Defence Research and
Development Canada
Centre for Security Science
222 Nepean Street, 11th floor
Ottawa, Ontario
K1A 0K2

Recherche et développement
pour la défense Canada
Centre des sciences pour la sécurité
222, rue Nepean, 11ième étage
Ottawa, Ontario
K1A 0K2

File/Project number: CSSP-2012-TI-1101 (DSS) DRDC LR 2013-047

December 3, 2012

Preliminary results of the Consolidated Risk Assessment to inform Capability Based Planning in support of emergency planning for the Metro-Vancouver region

INTRODUCTION

In 2009, Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS) started a pilot project with six regions aimed at implementing a Capability Based Planning (CBP) approach to emergency management and response planning. The first step in the CBP process is conducting an all-hazards risk assessment. The pilot seeks to engage, at the "grass-roots" level, regional response organizations, and develop a common framework and tools that would enable them to assess all-hazards risk in their regions. The Operations Research (OR) team at DRDC CSS was asked to help refine the risk assessment methodology and tool before the regional CBP Consolidated Risk Assessment (CRA) for the Capital Regional District around Victoria, BC. Members of the OR team observed the CRA Workshops in Victoria, and proposed additional adjustments to the CRA methodology, based on lessons learned. For the regional CBP CRA in Metro Vancouver, the authors provided on-site scientific advice during risk assessment workshops, and assisted with analyzing the data collected during the risk assessment workshops.

This Letter Report (LR) summarizes the main results and recommendations following the CBP CRA conducted in the Metro-Vancouver region.

RESULTS

As part of the CBP CRA process, risk event scenarios were developed by a regional working group across five threat/hazard categories, and assessed by subject matter experts from the region during risk assessment workshops. The starting point for scenario development was a pre-existing set of vignettes, inspired by the Chemical, Biological, Radiological and Nuclear, and Explosive (CBRNE) Research and Technology Initiative (CRTI) CRA. This CRTI CRA-inspired set of vignettes was generated using a threat-against-target structure. Only those vignettes deemed applicable to the region were developed into scenarios. Each scenario was evaluated in terms of likelihood and impact during a risk assessment workshop.

The workshops were grouped according to threat/hazard category. Workshops for rating Technological and Accidental risk scenarios were held in November 2011. Participants encountered difficulties when assessing scenarios in those categories due to the lack of suitable definitions and guidance on how to apply rating criteria. Regional organizers postponed the risk assessment workshops for Terrorism/CBRNE, Human Intentional, and Natural scenarios to February-March 2012. They requested assistance with preparing educational material for workshop participants. They also requested that a scientific advisor be present during the workshops, in order to address questions and clarifications about the methodology, and ensure consistency of ratings across the categories. During the remaining workshops, the on-site scientific advisor addressed many questions related to definitions of terms and the impact and likelihood rating. The CBP CRA methodology is summarized in Annex A.

Following the risk assessment workshops, the DRDC CSS OR analysts analysed the data collected. Based on the results of data analysis, summarized in Annex B, the analysts provided advice on selecting priority scenarios for the next phase in the CBP process, which is developing full-spectrum scenarios to aid the capability analysis. Uncertainty around the point estimates, scenario grouping, and sensitivity analysis were additional factors considered in the selection of scenarios. For each category, scenarios were grouped in different priority groups, and an additional workshop was organized on October 3rd, 2012, to present the results to regional stakeholders for discussion and validation.

RECOMMENDATION

The regional CBP CRA for the Metro-Vancouver region benefited from dedicated analytical support provided by the DRDC CSS OR team both through refining definitions of terms, clarifications about the methodology, and analysing risk assessment workshop data. On-site participation also provided the scientific advisor an opportunity to observe the process, which provided useful information both for subsequent data analysis and for further refining the scenario development, as well as the risk assessment methodology and tool.

