

---

<sup>27</sup> Crowdsourcing is a term used to describe the practice of obtaining services, ideas or content by soliciting contributions from a large number of people, in this case SMEs.

Table 6 Comparison of Products & Presentation

	Products		Presentation
<b>Australia</b>	Risk Register Establishes risk priority clusters (Highest Priority, High Priority, Medium Priority, Low Priority, Broadly Acceptable Risk) Then categorizes #1 Risks requiring treatment, #2 Risks requiring further analysis & subsequent valuation and #3 Risks (currently) requiring ongoing monitoring and maintenance of existing controls		
<b>Denmark</b>	National Risk Profile ("selective catalogue of risks") Scenario Bank	10 most serious natural & man made risks Stand by list of next 20	Radar plot (criteria provide axes + serious, very serious, critical rings)
<b>Estonia</b>	1. National Summary of Emergency Risk Assessments 2. Emergency Risk Assessments by Government Ministries 3. Emergency Risk Assessments by Vital Service Providers	Currently 27 types of emergency	Risk Matrix ((Probability & Impact axes)
<b>Finland</b>		21 risks 13 illustrative scenarios	Top Risks - 4 axes radar plot) Tier 2 - risk matrix Risk maps - risk zones defined based on the national incident database
<b>Hungary</b>	National Disaster Risk Assessment		Three risk diagrams Basic - equal weight to impact criteria Uncertainty - bounds impact & likelihood Sensitivity - defined weights for impact criteria
<b>Netherlands</b>	National Risk Assessment		Risk Matrix and Chart
<b>Norway</b>	National Risk Assessment (17 potentially "catastrophic" scenarios) Results briefed to ministers, incorporated into a government white paper		Risk Matrix Bar charts showing consequences by type (criteria) for each scenario + aggregation Bow Tie Model - Probability Reducing Barriers on one side, Consequence Reducing Barriers for each scenario
<b>Poland</b>	<i>Report on Threats to National Security</i> Conclusions reflected in the <i>National Crisis Management Plan</i>	Report on Threats to National Security approved by Council of Ministers	
<b>Sweden</b>	National Risk Assessment published online. 2013 NRA describes methodology, identifies 27 serious/national events risks, develops 11 risk scenarios and analyzes 7 of these		Risk Matrix. Colours used to suggests level of certainty
<b>United Kingdom</b>	National Risk Assessment (Classified) Unclassified National Risk register		
<b>All Hazard Risk Assessment</b>			Risk Matrix Groupings (Reduced, Nominal & Elevated Risks) CAMS Dashboard

Scenarios likelihoods can be compared and presented (Figure 6).

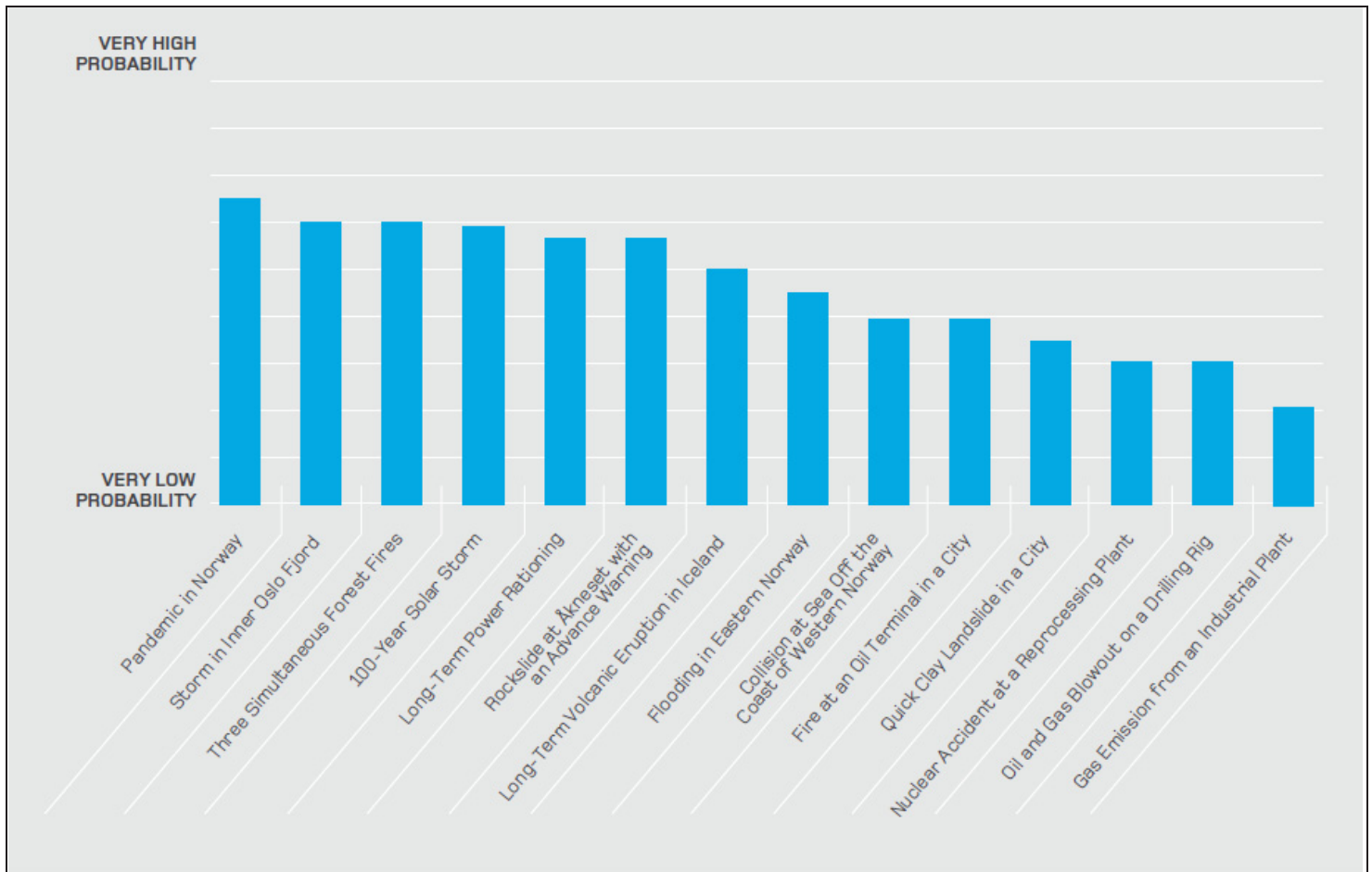


Figure 6 Norway – Probability Assessment by Scenario<sup>28</sup>

ISO 31000 notes that a common approach is to use bands to distinguish clusters e.g. high (unacceptable), medium (requiring costs/benefit analysis) and low (acceptable) risks and a number of countries have adopted this approach recognizing that algorithmic rankings based on value judgements may impart a false sense of precision.

Risk assessments are conducted to assist in ordering hazards and threats to facilitate establishing investment priorities and plans. The Danish “radar plot” (Figure 7) uses concentric circles (Inner circle = Critical consequences. Middle circle = Very serious consequences. Outer circle = Serious consequences) to distinguish impact. It offers one approach.

<sup>28</sup> Norwegian Directorate for Civil Protection. 2013 National Risk Analysis, page 172, [http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB\\_2013\\_english.pdf](http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf) accessed 24 March 2016.

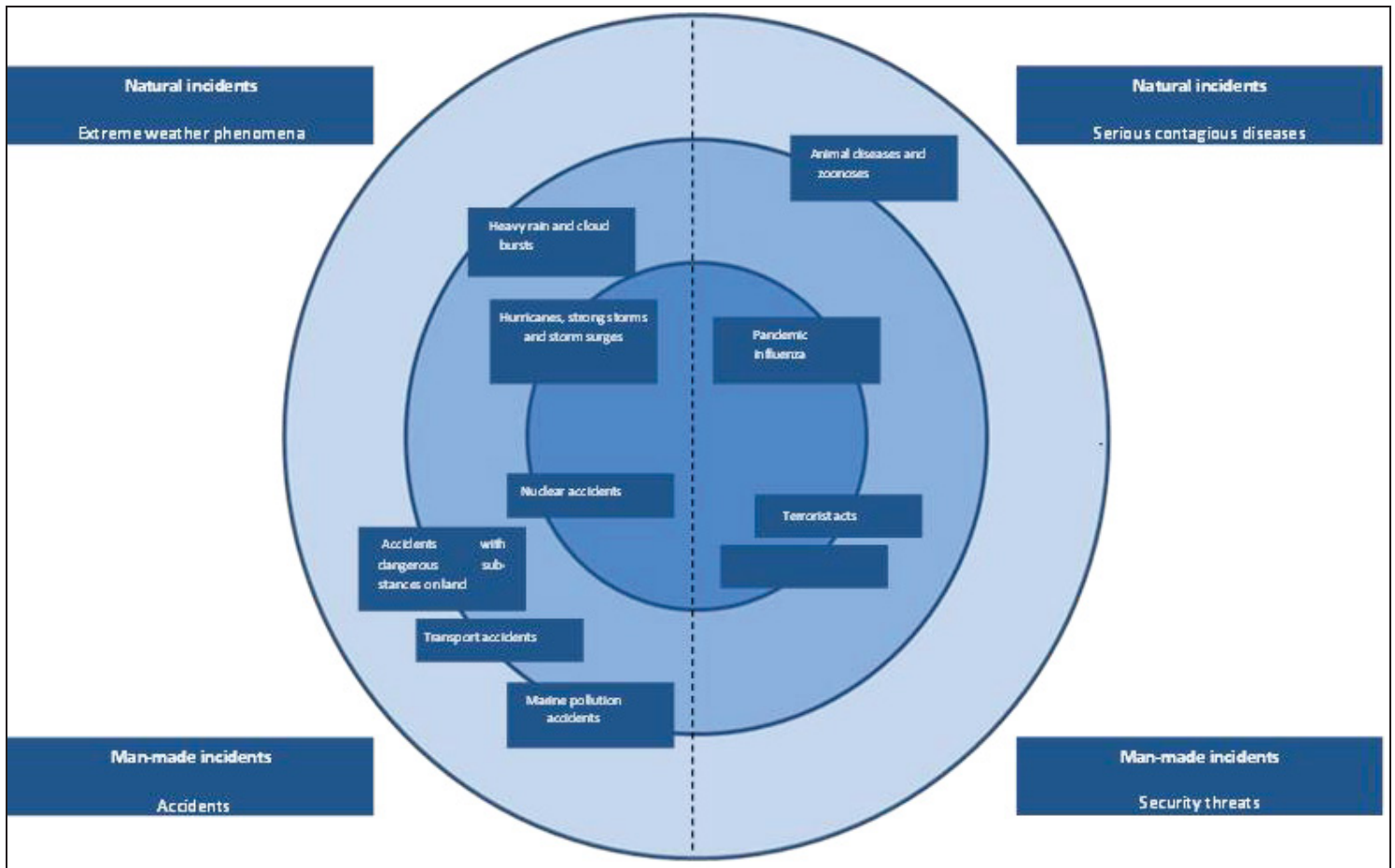


Figure 7 Danish Radar Plot<sup>29</sup>

Most commonly the results of national risk assessments are presented as a risk matrix with risks (often described using risk scenarios) positioned in a two dimensional likelihood versus impact graph. Often colours are added to distinguish higher order risk scenarios. Example are provided below (Figure 8 and Figure 9).

<sup>29</sup> The Danish Emergency Management Agency (DEMA). National Risk Profile, page 53, [http://brs.dk/viden/publikationer/Documents/National\\_Risk\\_Profile\\_\(NRP\)\\_-\\_English-language\\_version.pdf](http://brs.dk/viden/publikationer/Documents/National_Risk_Profile_(NRP)_-_English-language_version.pdf) accessed 24 March 2016.



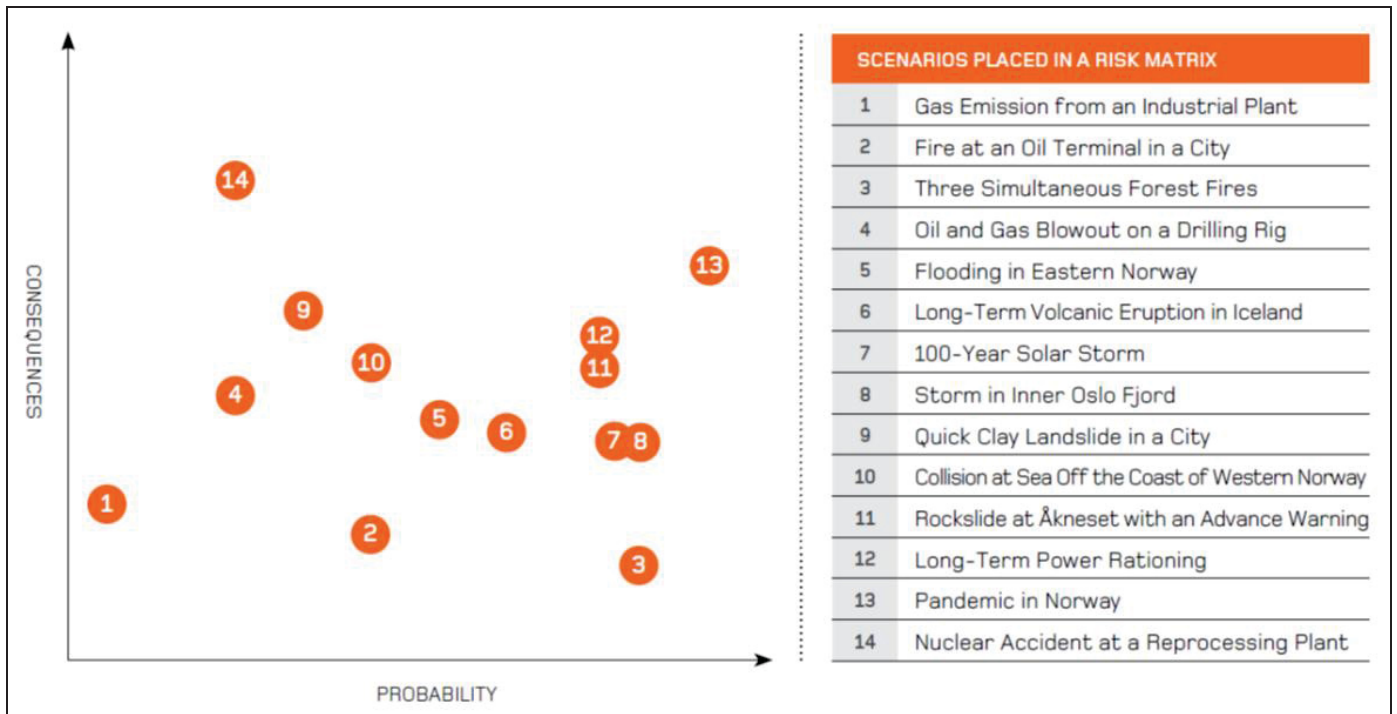


Figure 8 Norwegian Risk Matrix<sup>30</sup>

<sup>30</sup> Norwegian Directorate for Civil Protection. 2013 National Risk Analysis, [http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB\\_2013\\_english.pdf](http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf) accessed 24 March 2016.

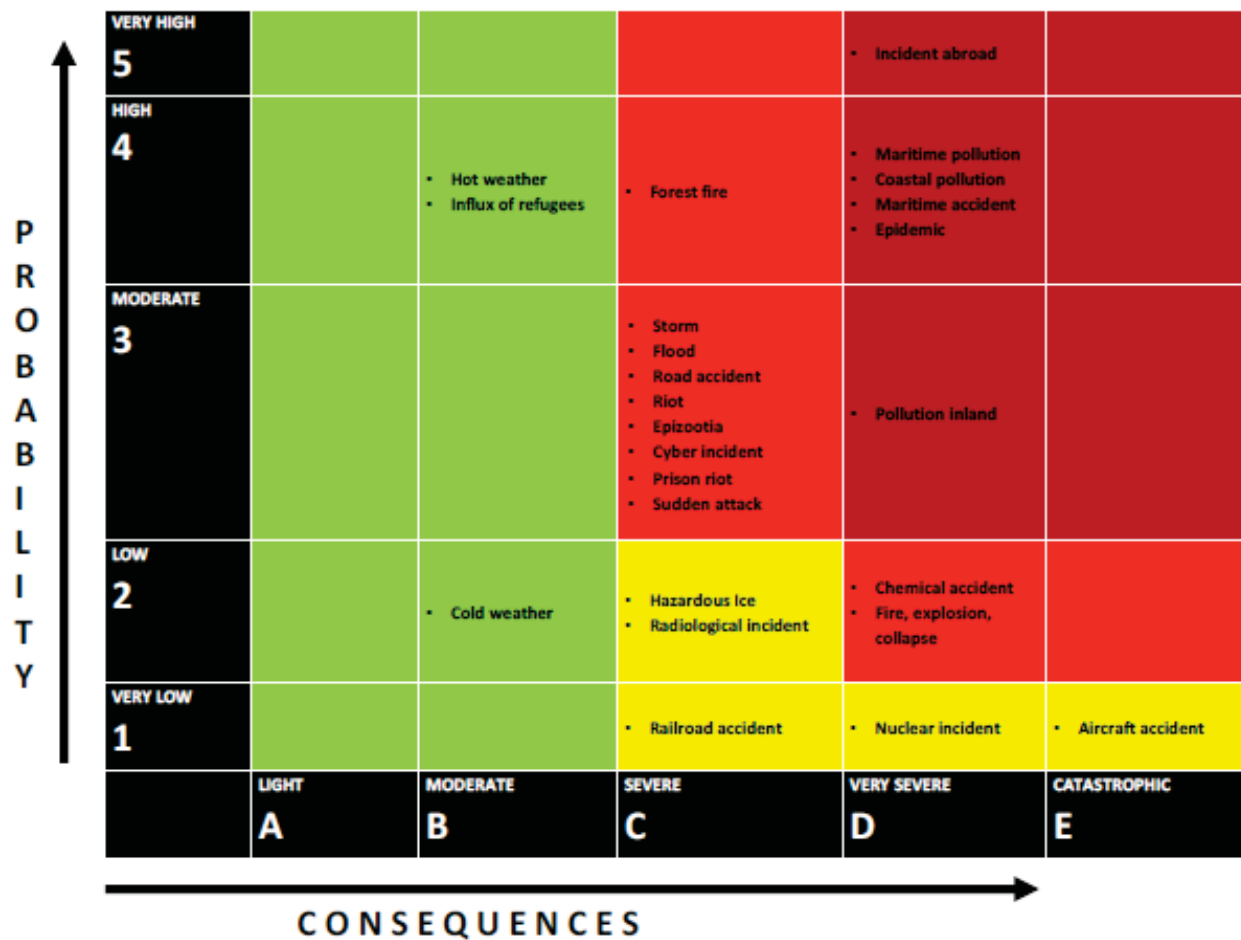


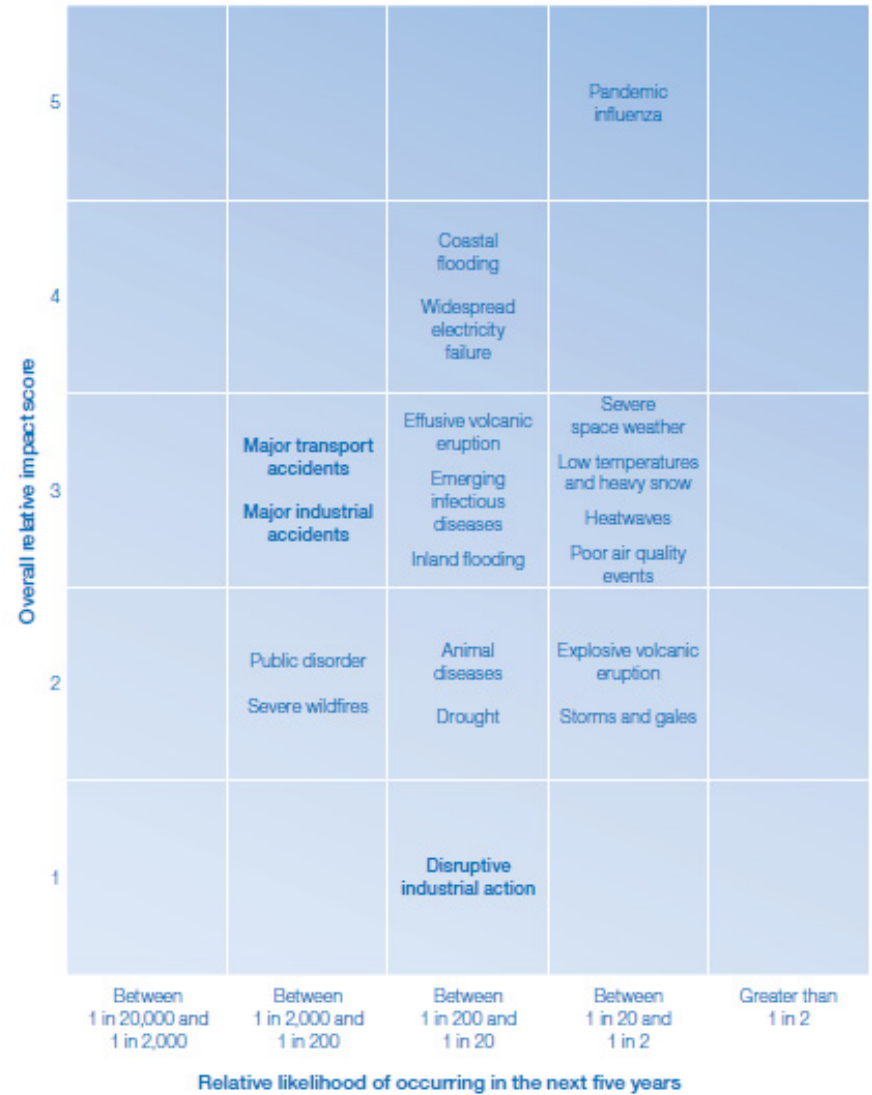
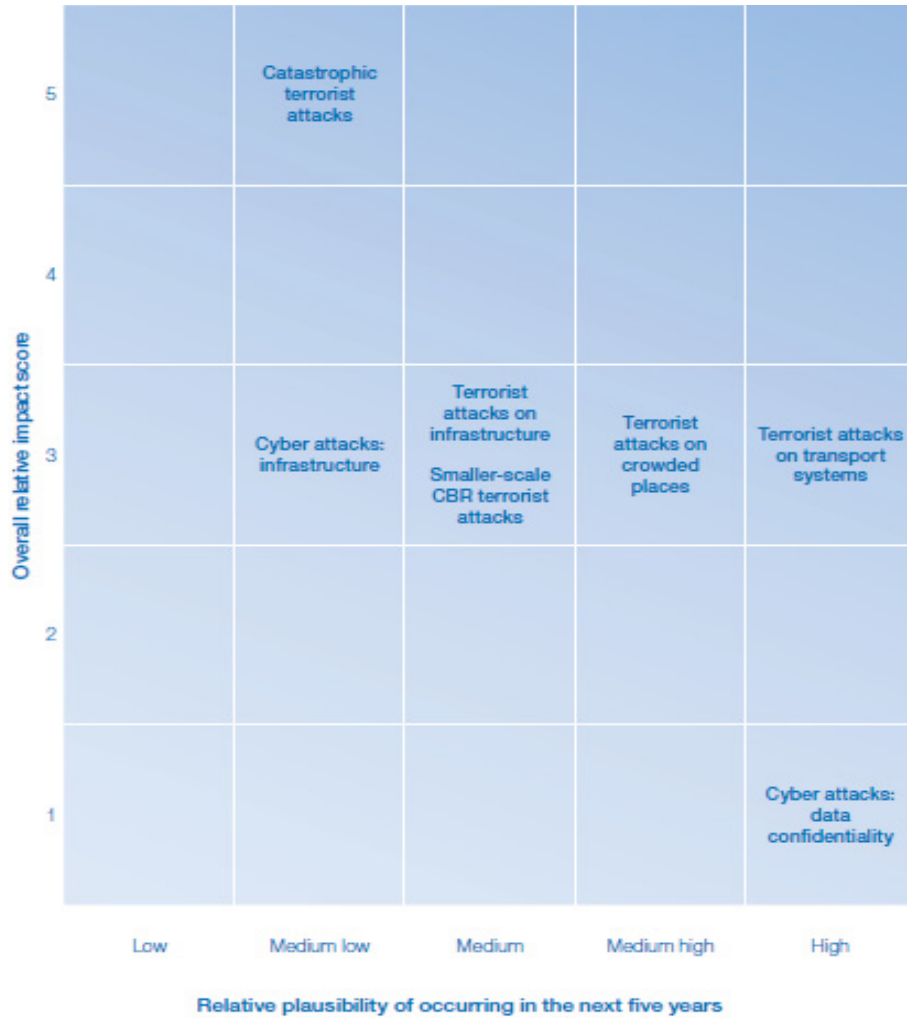
Figure 9 Estonia Risk Matrix<sup>31</sup>

These are referred to as Heat Maps, and they are visually appealing but present simplistic representations. It is noteworthy that most present equivalent scales for probability/likelihood and consequence/impact. Typically the aggregate or average risk ratings shown and compared are based on an equal weighting of impact criteria. Risk matrices provide an intuitively appealing visualization and ordering of risk evaluation.

The UK prefers to distinguish between hazards and threats and produce separate likelihood matrices rather than an integrated risk matrix (Figure 10).

<sup>31</sup> Organization for Economic Co-operation and Development. National Risk Assessment – Profiles of Selected OECD Countries, 2 December 2015, page 24.

Figure 10 UK Risk Likelihoods – Malicious Risks & Other Risks<sup>32</sup>



<sup>32</sup> U.K. Cabinet Office, National Risk Register of Civil Emergencies, 2015 edition, pg.10/11.

The Netherlands depict the results of their national risk assessment in terms of a likelihood versus consequence risk matrix but also include an indication of variability in the results (Figure 11).

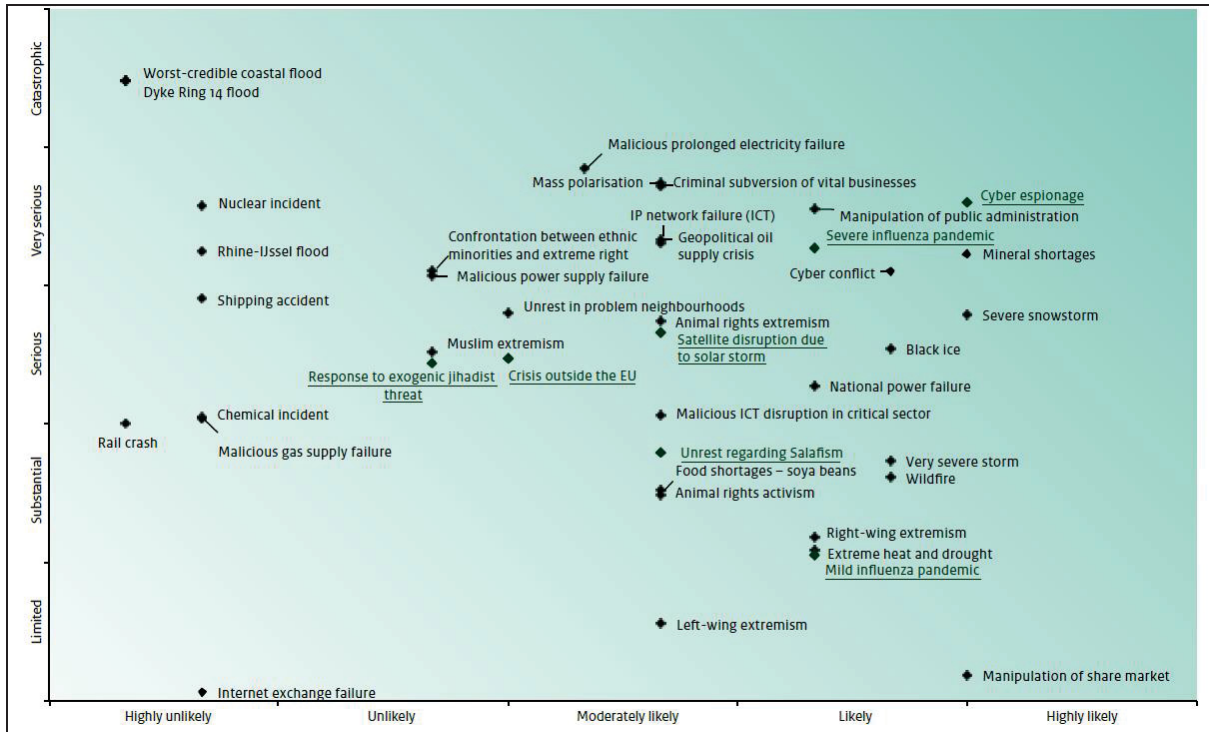


Figure 11 Dutch Risk Matrix<sup>33</sup>

Likelihood and Consequence can be broken down in more detail in separate graphs, e.g. Figure 12 and Figure 13 respectively.

<sup>33</sup> (Netherlands) Network of Analysts for National Security National Risk Assessment 2011, 2011, page 44, [file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011\\_tcm92-538995%20\(5\).pdf](file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011_tcm92-538995%20(5).pdf) accessed 24 March 2016.

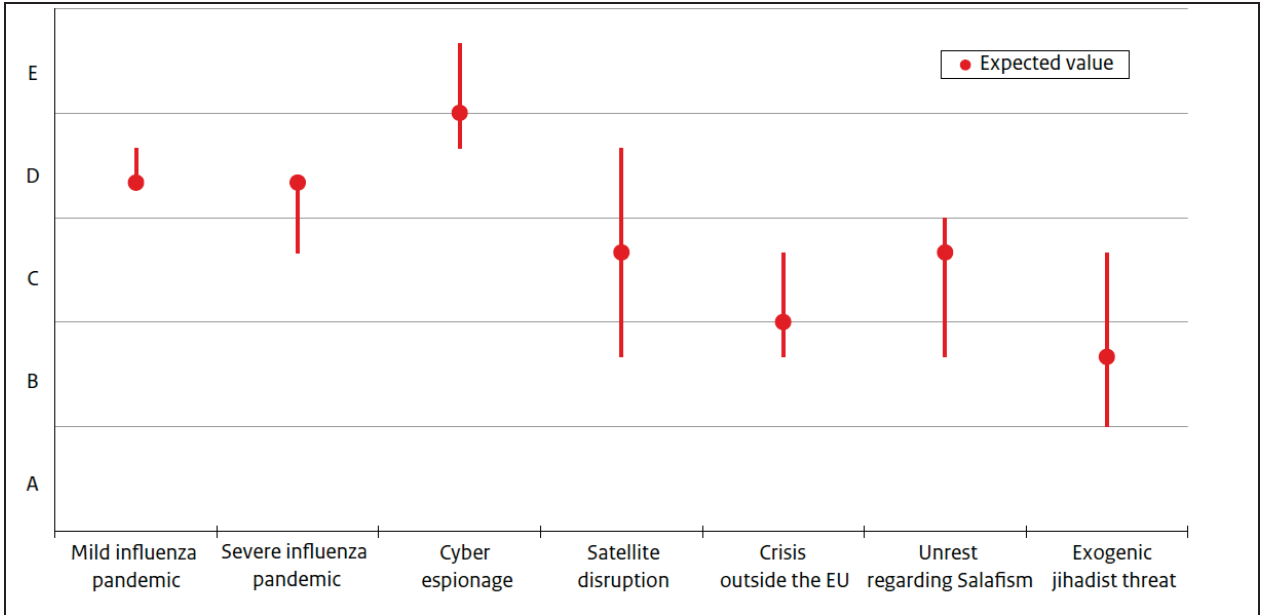


Figure 12 Netherlands – Upper and Lower Limits of Likelihood<sup>34</sup>

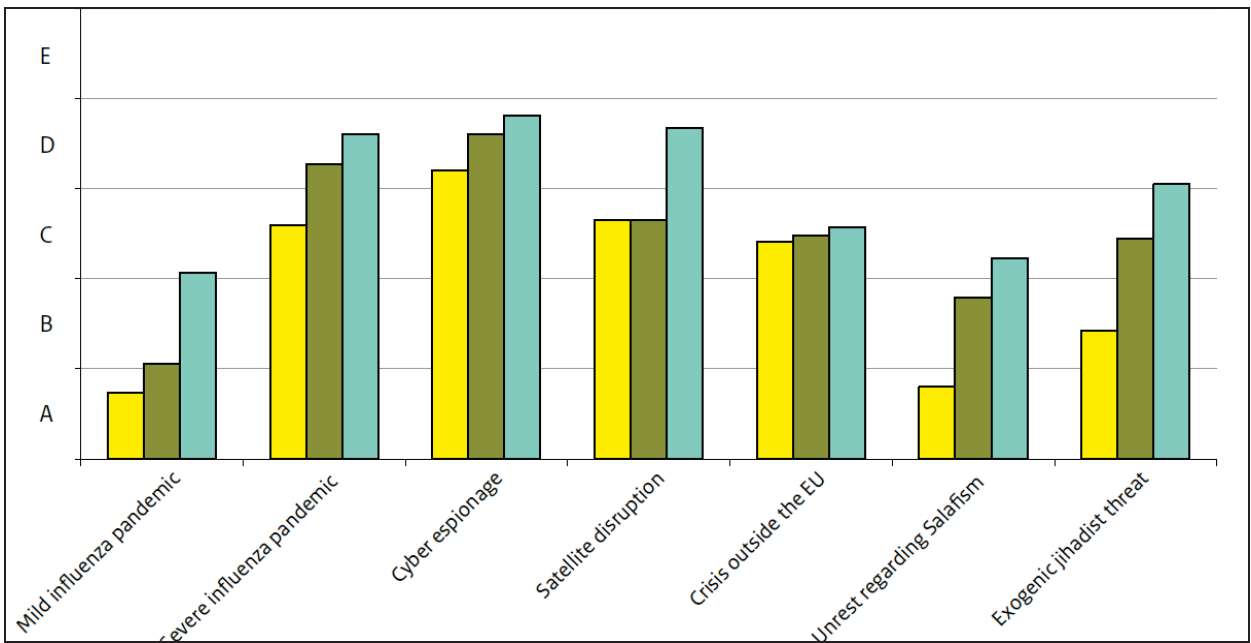


Figure 13 Netherlands – Upper and Lower Limits of Consequences<sup>35</sup>

<sup>34</sup> (Netherlands) Network of Analysts for National Security National Risk Assessment 2011, 2011, page 58, [file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011\\_tcm92-538995%20\(5\).pdf](file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011_tcm92-538995%20(5).pdf) accessed 24 March

Impact rating by criteria permits facilitates comparison between scenarios, frequently illustrated using bar charts. Illustrations from the Dutch and Norwegian National Risk profiles are shown below - Figure 14 and Figure 15 respectively.

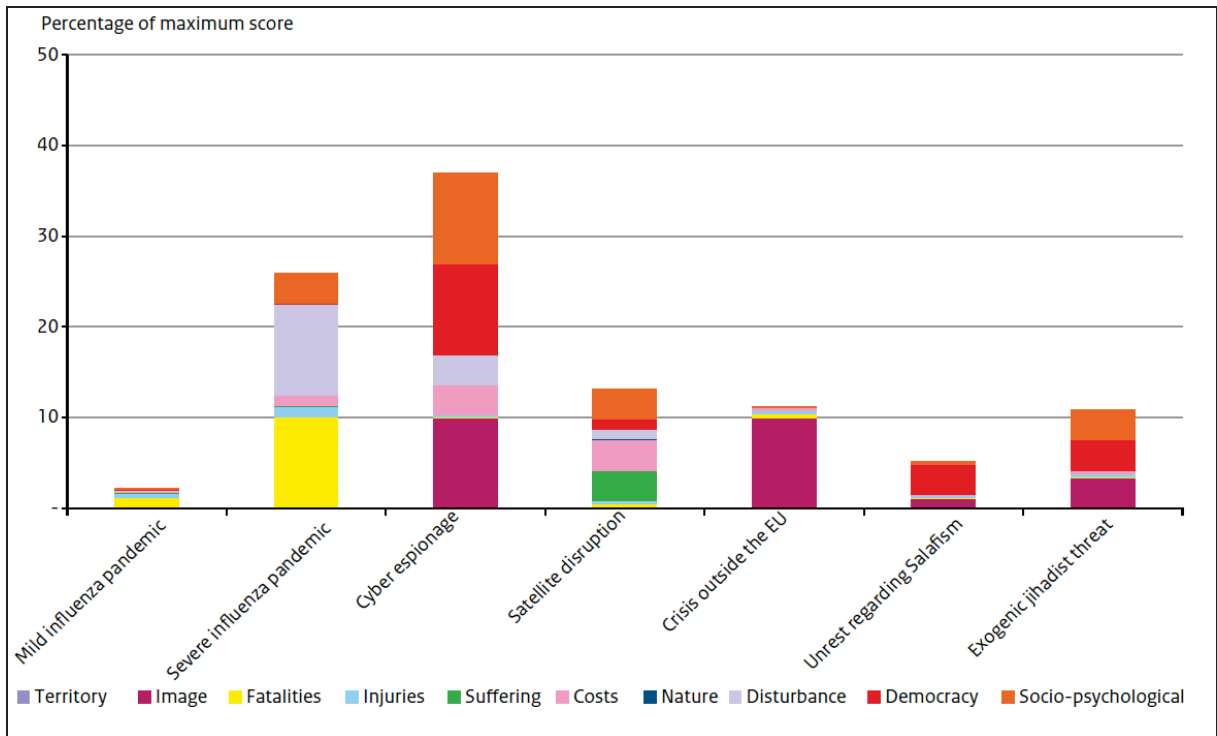


Figure 14 Netherlands Risk Ratings by Impact Criteria<sup>36</sup>

<sup>35</sup> (Netherlands) Network of Analysts for National Security National Risk Assessment 2011, 2011, page 59, [file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011\\_tcm92-538995%20\(5\).pdf](file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011_tcm92-538995%20(5).pdf) accessed 24 March

<sup>36</sup> (Netherlands) Network of Analysts for National Security National Risk Assessment 2011, page 46, [file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011\\_tcm92-538995%20\(5\).pdf](file:///C:/Users/DHatesConsulting/Downloads/national-risk-assessment-2011_tcm92-538995%20(5).pdf) accessed 24 March 2016.

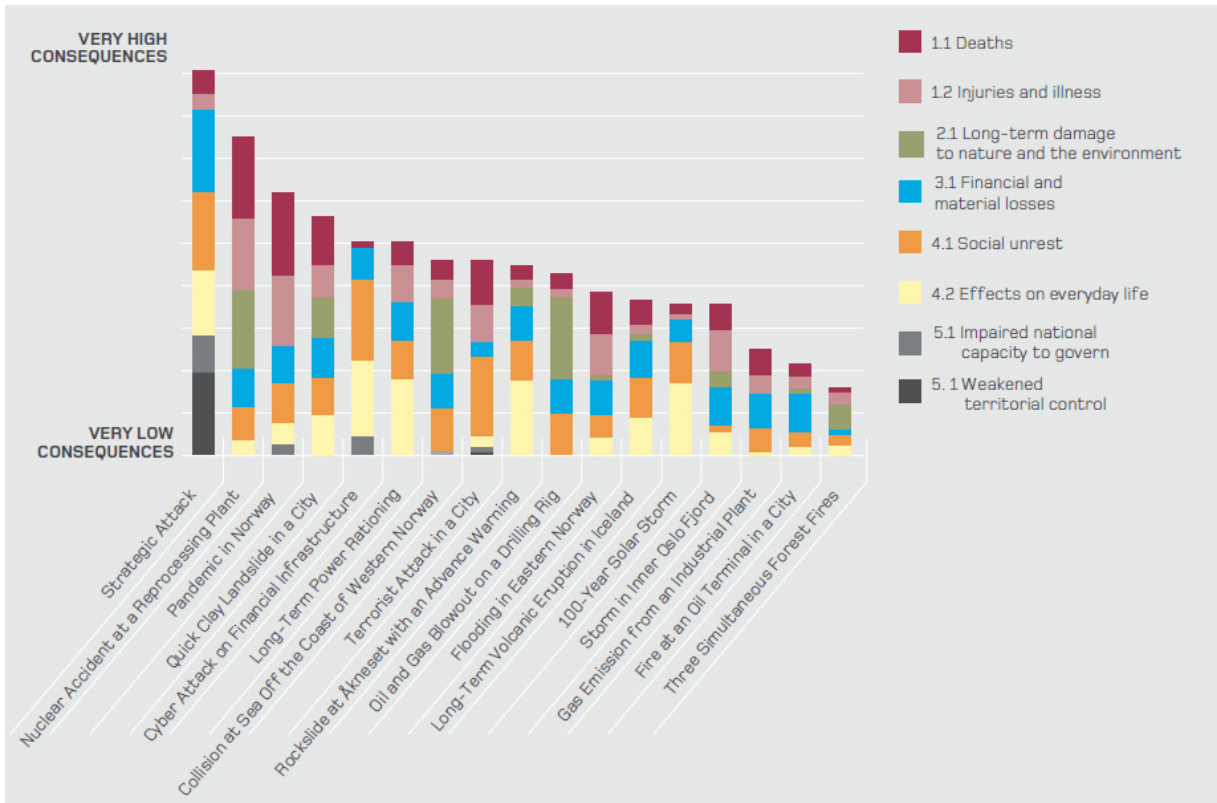


Figure 15 Norwegian Risk Ratings by Impact Category<sup>37</sup>

The Canadian AHRA has introduced the concept of iso-risk lines (equating impact and likelihood scores) and representing uncertainty as elliptical bubbles on a risk matrix.

<sup>37</sup> Norwegian Directorate for Civil Protection. 2013 National Risk Analysis, page 173, [http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB\\_2013\\_english.pdf](http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf) accessed 24 March 2016.

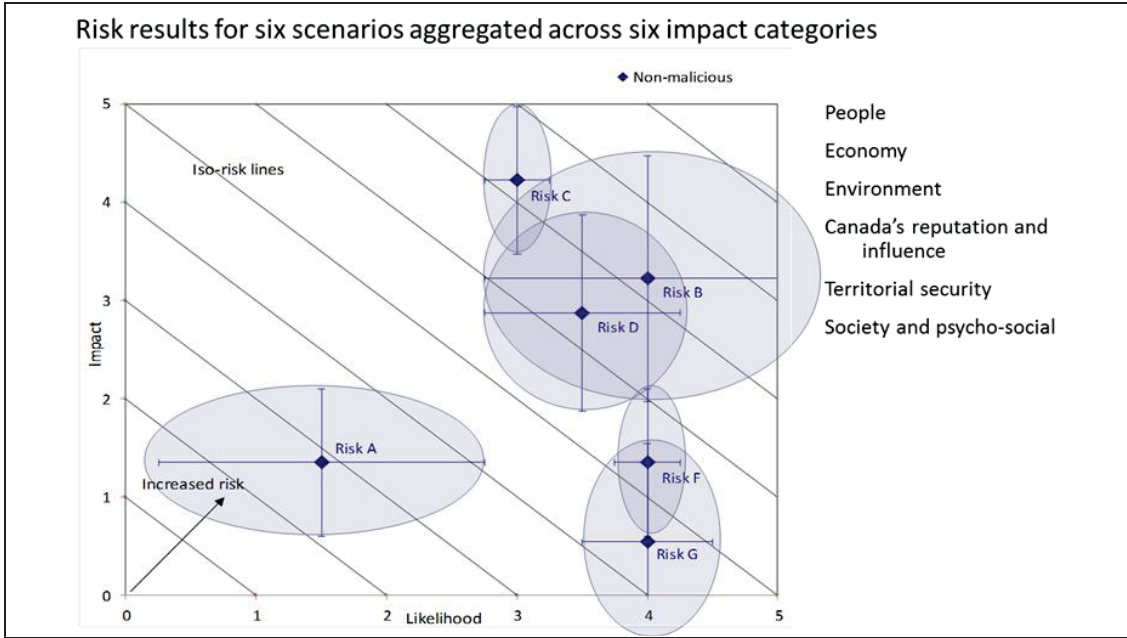


Figure 16 AHRA – Representation of Uncertainty

The Canadian All Hazard Risk Approach is the only methodology surveyed which has developed a customised tool, the Capability Assessment Management System (CAMS), for supporting capture and analysis of SME judgement. The CAMS application generates a dashboard (Figure 17) to facilitate analysis.

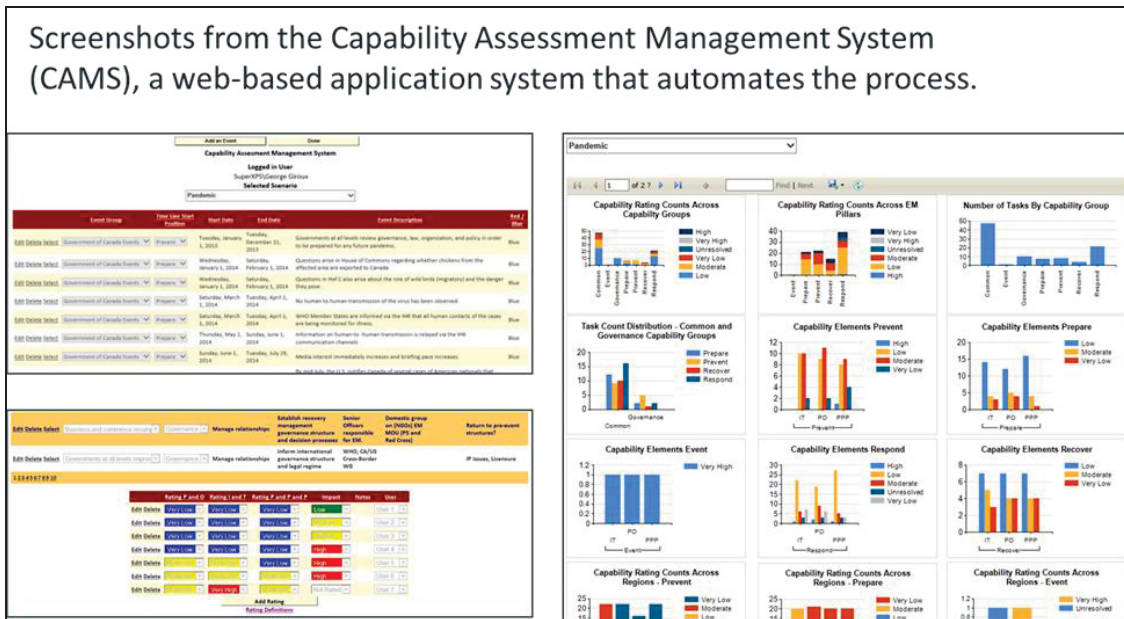


Figure 17 Capability Assessment Management System Dashboard



## Take Aways and Challenges

There are a number of emergent “best practices”/take aways relating to products and presentations:

- It is common practice to publish a national risk profile following a national risk assessment; some nations maintain separate classified risk registers;
- An accompanying narrative descriptions of priority/high risk scenarios provide a very useful venue for sharing planning assumptions;
- Aggregated/indicative comparisons of risk – typically illustrated using a “heat map” - are used to provide a visual reference and to raise awareness and promote prioritization and program alignment across silos;
- Nations are more comfortable relating comparative impact than likelihood particularly when it comes to malicious agents; and
- Data collection informs analysis and presentation. A breakdown by scenario and impact is useful in illustrating and defining the scope of the Health Portfolio’s involvement.

## 5. Country Case Studies

---

### The United States

The US does not publish a National Risk Profile as a matter of course. However, the Department of Homeland Security has taken the lead in developing a methodology and tools, and the advantages of prescribing a standardizing process are recognized:

All levels of government and the whole community should present and assess risk in a similar manner to provide a common understanding of the threats and hazards confronting our Nation. The information gathered during a risk assessment also enables a prioritization of preparedness efforts and an ability to identify our capability requirements across the whole community.<sup>38</sup>

Presidential Policy Directive/PPD-8 National Preparedness issued in March 2011 was aimed at strengthening the security and resilience of the US through systematic preparation for the threats. This included establishment of measurable preparedness priorities and targets. A Strategic National Risk Assessment (SNRA) was subsequently conducted:

- To identify high risk factors that supported development of the core capabilities and capability targets in the National Preparedness Goal;
- To support the development of collaborative thinking about strategic needs across prevention, protection, mitigation, response, and recovery requirements, and
- To promote the ability for all levels of Government to share common understanding and awareness of National threats and hazards and resulting risks so that they are ready to act and can do so independently but collaboratively.<sup>39</sup>

The results were classified; however, an overview of the unclassified findings was published several months later and is available online. The focus was on ‘cross-cutting’ risks which spanned critical infrastructure sectors and were deemed to pose a national risk. The risk assessment process was not described in detail but risk taxonomies and impact criteria are similar to those used by the other countries surveyed. The taxonomy grouping used to support the 2011 National Risk Profile included (1) naturally occurring risks; (2) unintentionally introduced manmade risks); and (3) intentionally introduced manmade risks.<sup>40</sup> The assessment relied on quantitative estimates of frequency and consequences where available and augmented this with qualitative assessments. Of note, the US SNRA identified thresholds for defining what constituted a

---

<sup>38</sup> DHS, National Preparedness Goal, Second Edition, September 2015, page 4, [http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National\\_Preparedness\\_Goal\\_2nd\\_Edition.pdf](http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf) accessed 27 January 2016.

<sup>39</sup> DHS Strategic National Risk Assessment December 2011 <http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf> accessed 27 January 2016.

<sup>40</sup> U.S. Department of Homeland Security (Homeland Infrastructure Threat and Risk Analysis Centre). 2011 National Risk Profile, July 2011, page 4, <https://info.publicintelligence.net/DHS-NationalRiskProfile2011.pdf> accessed 18 May 2016.

**national** emergency and was explicit in defining scope i.e. the SNRA focused on contingency events with defined beginning and endpoints and excluded societal trends and persistent *steady state* risks such as chronic disease, illegal immigration and drug trafficking.

DHS has adopted and endorsed a capability-based approach. In November 2011 an inaugural *National Preparedness System* was introduced outlining a set of core capabilities. In August 2013 a *Threat and Hazard Risk Identification and Risk Assessment Guide* was published. It advises that communities should focus on threats and hazards that are likely and that pose a significant threat and suggests but not prescribe impact criteria (e.g. size of geographic area, number of displaced households, number of fatalities, number of injuries/illnesses, disruption to critical infrastructure, intelligence requirements and needs, amount of direct economic impacts, and economic effects of supply chain disruption) or provide scales. It is interesting to observe, in passing, that the impact on people distinguishes between deaths, injuries and illnesses and that the impact on the economy distinguishes between direct and indirect effects. This is also the only risk assessment methodology that advocates using intelligence requirements as an impact criteria. Steps 3 and 4 provide linkage to capability assessment and involve articulating desired outcomes and establishing capability targets. These capability targets are described using the core capability inventory.

DHS is mandated to conduct a *Homeland Security Review* every 4 years; the first was published in February 2010 and the second in June 2014<sup>41</sup>. Descriptions of the threats which shaped the findings and assessments of organizational alignment and preparedness are included. The quadrennial reviews can be likened in part to Canadian Reports on Plans and Priorities (RPP). The 2014 Quadrennial Homeland Security Review identified six drivers of change and six challenges which pose strategic risk over the next five years. The former included the evolving terrorist threat, increasing reliance on information and communications technologies and inherent dangers in treating critical infrastructure as discrete, physical assets. The drivers and challenges are related to DHS missions and the review focuses on risk treatment and prevention programs and mitigation measures. It is noteworthy that bioterrorism and rising anti-viral and antibacterial resistance were identified as a challenges and the review concluded that a devastating pandemic remains the highest homeland security risk.

It is difficult to draw direct comparisons and conclusions from a survey of US practices. Still, some observations and take-aways can be drawn:

- Risk assessment is embedded in national/DHS planning and recognized as an essential corollary to risk treatment. The quadrennial review links risks to programs. Likely in part for security reasons it does not describe the risk assessment process and evaluation criteria ;
- Risk assessment can be tailored for use. A simplified four step process (described in the *Threat and Hazard Risk Identification and Risk Assessment Guide*) has been developed for community use. The benefits, chiefly ease of use, must be weighed against the rigor and consistency a more detailed and demanding approach offer; and
- Core capabilities have been defined to serve as an integrating framework – arguably an alternative to a more structure risk assessment methodology. The original and exhaustive

---

<sup>41</sup> US Department of Homeland Security. The 2014 Quadrennial Homeland Security Review, June 2014 <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf> accessed 17 February 2016.

Target Capability List (TCL)<sup>42</sup> (588 pages) published as a companion to the National Preparedness Guidelines has been pared down to foster adoption and broaden use.

## The Canadian All Hazard Risk Approach

A Federal AHRA methodology was developed in 2010 to standardize assessment methodology, support federal departments/agencies in fulfilling their legislative responsibility to conduct risk assessments and inform emergency management planning. The AHRA guide observed that the ownership of risks is often shared and spans ministerial mandates; hence, a common framework and consistent approach is required to assess and manage risks effectively. During three successive annual cycles (2010-2013,) twenty-five departments/agencies including Health Canada (HC) and the Public Health Agency of Canada (PHAC) participated and twenty six scenarios were assessed. Efforts were suspended after 2013. In 2015 Defence Research & Development Canada (DRDC)'s Centre for Security Science (CSS) approved a project to advance. For its part Public Safety Canada (PS) is considering refreshing the AHRA and developing a National Risk Profile.

The AHRA reflects many of the best practices discussed, and outlines 5 steps (Figure 18) based on ISO 31000.

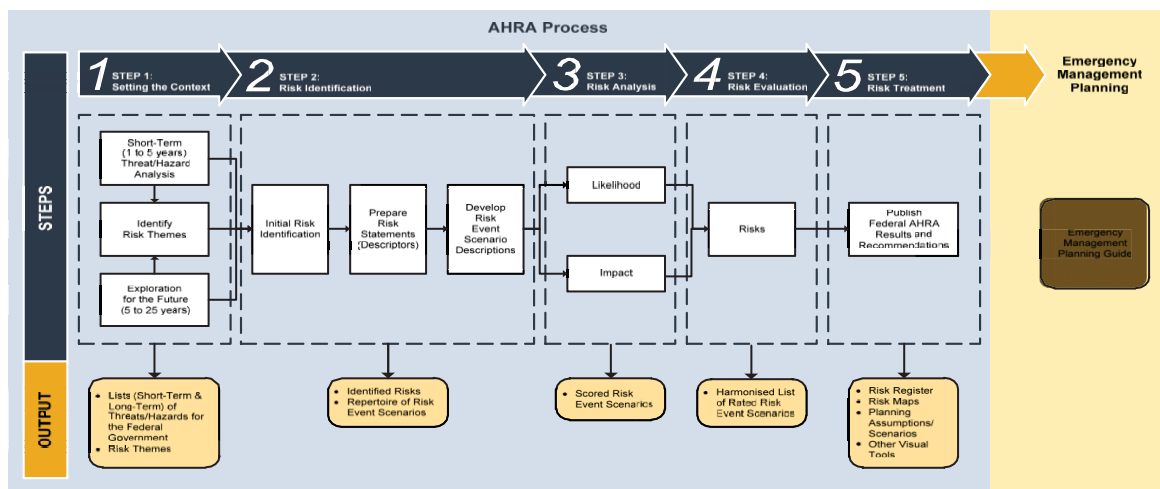


Figure 18 Canadian All Hazards Risk Approach

There are sound arguments for leveraging the AHRA model. However, it is likely overambitious and overelaborate to adopt/“operationalize” without modification. Notably an annual cycle was intended linked to the Government of Canada (GC)’s fiscal year (FY) and programmatic activities (Figure 19). In the event, resource constraints led to suspension after a pilot and two cycles.

<sup>42</sup> U.S. Department of Homeland Security. Target Capabilities List, September 2007 <http://www.fema.gov/pdf/government/training/tcl.pdf> accessed 17 February 2016

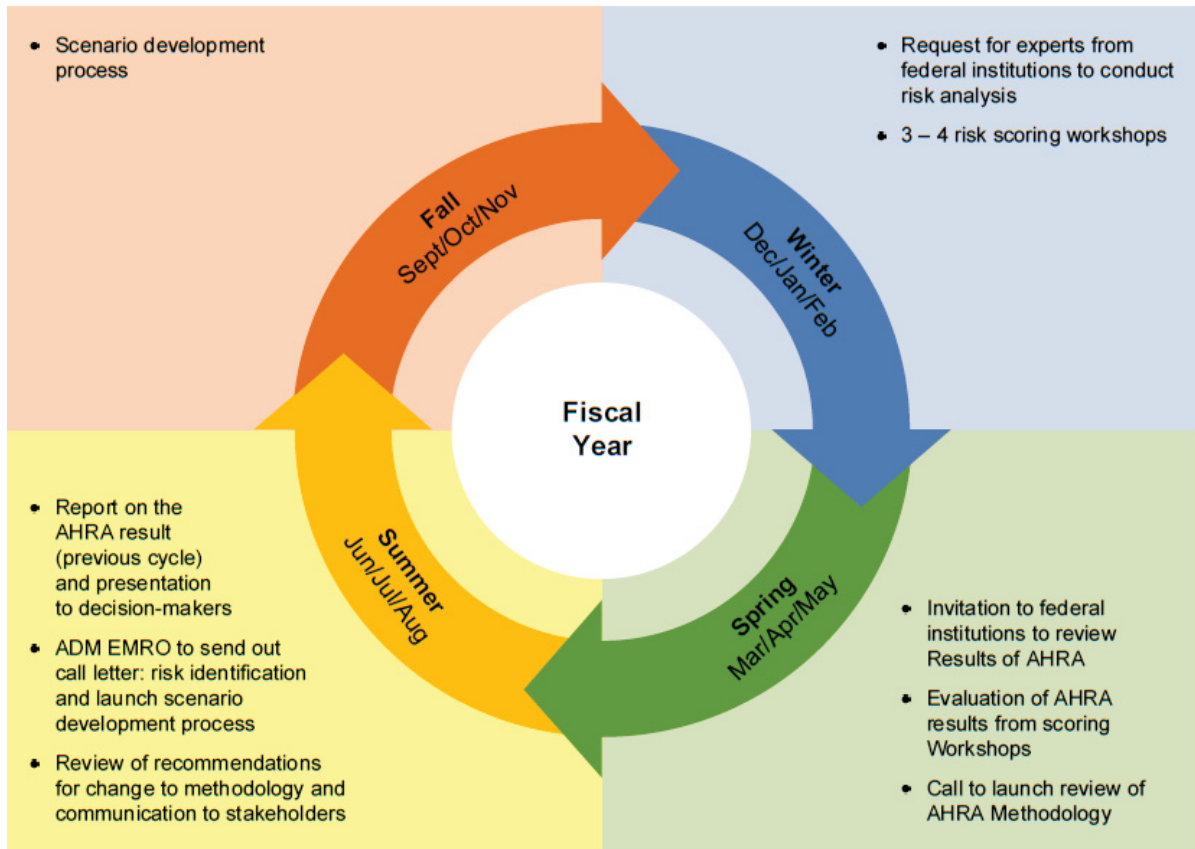


Figure 19 AHRA Business Cycle

The AHRA also initially attempted to integrate two threat horizons: 1-5 years and 5-25 years. This proved difficult and, in the event, the focus was restricted to a 1-5 year threat horizon. At best it would be challenging to address two horizons simultaneously. Arguably foresight is a science in its own right. In the event, best practices suggest that there are advantages to distinguishing near term risk assessments from longer term foresight activities.

Best practices suggest that institutionalization entails the establishment of a core staff to oversee documentation, administration and analysis – particularly if an annual cycle is intended. Often the results are presented to national cabinets. A senior level, cross government oversight and approval process assures appropriate priority and lends authority to the assessment. An *Interdepartmental Risk Assessment Working Group* oversaw conduct of the AHRA. The process was never institutionalized nor embedded in decision cycles/processes.

The focus of the AHRA was on national risks facing the Federal Government, driven in part by the mandated responsibility for departments and agencies to conduct risk assessments as a basis for emergency planning. Risk scenarios were proposed and prepared by Lead Departments. Stakeholders participated in *Risk Analysis*; PS and CSS developed a multi-criteria decision support tool for capturing and consolidating SME ratings. The Capability Assessment Management System (CAMS) characterizes scenarios, catalogues tasks, automates capture and consolidation of AHRA ratings by SMEs and generates production of heat maps and graphs.

Scenario details, capability frameworks and task inventories and voter lists can be easily entered. The Global Health Security Initiative (GHSI) considered using CAMS to support its January 2014 Face-to-Face meeting to assess core capabilities.<sup>43</sup> In the event, there proved to be insufficient preparatory time to develop an overarching framework and familiarize participants with the tool. CAMS has subsequently been enhanced and is now capable of supporting distributed (off-site) voting. It could be used to support Health Portfolio risk and capability assessments and will be trialed as part of the pilot assessments. Information Technology (IT) support could prove a concern going forward. The tool has been developed by CSS through a series of contracts. It is not well documented and CAMS is hosted on the contractor's server.

The AHRA Risk Taxonomy scheme (Figure 20) reflects best practices, differentiating between non malicious (natural causes and accidents) and malicious (criminal and state-sponsored) threats. It is noteworthy that, unlike most other schemas, after feedback following the 2011 Health Portfolio Risk Assessment, the AHRA segregates health related hazards.

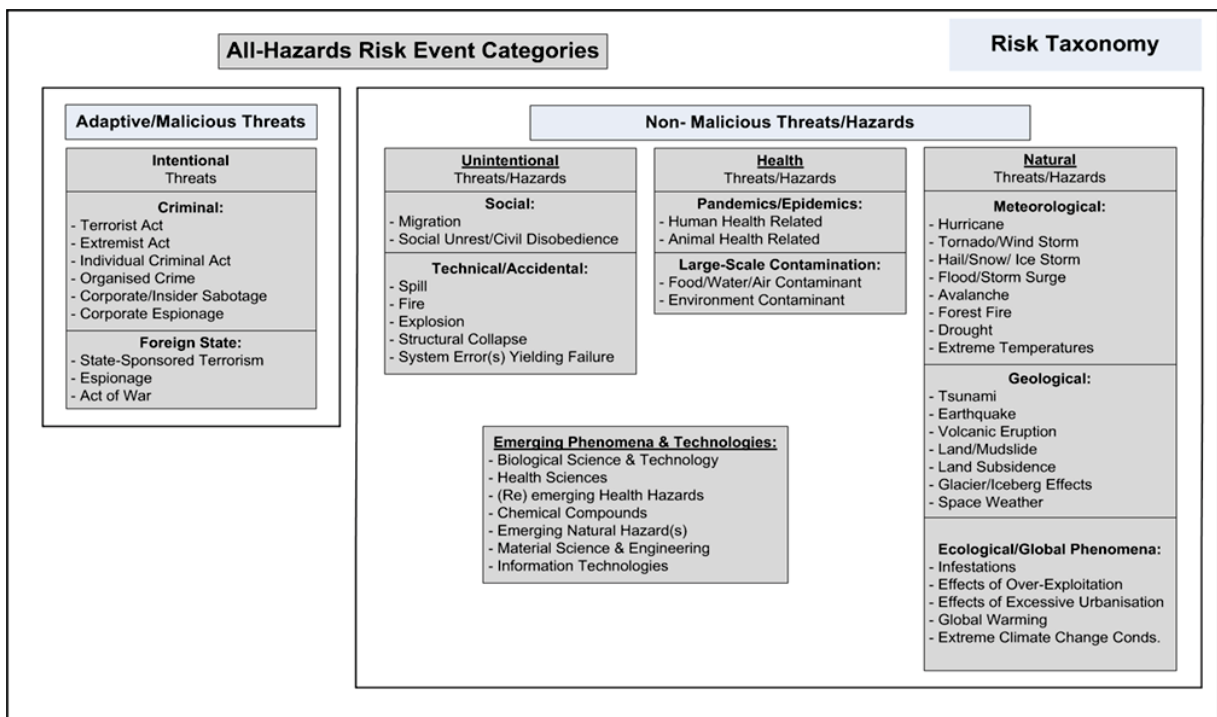


Figure 20 AHRA Risk Taxonomy

The AHRA impact assessment criteria reflect, for the most part, emergent best practices. Six categories are identified (Figure 21). In practice; however, it has proven challenging to evaluate threats to Territorial Security, Canada's Reputation & Influence and Society and Psycho/Social Equilibrium. Increasingly threats permeate borders and jurisdictional boundaries and territorial security is primarily a federal concern for a few departments. Secondly, it is difficult to agree and isolate causal relationships and to identify meaningful indicators for all reputational and societal

<sup>43</sup> Hales, Douglas R and Shaye K. Friesen. Capability Assessment Management System Support to the Global Health Security Initiative (GHSI) Face-to-Face Meeting, DRDC-RDDC-2014-L24, 4 March 2014.

impacts. Consequently, in practice, analysis has focused on “the three more ‘robust’ impact categories (People, Economy and Environment)”<sup>44</sup>.

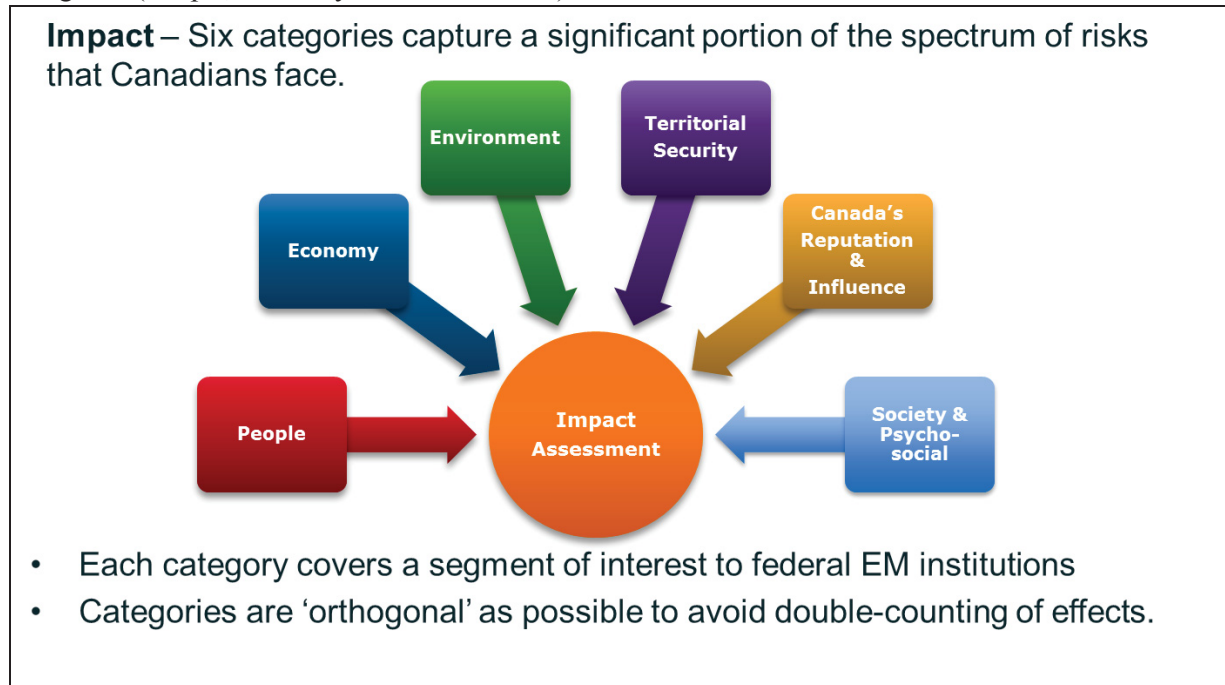


Figure 21 AHRA Impact Criteria

A survey of best practices confirms that all nations include the safety and well-being of People as a criterion in assessing the impact risk events might initiate. Typically this is calculated in terms of fatalities, illnesses and injuries. Longer term and mental health concerns are both more difficult to forecast and less well handled. Based on Health Portfolio advice, the AHRA uses *Disability-Adjusted Life Years (DALY)* and employs the *Number of Adult Fatalities* to assess the impact on People. Based on Health Portfolio advice, the AHRA uses *Disability-Adjusted Life Years (DALY)* and employs the *Number of Adult Fatalities* to assess the impact on People. Emergencies/disasters cause perturbations in economic systems. Assessing the costs is not straight forward. The direct costs – the immediate and tangible consequences of damage and destruction to physical assets – are more apparent and easily calculated than those associated with productivity disruption and “non-market losses”

Non-market direct losses include all damages that cannot be repaired or replaced through purchases on a market. For them, there is no easily observed price that can be used to estimate losses. This is the case, among others for health impacts, loss of lives, natural asset damages and ecosystem losses, and damages to historical and cultural assets. Sometimes, a price for non-market impacts can be

<sup>44</sup> Simona Verga and Shaye Friesen. Federal All Hazards Risk Assessment (AHRA) – Analysis of Scenario Results. DRDC-RDDC-2014-L310, 17 December 2014, page 1.

built using indirect methods, but these estimates are rarely consensual (e.g. the statistical value of human life).<sup>45</sup>

Indirect costs are even more difficult to estimate; they span longer time horizons and impact a larger geographic area and other economic sectors.

The magnitude of the response, extent (geographic scale, forfeiture of biodiversity/loss of species, and duration of disruptions) are used in assessing environmental impact. The magnitude of response, defined by the AHRA in jurisdictional terms (local, multi-regional, multi-jurisdictional, national & international) attempts to capture the degree of organizational complexity. Its value in assessing environmental impact deserves questioning.

Territorial Security is not applicable as a generic criterion i.e. useful in informing subordinate risk assessments and, despite accompanying work ladders; it has proven challenging to apply Reputation & Influence and Social & Psycho-Social meaningful. Reputation & Influence is used to assess external reaction to an incident and Society and Psycho-Social to assess the (often transient) public mood. There are contributing factors which can't be easily isolated and, hence, assessments are very subjective. The UK has experienced similar issues trying to anticipate and quantify public anxiety. Projects using the AHRA often discount these three criteria.

Most countries have opted for a 5 point Richter scale for assessing Impact. The AHRA uses a 10 point scale i.e. 1-5 with 0.5 intervals and the rating schema used by the AHRA may be over elaborate. The likelihood for maliciously triggered incidents provides for separate assessments of technical feasibility, enabling capabilities and intent.

The AHRA notes the importance of Risk Treatment and lists options (risk avoidance/risk transfer, risk acceptance, and risk mitigation through reducing likelihood and/or consequence) by, in keeping with other countries' practices does not provide much direction – beyond awareness - on best practices for coordinating treatment of co-shared risks.

## 2011 Health Portfolio Risk Assessment

A Health Portfolio Risk Assessment was conducted in the fall of 2011. The results were attached as an appendix to the Health Portfolio Strategic Emergency Management Plan. An evaluation was conducted via survey following the assessment. Participants were asked to indicate agreement or disagreement with a number of statements using a scale from 1-5 and 12 responses. Given the participation level the results are considered informative/indicative rather than definitive. Of note:

- Most responders were supportive of the process but hesitant to agree that the results had informed other processes. *In many cases there is an organizational/accountability "seam" between risk assessment and treatment which poses challenges. This may be particularly true in the case of the Health Portfolio in which responsibilities are distributed between Health Canada and the Public Health Agency and between levels of government;*

---

<sup>45</sup> Stephane Hallegatte and Valentin Przyluski. The Economics of Natural Disaster: Concepts and Methods, The World Bank, Policy Research Paper 5507, December 2010, page 3, <http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5507> accessed 14 March 2016.



- The need and a desire to both align with and adapt the broader Federal Government/Public Safety’s methodology were recognized. *A refreshed Health Portfolio Risk Assessment process should acknowledge/accommodate this;*
- Most responders felt that a *Health Portfolio Risk Assessment* should include malicious threats, and consider including longer term horizons and providing for additional risk drivers e.g. regional variations and special populations;
- Most responders felt the structured elicitation methodology adopted which seeks consensus is appropriate. It was noted in some cases limited data was available to support assessments and that “consensus” sometimes reverted to defaulting to the judgement of subject matter experts i.e. the view of one carried more weight. *This underscores the need – particularly in the absence of data – to ensure broad SME representation and provide for capture and review of outliers. Automated systems such as CSS’ Capability Assessment Management System (CAMS) both ensure that all “voices” are heard and allow for distinguishing (and weighing as part of sensitivity analysis) judgments from different communities/fields;*
- Respondents felt that the extensions to the AHRA 2011 Risk Taxonomy were somewhat useful. *Minor modifications were made to the 2012/13 AHRA Risk Taxonomy.*
- One respondent suggested that there was a need for a more objective selection of scenarios to avoid bias and felt that consequence assessment dominated. *The AHRA used a small number of full scenarios as opposed to the Health Portfolio’s use of a larger number of shorter vignettes. Care needs to be taken in selecting vignettes/scenarios to ensure the full range of credible high consequence hazards and risk are represented;*
- It was felt that risk vignettes provided sufficient detail for this first assessment but there was no consensus on whether more detailed scenarios and a focus on higher order risk themes offered a preferable approach. *Best practices would appear to support a two pass approach using vignettes to identify and order risks and full scenarios to support options analysis risk treatment;*
- Point estimates of likelihood and impact were used. It was felt that this was appropriate for a first assessment but future assessments should provide for ranges/distributions; and
- Malicious Capability, Technical Feasibility and Intent ratings were not included as part of the risk assessment process alleviating the requirement to classify the results. A majority of survey participants expressed strong support for continuing this practice. A minority suggested inclusion was “worth the effort”.
- The impact criteria considered were restricted to Deaths, Illnesses/Injuries and Displacement. While these were considered adequate for the initial assessment, most responders felt including a psych-social component would add value;
- A majority of respondents felt that a *Confidence* rating should be captured and the scale used was suitable;
- Responders felt the presentation accurately reflected both the assessment and risk environment but also identified the issues involved in amalgamating unintentional and intentional results.<sup>46</sup>

The 2011 Health Portfolio Risk Assessment provided an opportunity to adapt and apply the All Hazard Risk Approach methodology. It provided useful recommendations to consider in

---

<sup>46</sup> Evaluation of the 2011 Health Portfolio Public Emergency Risk Assessment Process.

operationalizing and institutionalizing a Health Portfolio Risk Assessment methodology and it identified a number of issues which should be addressed.

## Risk Treatment

It is one thing to note risk, another to manage them in the sense of accepting risk or taking measures to mitigate risk. The Norwegian “bow tie” model (Figure 22) offers a useful reminder that the latter can include measures to reduce the likelihood of risks events and/or measures to reduce the impact of risk events.

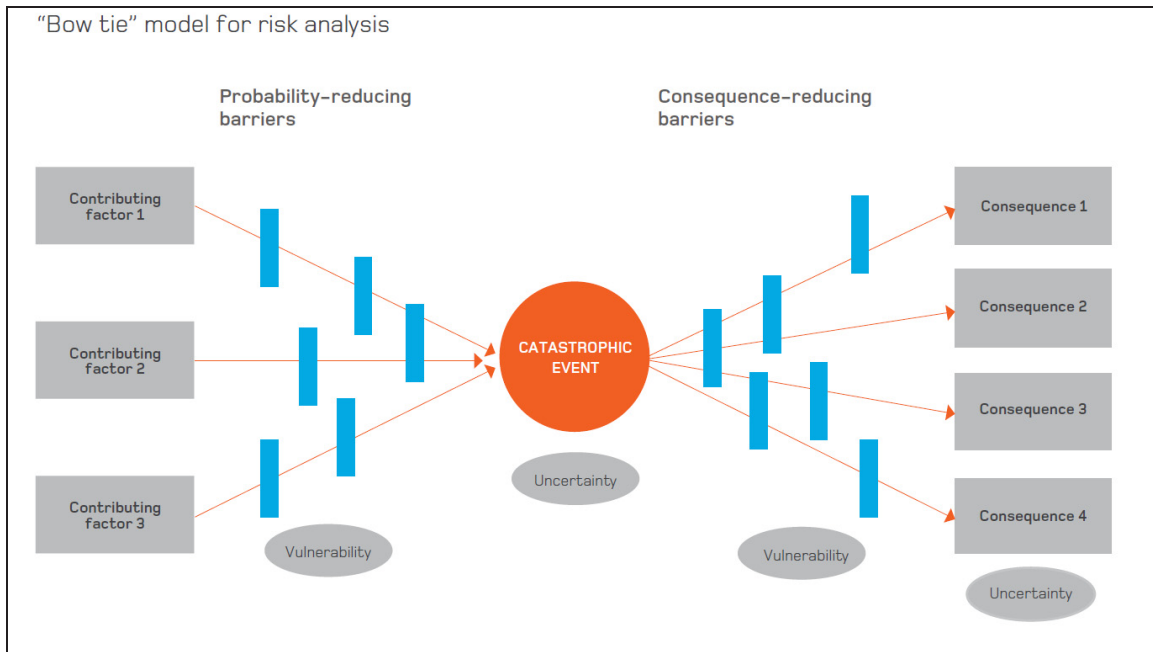


Figure 22 Norwegian “Bow Tie” Model<sup>47</sup>

<sup>47</sup> Norwegian Directorate for Civil Protection. 2013 National Risk Analysis, page 17, [http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB\\_2013\\_english.pdf](http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf) accessed 24 March 2016.

The Australia National Emergency Risk Assessment Guidelines (NERAG) is unique in proposing evaluation criteria and a scale for assessing risk control measures (Table 7).

*Table 8 Australian Control Measures Indicators & Scale.*

Level	Control strength	Control expediency
High	Control is highly effective in reducing the level of risk	The control is frequently applied. A procedure to apply the control is well understood and resourced. The cost of applying the control is within current resources and budgets.
Medium	Control is effective in reducing the level of risk	The control is infrequently applied and is outside of the operators' everyday experience. The use of the control has been foreseen and plans for its application have been prepared and tested. Some extraordinary cost may be required to apply the control.
Low	Control has some effect in reducing the level of risk	The control is applied rarely and operators may not have experience using it. The use of the control may have been foreseen and plans for its application may have been considered, but it is not part of normal operational protocols and has not been tested. Extraordinary cost is required to apply the control, which may be difficult to obtain.
Very low	Control has almost no effect in reducing the level of risk	Application of the control is outside of the experience and planning of operators, with no effective procedures or plans for its operation. It has not been foreseen that the control will ever need to be used. The application of the control requires significant cost over and above existing resources, and the cost will most likely be objected to by a number of stakeholders.

Figure 23, from the Netherlands National Safety and Security Strategy provides a useful presentation of the link between Risk Assessment and Risk Management, and hints at the role Capability Analysis could play in describing gaps and supporting options analysis.

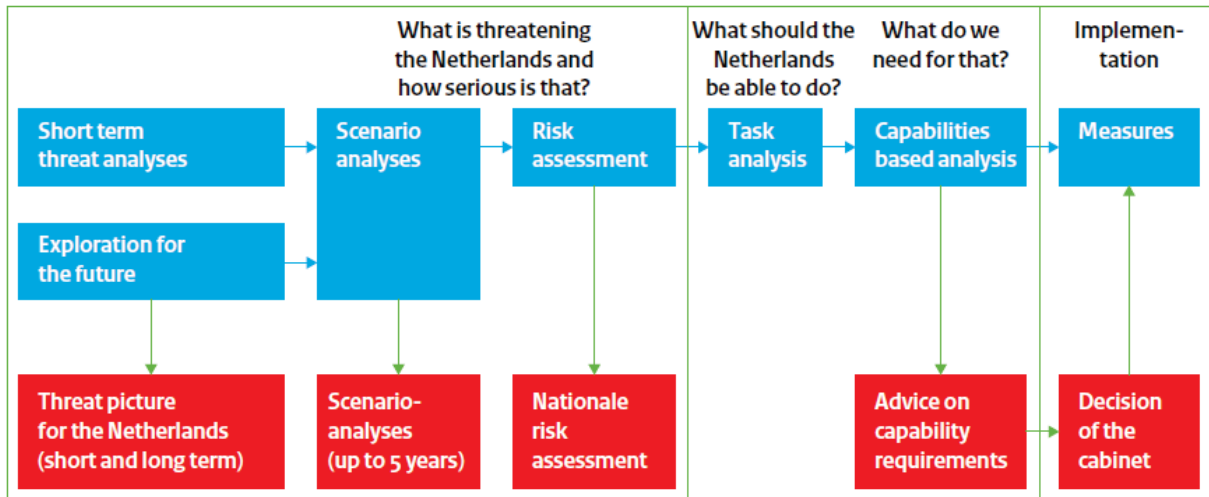


Figure 23 Netherlands National Safety & Security Strategy<sup>48</sup>

## Capability Based Planning

Capability Based Planning (CBP) was introduced in the 1990s to address the inherent ambiguity in the post-Cold War security circumstances; an environment that has been characterized as volatile and uncertain. Threat based, single point-in-time scenario solutions were inadequate if only because the pace of political and technological change was outstripping the ability of staffs to keep up. A “new” planning framework was needed: emphasis was placed on delivering “capabilities” to address a widening range of risks.

“Threat-based planning focused on point/individual scenarios. “The core idea of the CBP approach is to confront rather than discount uncertainty”.

A capability is commonly defined as the means to accomplish a mission or function and achieve desired outcomes by performing essential tasks under specified conditions to targeted levels of performance. CBP is planning, under uncertainty, to build capabilities suitable for a wide range of threats and hazards, while working within an economic framework that requires choice. It is an approach to emergency preparedness planning that focuses on managing results while considering needs and costs. It provides for a functional analysis of operational requirements, i.e. it identifies and characterizes the capability demands necessary to respond to a broad range of circumstances and challenges, and it is an approach intended to support (not supplant) decisions and to inform the development of operational and investment plans through the apportionment of risk.

CBP principles can be exploited to support an all-hazards approach to Health Portfolio preparedness by identifying and developing capabilities that are applicable to a wider, less-specific range of threats and hazards.<sup>49</sup>

<sup>48</sup> Ministry of Security and Justice. Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands, page 12, [http://www.preventionweb.net/files/26422\\_guidancemethodologynationalsafetyan.pdf](http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf) accessed 21 December 2015.

To facilitate synthesis and collaboration analysis a common logic model should be accepted and a co-joined taxonomy adopted to ensure definitional consistency.

The CBP process starts with formulation of what must be accomplished in order to meet strategic objectives and then proceeds to the development of a range of solutions to meet those objectives. Next potential solutions are evaluated in a broadly framed security environment using multiple scenarios and, perhaps more importantly, parametric exploration of numerous cases within each scenario.

Scenarios are a central component of CBP. They provide context and a means to share assumptions. Multiple plausible and illustrative scenarios should be used to hedge against uncertainty and to test concepts and compare options i.e. organizational structures, critical business processes and supporting systems.

Gaps and requirements, and sometimes even plans, should be descriptive not prescriptive i.e. framed in terms of system of “solution agnostic” functional services linked if possible to conditions and performance standards.

### ***Exercise Perseverance (June 2013)***

A Table Top Exercise (TTX)/pilot was held in Ottawa in June 2013. The objectives of Exercise Perseverance were twofold: to trial capability assessment and to solicit subject matter expertise to identify capability requirements and gaps relating to the Health Portfolio (HP). In preparation for the TTX, a methodological approach was agreed upon and a *Users' Guide* was drafted and distributed. The approach was based on a Strategy-to-Task, Mission/Function/Task decomposition. A capability framework based on the Government of Canada (GC) Emergency Management (EM) pillars was employed and a task library drawn from the Target Capability List – Canada (TCL-C), existing plans, and recent lesson learned reports was generated. A full-spectrum scenario was developed to provide context and invoke capability requirements and, to facilitate assessment and to seed the discussion, observations from some previous after-action reports were related to HP capabilities and tasks. The scenario was parsed into Prevent, Prepare, Respond and Recover segments, corresponding to the four EM pillars. At the end of each segment, an examination of setting, identification of triggers and discussion of illustrative tasks was conducted. Participants were then invited to individually complete an assessment of HP tasks and asked to record comments explaining their rationale. Worksheets were collected, individual assessments collated, and ‘scorecards’ generated using a Green/Yellow/Red stoplight rating scale. Although neither validated nor definitive, the results were instructive and insightful. While there are some areas of variance; in general, there was a broad consensus among the HP representatives who took part. The preponderance of capabilities was assessed to be adequate (rated Green).<sup>50</sup> However, a number of concerns (rated Yellow) were noted and the findings documented.<sup>50</sup>

The TTX provided the opportunity to trial the capability assessment methodology. The After Action Report concluded:

---

<sup>49</sup> Capability Domains & Functional Requirements

<sup>50</sup> Hales, Doug, Peter Avis and Shaye Friesen. Exercise Perseverance: Capability Assessment Table Top Exercise After Action Report, DRDC CSS Technical Report TR2013-010 August 2013 [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p538062\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p538062_A1b.pdf) accessed 24 February 2016.

- Using the EM pillars to group capabilities proved a sound decision, coupling the framework to existing policy and legislation (e.g. the Emergency Management Act) and, with the introduction of a common/enabling group providing linkage to the TCL-C. The introduction of a governance group was not commented on, and analysis of the worksheets suggests it did not present any problem in application;
- The Mission/Function/Task decomposition model was well accepted. The people and organization; policies, processes and practices; and infrastructure, technology and tools construct appeared to work well. It allowed for some discrimination in capability assessment and gap attribution;
- While the scoring of capability elements was found to be simple and reasonable, it was observed that a more robust system of performance measurement would assist in understanding capability levels across the spectrum. At a minimum, the word ladders should be reviewed and refined;
- An initial task library was developed in Microsoft Excel following a review of After Action Reports and the Target Capability List- Canada (TCL-C). It was refined prior to the TTX and rows describing tasks which were deemed outside HP's mandate were hidden. This proved a convenient means to maintain an extensive library while allowing for the selection of tasks tailored for a subset of the community or a specific exercise. During the exercise, a number of minor amendments to the task library were suggested. The HP Exercise Program Division indicated they also had a task list and it was recommended that these be reconciled, the Exercise Division assume ownership, and, as a next step, performance measures (e.g. capability goals) be developed and published as part of the effort to refresh the TCL-C;
- Extracts from publicly available reports on previous pandemic events were reviewed and relate to HP tasks, using the master Excel spreadsheet. The reports were arranged in columns in reverse chronological order from left to right in an effort to allow participants to note remedial progress and support a current assessment. It was not clear if reference was made to the comments in conducting assessments and how useful, if at all, the seeding was. However, in reviewing the methodology at the end of the TTX, there were two proposals, indicating that some found the seeding data useful. It was observed that more and more current data was available, and noted that time and access had constrained a more extensive pre-TTX population. Secondly, it was suggested that executive summaries of the major reports/references be provided to situate comments and that examples should be refreshed;
- Participants were asked to and had difficulty assessing task criticality. It should be made explicit that this includes a sense of how often a capability is invoked/how frequently the HP task must be performed. It was recommended that task importance and frequency be substituted for criticality to avoid any overlap or confusion with capability element assessments, and that an appropriate word ladder be developed;
- Some participants expressed a preference for using an ordinal Likert scale rather than categorical values and a spotlight system. Consensus and a definite recommendation was not realized;
- During the hot wash, it was suggested that a system of weighing the capability elements be introduced. It was not clear the relative importance of elements would contribute much to a capability assessment and may belong more appropriate to analyses of capability generation (solution) options. It was recognized that there is an inherent danger in trying to extrapolate too widely from a single scenario; and

- There were some tasks in which individual assessments diverged significantly and no time or process for resolving the variance. It was not determined whether it was interpretation of the task or unique knowledge sets which contributed. This underscored the shortfalls of a one pass system and the merits of a Delphi approach which feeds back the results (non-attributable) for further discussion. It was recommended that initial assessments should be distributed to participants for review and comment.

The Capability Assessment Management System (CAMS) decision support aid, referred to previously, was developed by the Centre for Security Science to support the Federal Government's All Hazard Risk Approach (AHRA) and systemize Capability Assessments. It can be used to:

- Characterize scenarios and maintain an inventory of "master events" and scenarios,
- Catalogue tasks and maintain a historical record of assessments, and
- Capture SME judgement and facilitate comparison and analysis.

A prototype CAMS has been created in Microsoft Access and a SharePoint site established to support distributed (web-enabled) knowledge elicitation. Task inventories, assessor profiles and impact evaluation scales can be entered beforehand and CAMS used to collect, collate and present ratings.

## 6. Conclusion – Summary of Key Findings

---

There is increasing recognition of the need to establish a rigorous and transparent strategic-level risk analysis methodology and embed it in corporate decision processes and enterprise management structures. In common with other, the 2011 US National Risk Profile was “designed to help policy and budgetary decision makers and critical infrastructure partners understand the critical infrastructure risk landscape and inform their risk management decisions”<sup>51</sup>.

This environmental scan was time and resource constrained and the result far from a comprehensive survey. Nonetheless there are a number of conclusions which can be drawn and take aways which can be tapped to inform a Health Portfolio risk assessment methodology.

All nations follow the staged processes (Establish Context, Risk Identification, Risk Analysis, Risk Evaluation, and Risk Treatment) reflected in the ISO 31000 Risk Management model. There is considerable information pertaining to Risk Assessment (Risk Identification, Risk Analysis and Risk Evaluation), but very little information on Risk Treatment. The survey identified a number of principles describing what a risk assessment process should be:

- Tailored and responsive to an organization’s mandate, culture and capacity;
- Systematic in order to afford an enterprise perspective and identify trade space;
- Inclusive to provide all key stakeholders an opportunity to contribute and share “ownership”;
- Traceable (transparent) in order to facilitate auditing and assure confidence;
- Embedded in corporate management processes and decision cycles.

The survey concluded that few countries have completed many national risk assessment cycles and, hence, practices are evolving and maturing. Frequency, Time Horizon, Oversight and Guidance were examined. It was found that most countries follow a 4-5 year cycle. The Dutch are moving from an annual cycle to a 4 year cycle; the UK maintains a dedicated staff that spends about 9 months a year overseeing an annual national assessment. Typically the focus is on the near term and assessments based on a 5 year time horizon. The AHRA attempted unsuccessfully to combine this with a longer term 25 year outlook. “Best practices” also suggests that a risk assessment guide should be formally approved and published if the intent is to direct and integrate subordinate and partners’ assessments. High level oversight appears the norm ensuring adequate visibility, import and administrative support is accorded risk assessment. In many cases national risk assessments are approved at cabinet or ministerial level.

It is standard practice to solicit community participation and integrate subject matter experts’ judgement in national risk assessments both to draw on their knowledge and establish or reinforce networks of experts and to raise awareness and promote program alignment. In some cases, risk identification is conducted internally; in others, external stakeholders are consulted to ensure a comprehensive recording of hazards and threats. Most countries, including Canada, have

---

<sup>51</sup> U.S. Department of Homeland Security (Homeland Infrastructure Threat and Risk Analysis Centre). 2011 National Risk Profile, July 2011, page 4, <https://info.publicintelligence.net/DHS-NationalRiskProfile2011.pdf> accessed 18 May 2016.



developed a Risk Taxonomy to assist in grouping and characterizing threats and hazards. Typically a distinction is drawn between natural hazards and accidents and malicious attacks. In many countries “outside” experts are invited to participate in evaluating risks to ensure that different perspectives are taken into account.

Scenarios are used to capture assumptions and articulate the themes generated through risk identification. Risk scenarios provide a representational context to situate evaluations. Fidelity differs. In many if not most cases a simple narrative description suffices; in others a more elaborate description is generated. “Best Practices” is to develop “plausible, high consequence”, “reasonable worst case” scenarios as illustrative use cases to situate scenario analysis and evaluation. The All Hazard Risk Approach has introduced the term ‘Full-Spectrum Scenario’ to underscore that emergency management (prevention and preparation) starts before an incident occurs and consequence management (response and recovery) extends beyond the immediate reaction to a risk event. Full spectrum scenarios can be employed to provide a horizontal perspective and consideration of capability requirements both pre and post incident but are not widely used.

All countries acknowledge that risk is a function of likelihood and impact and have developed criteria and logarithmic scales to facilitate comparative assessments of hazards and threats. Common practice is to use a 5 point scale (Very Unlikely, Unlikely, Possible Likely, Highly Likely); this may be complemented (e.g. the AHRA) with a frequency description i.e. Highly Likely = once every year. Combinations of historical data, trend analysis and/or simulations to project the likelihood of occurrence are used to inform assessments of the likelihood of natural hazards and accidents. Intelligence judgments inform estimates of the likelihood of threats posed by human agents. In this case likelihood is, in part, a function of subjective assessment of capability and human intent and there is generally very limited data upon which to base assessments and; hence; heavy reliance on the Intelligence community to estimate the intent and organizational competence and reach of terrorist groups. This introduces security classification issues – both in assessment and communication. No clear “best practice” has emerged and many nations separate assessment of malicious and non-malicious threats and publish and maintain separate risk registers. External stakeholders outside government may have a substantial understanding of the “science” (e.g. manufacture, perishability) of threat agents and, in some countries, are “cleared” and invited to take part in assessments of malicious threats. In the recent (February 2016) CBRNE Consolidated Risk Assessment (CRA) sponsored by Public Safety Canada, subject matter experts from Other Government Departments contributed to a “vulnerability determination”.

There is a general consensus on the need for a set of criteria to assess the impact of risks. Some countries explicitly link these to national values or national interest; others simply identify and describe impact criteria. The set of 4-6 criteria always includes people, economy and environment and often includes critical services and/or societal stability. The AHRA is the most complete; it includes Canadian Territorial Security and Reputation & Influence in addition to Psych-Social as impact measures. In practice, it has proved difficult to apply public outrage and anxiety as indicators. In all cases associated logarithmic scales and word ladders are provided to assist and standardize likelihood and impact assessments. Typically the impact on people is assessed in terms of numbers of deaths, injuries/illness and displaced personnel. The AHRA uses Disability-Adjusted Life years (DALY).

People have a preference for communicating uncertainty using words. “Best Practices” suggest that numerical scores and descriptions should be used to elaborate and establish communication standards to support consumers. There is less of a consensus on to handle uncertainty per se. Scenarios provide a means to make explicit assumptions and inform order of magnitude impact estimates. “Stories” are a particularly effective means for fusing information albeit subject to interpretation and extrapolation.

In some countries, the range of estimates is presented, often as a vector or an oval on a risk matrix diagram, to depict graphically the variance among subject matter experts. It does not appear standard deviation is calculated or used. In many countries, assessors are asked to rate their level of confidence in the supporting data and in their likelihood and impact assessments. Again, this may be represented on a risk matrix to convey an appropriate assurance in the results. In most cases, the presentations depict aggregate and normalized scores with equal weighting assigned to impact criteria. Some countries (e.g. Hungary) conduct sensitivity analysis and publish the results.

Risk Communication is viewed as important. Most countries publish the results of their national risk assessments as a risk register and description and discussion of risk scenarios in part to raise awareness and in part to facilitate program alignment. Several countries, notably the U.K., publish both a classified (National Risk Assessment) and a complementary, unclassified document (National Risk Register of Civil Emergencies).

Most countries present comparative risk evaluation assessments as a risk matrix with risks (risk scenarios) positioned in a two dimensional likelihood versus impact graph. Often colours are added to distinguish higher order from lower order risk scenarios. These Heat Maps offer a tangible output and an intuitively appealing visualization and ordering of identifies risks. Use of a standardized set of criteria facilitates a more detailed analysis of impacts.

Not surprisingly Risk Treatment is not described in equivalent detail. The Norwegian methodology notes that a distinction can be drawn between measures undertaken to reduce the likelihood of risks events and measures undertaken to reduce the impact of risk events. The Australian methodology proposes a scale for use in evaluating the strength and expediency of control measures. The Dutch methodology highlights the link between Risk Assessment and Risk Management, and hints at the role Capability Analysis could play in describing gaps and supporting options analysis.

Capability Based Planning was introduced to address the inherent ambiguity in the public safety and public security environment. The core idea is to confront rather than discount uncertainty. It proposes conducting a functional analysis of operational requirements thereby avoiding prematurely foreclosing on options and fostering the development of people, processes and technology to cater to a broad range of circumstances and challenges.

Increasing interdependence is amplifying the impacts of emergencies, and increasingly importance is being attached to risk informed decision support. The Environmental Survey has identified a number of emergent “best practices” which can – and should – be exploited and adapted in refreshing the Health Portfolio’s Risk assessment/Capability Assessment methodology.

## General

- There is a mature and well defined vocabulary. **The HP should adopt and use ISO and TBS definitions.** There is no need to develop a new/competing lexicon.
- Most counties risk assessment methodology - including the AHRA – are based on - on the ISO process model. **The HP should adopt the ISO process model.**
- These models focus primarily on risk assessment (risk identification, risk analysis and risk evaluation). Although the merits of an integrated approach are appreciated less attention and there is less agreement on best practices for risk treatment. This is likely attributable to organizational structure and accountability frameworks. Increasingly risks, particularly on a national level, span jurisdictions and are shared and require horizontal treatment and program integration. **Insofar as possible a HP capability assessment should acknowledge and address such seams.**

## Governance

- Consistency and acceptance is tied to transparency and traceability. Most countries publish guides to inform both national processes and complementary/subordinate risk assessments. This promotes collective understanding and alignment of treatment. It is likely the AHRA will be refreshed as part of an effort to develop a Canadian risk profile. **The HP should support this effort and may wish to consider in due course maintaining Health Portfolio Guides as an addendum. Meanwhile guides should be prepared; reviewed, approved and published by senior management and distributed/available to stakeholders and partners.**
- Emergent best practices prescribe centralized oversight and senior management ownership e.g. approved by ministers or cabinet. This lends credibility and authority to the assessment and helps ensure that risk assessment is integrated fully into enterprise business processes. **Senior management championship and engagement is required to institutionalize Health Portfolio risk and capability assessment and ensure the results inform decisions.**
- Nations and enterprises aspire to a cyclical risk assessment process. In many nations, not least the AHRA, assessment frequency has not been formalized. The UK maintains an annual cycle with the risk assessment itself taking 9 months. The Dutch have proposed moving from an annual cycle to a 4-5 year cycle. This appears to be the norm. **In determining an appropriate frequency for a HP risk assessment consideration should be given to the national cycle (if one develops), resource requirements needed to conduct a risk assessment and the pace at which health risks are likely to materialize. A preferred option may be to conduct periodic risk assessments to complement a national risk profiling cycle with annual reviews in the intervening period.**

## Conduct

- Stakeholder engagement has become an integral element of best practice. Most commonly SMEs (inside and outside government) support risk analysis. Stakeholders may also be asked to assist in risk identification and elaboration/developing risk

scenarios. **A HP risk and capability assessment should provide for participation by other levels of government, academic communities and external partners.**

Workshops, interviews and/or distributed multi-attribute decision support tools are among the common means used to engage stakeholders.

- Risk Identification
- “Best Practices” suggest that most countries have adopted an **all hazards approach**. This is really a “no brainer”.
- There is no clear best practice relating to risk identification. Some countries have opted to start the process with an internal canvas; others with a bottom-up solicitation. Given the pervasive presence and decentralized nature of health care in Canada, **the HP may prefer to trial integrating top-down and bottom-up approaches.**<sup>52</sup>
- “Best Practices” suggest that it is useful to generate then cull from a comprehensive list of risks. Ideas spawn ideas. Hence **some form of dedicated and broadly-based real or virtual interaction is recommended.**
- Risk taxonomies provide a collation and characterization schema. National taxonomies inherent attempt to provide for all things to all people. Most distinguish between non-malicious and malicious agents. **The Health Portfolio should consider generating a tailored Health Portfolio risk taxonomy to complement the national/AHRA risk taxonomy.**

## Risk Analysis/Risk Evaluation

- The fidelity may vary but all countries **employ risk scenarios to articulate risk and capture key assumptions**. Another “no brainer”. **Developing a plausible high consequence risk scenario rather than higher and lower impact variants seems the preferred course.**
- All countries survey, following the ISO definition, **distinguish between likelihood and impact in assessing and ordering risks**. This too is a “no brainer”.
- “Best Practices” suggests that **word descriptors with numerical scales and explanations** assist in framing and standardizing assessments enabling synthesis and comparison.
- All countries – and **a Health Portfolio risk assessment methodology should - rely Subject Matter Experts’ value judgements**. Collaborative efforts have indirect benefits e.g. knowledge dispersion and creation of networks and communities.
- It is common practice to **base likelihood assessments of natural hazards and accidents on historical data or models**.
- There is less consensus on how to evaluate the likelihood of malicious acts. It is generally accepted this is a function of capability and intent, and a full assessment reliant on Intelligence. Subject Matter Experts may be invited to assist in assessing vulnerabilities. Some countries separate non-malicious and malicious threat assessment and maintain separate open and classified risk registers. **Health Portfolio SMEs are in a position to assist with vulnerability assessments of chemical, biological and radiological threats.**

---

<sup>52</sup> A review of the risk themes and scenarios the countries surveyed developed is attached as an annex to the draft Health Portfolio Guide to Risk Assessment.

- There is general consensus that consequence assessments should consider several key criteria e.g. impacts People, Economy, Environment and Society. **The focus for the Health Portfolio will be People generally expressed in terms of Deaths, Injuries & Illness and Displaced.** A number of countries also factor in the ability to maintain critical services. **A Health Portfolio risk assessment methodology may wish to incorporate a criterion related to critical health services.**
- **“Best Practices” should be followed and assessors’ confidence in the supporting data and likelihood and impact assessments captured.**
- Risk Communication
- **The Health Portfolio should follow “best practices” and share if not publish the results of a risk assessment.**
- **A risk matrix (likelihood versus impact) graph using colours to distinguish higher order risks should be used to depict the results (comparative ordering) of risks.**

## Risk Treatment

- There is very limited “best practices” to draw upon. It could be argued that *Exercise Perseverance* went some way to establishing “best practice”. The potential for a functional approach – capability based analysis – is recognized and has been adopted in many countries, notably The Technical Cooperation Program (TTCP) community.<sup>53</sup> **It is recommended that the Health Portfolio develop and trial a Capability Assessment methodology to support gap analysis and risk treatment.**

---

<sup>53</sup> The aim of The Technical Cooperation Program (TTCP) is to foster exchange and collaboration in defence related a research and development between Australia, Canada, New Zealand, the United Kingdom and the United States.

## 7. Bibliography

---

- Asian Disaster Preparedness Centre. Developing A National Risk Profile of Laos, Part 1: Hazard Assessment, November 2010 [http://www.adpc.net/igo/category/ID275/doc/2013-sWNa61-ADPC-Final\\_Report\\_Part1.pdf](http://www.adpc.net/igo/category/ID275/doc/2013-sWNa61-ADPC-Final_Report_Part1.pdf) accessed 24 April 2016.
- Asian Disaster Preparedness Centre. Developing a National Risk Profile of Laos, Part 2: Exposure, Vulnerability and Risk Assessment, 2010, [http://www.gripweb.org/gripweb/sites/default/files/Lao\\_RiskProfile\\_Part2.pdf](http://www.gripweb.org/gripweb/sites/default/files/Lao_RiskProfile_Part2.pdf) accessed 24 April 2016.
- Association of Insurance and Risk Managers, The Public Risk Management Association and The Institute of Risk Management. A Structure Approach to Enterprise Risk Management (ERM) and the Requirements of ISOP 31000, [http://www.airmic.com/sites/default/files/ERM\\_ISO-31000\\_guide.pdf](http://www.airmic.com/sites/default/files/ERM_ISO-31000_guide.pdf) accessed 22 December 2015.
- Australian Government. National Emergency Assessment Guide lines (Handbook 10), Second Edition, 2015, <https://www.ag.gov.au/EmergencyManagement/Tools-and-resources/Publications/Documents/Handbook-series/NERAG-Handbook10.pdf> accessed 22 December 2015.
- Australian Government. National Emergency Assessment Guidelines Practice Guide (Handbook 11), 2015, <https://www.ag.gov.au/EmergencyManagement/Tools-and-resources/Publications/Documents/Handbook-series/NERAG-Handbook11.pdf> accessed 22 December 2015.
- Bayne, Ian, Jim Duncan, Brad Mills and Shaye Friessen. The Federal All Hazards Risk Assessment Framework Body of Knowledge: Volume I Establishing an Information Baseline and Way Forward, DRDC Technical Report CSS TR 2013-014, September 2013, accessed 21 December 2015.
- Bayne, Ian, Jim Duncan, Brad Mills and Shaye Friessen. The Federal All Hazards Risk Assessment Framework Body of Knowledge: Volume II Supporting Material, DRDC Technical Report CSS TR 2013-015, September 2013, accessed 21 December 2015.
- Bayne, Ian and Jim Duncan. All Hazard Risk Assessment: Documenting the Calibration Process and Methodology, Defence R&D Canada- Centre for Security Science, DRDC CSS-CR 2013-016, September 2013 [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p537911\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p537911_A1b.pdf) accessed 27 November 2015.
- Caudle, Sharon. Homeland Security: Advancing the National Strategic Position, Homeland Security Affairs Volume 8, Article 11 (August 2012) <https://www.hsaj.org/articles/225> accessed 15 February.
- Centre for Security Science. *Building Canada's National Risk Profile*, presentation to the Associate Deputy Ministers' Emergency Management Committee, 14 December 2015.
- Davis, Paul K., Walter L. Perry, John S. Hollywood, David Manheim. Uncertainty-Sensitive Heterogeneous Information Fusion, RAND, 2016 [http://www.rand.org/pubs/research\\_reports/RR1200.html](http://www.rand.org/pubs/research_reports/RR1200.html) accessed 21 April 2016.
- Government of Canada. Guide to Risk Taxonomies, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/grt-gtr/grt-gtrtb-eng.asp> accessed 25 January 2016.
- Government of Canada. Guide to Integrated Risk Management, <https://www.tbs-sct.gc.ca/hgw-cgf/pol/rm-gr/girm-ggir/girm-ggirpr-eng.asp> accessed 25 January 2016.

- Hales, Doug and Paul Chouinard. Implementing Capability Based Planning within the Public Safety and Security Sector, DRDC Centre for Security Science TM2011-26, December 2011 [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc122/p537217\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc122/p537217_A1b.pdf) accessed 24 February 2016.
- Hales, Doug, Peter Avis and Shaye Friesen. Exercise Perseverance: Capability Assessment Table Top Exercise After Action Report, DRDC CSS Technical Report TR2013-010 August 2013 [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p538062\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc140/p538062_A1b.pdf) accessed 24 February 2016
- Hallegatte, Stephane and Valentin Przulski. The Economics of Natural Disaster: Concepts and Methods, The World Bank, Policy Research Paper 5507, December 2010 <http://elibrary.worldbank.org/doi/abs/10.1596/1813-9450-5507> accessed 14 March 2016..
- International Organization for Standardization. ISO 31000 2009 Risk Management - Principles and Guidelines, 15 November 2009.
- International Organization for Standardization. ISO/IEC 31010.2009 Risk Management – Risk Assessment Techniques, 1 December 2009.
- International Organization for Standardization. ISO Guide 73.2009 Risk Management - Vocabulary, 15 November 2009 Section 2.1.1 , <https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en> accessed 20 April 2016.
- Leung, Kevin and Simona Verga. Expert Judgement in Risk Assessment, DRDC Centre for Operational Research & Analysis, TM 2007-57, December 2007 <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc88/p529083.pdf> accessed 14 March 2016.
- Lundberg, Russell. Comparing Homeland Security Risks Using a Deliberate Risk Ranking Methodology, RAND, 2013 [http://www.rand.org/pubs/external\\_publications/EP66409.html](http://www.rand.org/pubs/external_publications/EP66409.html) accessed 21 April 2016.
- Make IT Inc. Enterprise Risk Management – User’s Guide, DRDC CSS CSSP-2013-1024, May 2015.
- Mandel, David. Accuracy of Intelligence Forecasts From the Intelligence Consumer’s Perspective, DRDC-RDDC 2015-PO92, [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc198/p802390_A1b.pdf) accessed 28 March 2016.
- Ministry of Security and Justice. Working with Scenarios, Risk Assessment and Capabilities in the National Safety and Security Strategy of the Netherlands, [http://www.preventionweb.net/files/26422\\_guidancemethodologynationalsafetyan.pdf](http://www.preventionweb.net/files/26422_guidancemethodologynationalsafetyan.pdf) accessed 21 December 2015.
- NATO Joint Analysis and Lessons Learned Centre. The NATO Lesson Learned Handbook, Third Edition, February 2016, [http://www.jallc.nato.int/products/docs/Lessons\\_Learned\\_Handbook\\_3rd\\_Edition.pdf](http://www.jallc.nato.int/products/docs/Lessons_Learned_Handbook_3rd_Edition.pdf) accessed 24 April 2016.
- (Netherlands) Network of Analysts for National Security National Risk Assessment 2011, [C:\Users\DHatesConsulting\Downloads\national-risk-assessment-2011\\_tcm92-538995\(5\).pdf](C:\Users\DHatesConsulting\Downloads\national-risk-assessment-2011_tcm92-538995(5).pdf) accessed 24 March 2016.
- Norwegian Directorate for Civil Protection. 2013 National Risk Analysis, [http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB\\_2013\\_english.pdf](http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013_english.pdf) accessed 24 March 2016

- Organization for Economic Co-operation and Development. National Risk Assessment – Profiles of Selected OECD Countries, 2 December 2015.
- Public Safety Canada, All Hazards Risk Assessment: Methodology Guidelines 2012-2013, 2012, <http://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ll-hzrds-sssmnt/index-eng.aspx> accessed 23 April 2015,
- U.K. Cabinet Office, National Risk Register of Civil Emergencies, 2015 edition, [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/419549/20150331\\_2015-NRR-WA\\_Final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/419549/20150331_2015-NRR-WA_Final.pdf) accessed 20 April 2016.
- U.S. Department of Homeland Security. Target Capabilities List, September 2007 <http://www.fema.gov/pdf/government/training/tcl.pdf> accessed 17 February 2016.
- U.S. Department of Homeland Security. Risk Lexicon, September 2008, [https://www.dhs.gov/xlibrary/assets/dhs\\_risk\\_lexicon.pdf](https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf) accessed 25 January 2016.
- U.S. Department of Homeland Security. Presidential Policy Directive/PPD-: National Preparedness, 30 March 2011 <http://www.dhs.gov/presidential-policy-directive-8-national-preparedness> accessed 27 January 2016
- U.S. Department of Homeland Security. Risk Management Fundamentals, <http://www.dhs.gov/xlibrary/assets/rma-risk-management-fundamentals.pdf> April 2011 accessed 17 February 2016.
- U.S. Department of Homeland Security (Homeland Infrastructure Threat and Risk Analysis Centre). 2011 National Risk Profile, July 2011 <https://info.publicintelligence.net/DHS-NationalRiskProfile2011.pdf> accessed 18 May 2016.
- U.S. Department of Homeland Security. DHS Strategic National Risk Assessment, December 2011 <http://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf> accessed 27 January 2016.
- U.S. Department of Homeland Security. Threat and Hazard Identification and Risk Assessment Guide. August 2013. [http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201\\_htirag\\_2nd\\_edition.pdf](http://www.fema.gov/media-library-data/8ca0a9e54dc8b037a55b402b2a269e94/CPG201_htirag_2nd_edition.pdf) accessed 16 February 2016.
- U.S. Department of Homeland Security. The 2014 Quadrennial Homeland Security Review, June 2014, <http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf> accessed 17 February 2016.
- US Department of Homeland Security. National Preparedness Goal, Second Edition, September 2015 [http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National\\_Preparedness\\_Goal\\_2nd\\_Edition.pdf](http://www.fema.gov/media-library-data/1443799615171-2aae90be55041740f97e8532fc680d40/National_Preparedness_Goal_2nd_Edition.pdf) accessed 28 January 2016.
- Verga, Simona. Intellectual Experts Group: All-Hazards Risk Assessment Lexicon, DRDC Centre for Security Science, N-2007-001, [http://cradpdf.drdc-rddc.gc.ca/PDFS/unc144/p528740\\_A1b.pdf](http://cradpdf.drdc-rddc.gc.ca/PDFS/unc144/p528740_A1b.pdf) accessed 14 March 2016.
- Verga, Simona and Shaye Friesen. Federal All Hazards Risk Assessment (AHRA) – Analysis of Scenario Results. DRDC-RDDC-2014-L310, 17 December 2014.



## 8. Annex A. RAND Conceptual Models

---

A recent RAND report offers conceptual models illustrating the complexity of estimating the threats posed by malicious actors. As depicted in Figure 24, it is posited that motivation, legitimacy, opportunity and cost calculations inform the propensity for an individual to conduct a terrorist act.

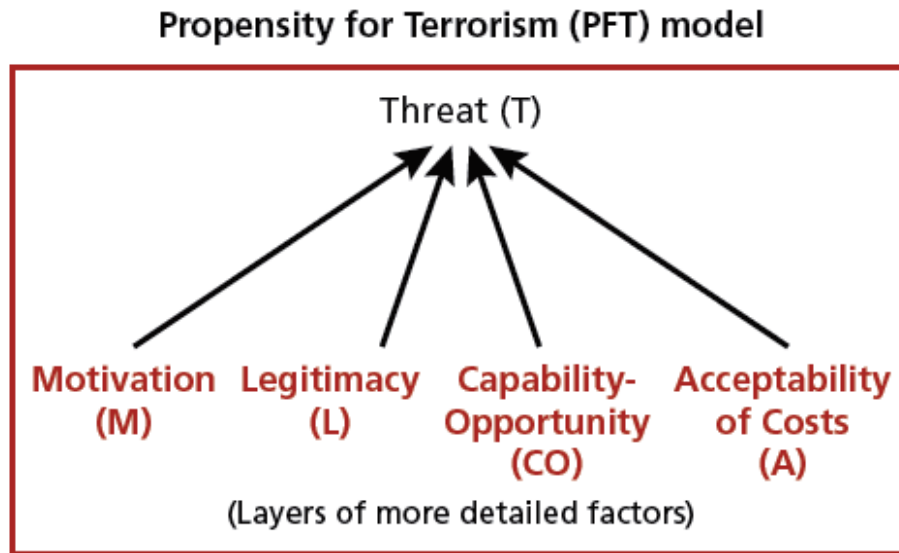


Figure 24 RAND Propensity for Terrorism Conceptual Model<sup>54</sup>

Further, as depicted below (Figure 25) the threats terrorists pose need to be assessed in terms of willingness, impact and target vulnerability (probability of success).

---

<sup>54</sup> Davis, Paul K., Walter L. Perry, John S. Hollywood, David Manheim. Uncertainty-Sensitive Heterogeneous Information Fusion, RAND, 2016, page 8, [http://www.rand.org/pubs/research\\_reports/RR1200.html](http://www.rand.org/pubs/research_reports/RR1200.html) accessed 21 April 2016.

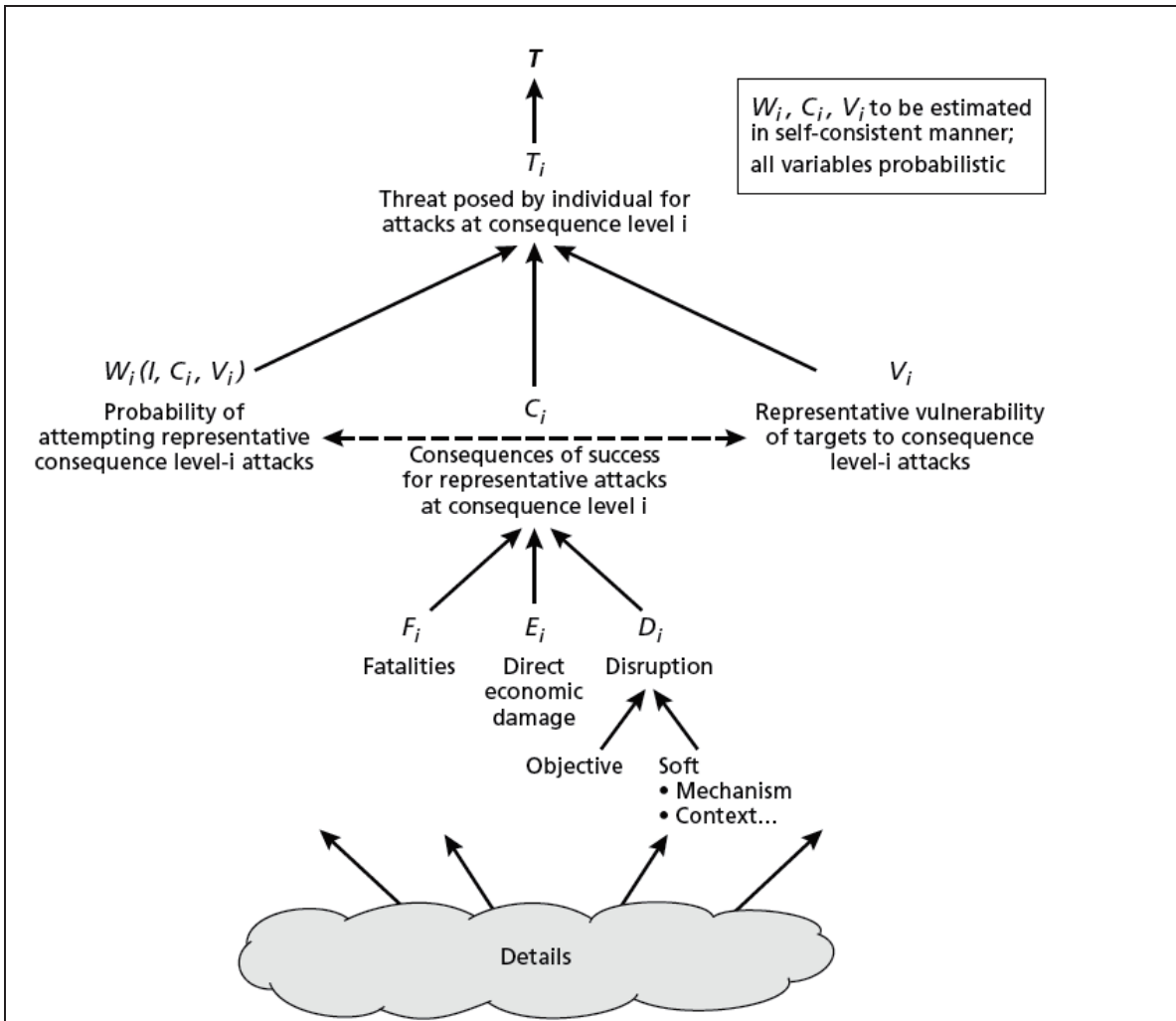


Figure 25 RAND Conceptual Terrorist Threat Model<sup>55</sup>

<sup>55</sup> Davis, Paul K., Walter L. Perry, John S. Hollywood, David Manheim. Uncertainty-Sensitive Heterogeneous Information Fusion, RAND, 2016, page 109, [http://www.rand.org/pubs/research\\_reports/RR1200.html](http://www.rand.org/pubs/research_reports/RR1200.html) accessed 21 April 2016.

## 9. Acronyms and Abbreviations

---

ADM	Associate Deputy Minister
AHRA	All Hazards Risk Assessment
CAMS	Capability Assessment Management System
CBP	Capability Based Planning
CI	Critical Infrastructure
CRA	Consolidated Risk Assessment
CSS	Centre for Security Science
DALY	Disability-Adjusted Life Years
DEMA	Danish Emergency Management Agency
DHS	(US) Department of Homeland Security
DRDC	Defence Research & Development Canada
EM	Emergency Management
EMA	<i>Emergency Management Act</i>
ESF	Emergency Support Functions
FY	Fiscal Year
GC	Government of Canada
GHSI	Global Health Security Initiative
HC	Health Canada
HP	Health Portfolio
ISO	International Organization for Standardization
MCM	Medical Counter Measures
MTA	Material Threat Assessment
NERAG	National Emergency Risk Assessment Guidelines
NRP	National Risk Profile
PHAC	Public Health Agency of Canada
PPD	Presidential Policy Directive
PS	Public Safety Canada
OECD	Organization for Economic Co-operation and Development
OGD	Other Government Departments
PS	Public Safety Canada
RPP	Report on Plans and Priorities
SME	Subject Matter Expert
SNRA	Strategic National Risk Assessment
TBS	Treasury Board Secretariat

TCL	Target Capability List
TCL-C	Target Capability List-Canada
TTX	Table Top Exercise
UK	United Kingdom
US	United States
VFT	Value Focused Thinking
WHO	World Health Organization