Based on the results of the data analysis, the DRDC CSS OR team recommends a set of scenarios for further evaluation, in order to inform the next step, developing full-spectrum scenarios to aid the capability assessment across the full spectrum from prevention, protection, mitigation, through to response and recovery. The recommended set of priority scenarios is presented in Annex C. Depending on stakeholder/planning requirements, further evaluation of scenarios in the priority set is recommended, including factors such as the overall risk score, relative positioning on an impact vs. likelihood scatterplot within each category, and desired representation of risks across categories, in order to test capabilities across the all-hazards domain.

Comments or questions on this Letter Report are welcome and should be addressed to Simona Verga at (613) 944-8165 or by email to simona.verga@drdc-rddc.gc.ca .

Prepared for: Clarence Lai, IPREM Emergency Management Planning Coordinator
Heather Lyle (Director, Integrated Public Safety, Emergency Management British Columbia)

Prepared by:

XXX - Original signed by - XXX
Simona Verga
Operational Research Analyst

XXX - Original signed by - XXX
Paul Chouinard
Senior CSSP OR&A Advisor

Approved by:

XXX - Original signed by - XXX
Denis Bergeron
Manager, Decision Support

Cc: Sheldon Dickie, Alain Goudreau

Canada

DEFENCE DÉFENSE

ANNEX A – THE METRO-VANCOUVER REGIONAL CBP CRA: METHODOLOGY, WORKSHOPS, AND DATA ANALYSIS

Capability Based Planning

Capability-Based Planning is a type of planning that requires a functional analysis of future operational requirements. CBP involves planning, within an economic framework, and under uncertainty, for response capabilities that are flexible and interchangeable, to address a wide range of potential threats and hazards[1]. The solution sought is expressed in terms of an ability to perform tasks (i.e., a capability), rather than specific resources such as personnel, equipment, etc., although a capability will involve a combination of such resources. By being functionally focused, CBP is well suited for all-hazards, longer-term planning processes within the public safety and security domain. In addition, the functional focus aids in comparing requirements across different stakeholders, which makes CBP well suited to planning within a multi-agency context, which is often the case with planning for public safety and security emergencies.

Consolidated Risk Assessment

The Consolidated Risk Assessment is the first step in the Capability Based Planning Process. Risk provides the means to articulate potential threats and hazards in a way that helps determine functional requirements and assess capability gaps. Scenarios are employed to sample the problem space, and to provide context and specificity to identified sources of risk. They serve to move CBP from concept to practice, providing the means to establish metrics, evaluate response options, define requirements, and focus exercises and training.

Threat/Hazard-Based Scenarios

As in all regions where a CBP CRA was conducted previously, scenarios in for the Metro-Vancouver CRA were researched and developed by a scenario development group comprised of regional experts. The starting point was a prior set of vignettes inspired by the Consolidated Risk Assessment (CRA) conducted to inform investment through the Chemical, Biological, Radiological and Nuclear, and Explosive (CBRNE) Research and Technology Initiative (CRTI), one of the programs managed by CSS until April 2012. The CRTI CRA-inspired set of vignettes was generated using a threat-against-target structure.

There are five threat/hazard categories: Human Intentional (HI), Terrorism Attack (TA)/CBRNE, Human Accidental (HA), Technological (T), and Natural (Weather – NW, Geological – NG, and Biological – NB). There are also five “target” categories: Citizens and their Assets, Agriculture, Infrastructure-Fixed, Infrastructure-Transportation, and Communications/Cyber/Control. Each vignette is derived by “applying” a “threat” (e.g., Natural Weather – NW) to a “target” (e.g., Citizens and their Assets – CA). The value of this approach is that it provides a structured way to generate scenarios that ensures comprehensive coverage across the all-hazards domain, common across participating regions. The fairly large set of starting vignettes posed a challenge; however, scenarios were only developed from vignettes deemed applicable to the region.

[1] Paul K. Davis, Analytical Architecture for Capabilities-Based Planning, Mission-System Analysis and Transformation, RAND, Santa Monica, 2002, pp.1

The resulting set of scenarios spanned the range of threats and hazards that are present in the region. The scenario set is intended to highlight issues that require further analysis of required capabilities for mitigation, prevention, protection, response, and recovery.

Workshops

Scenarios were evaluated during regional workshops, with experts from the region providing input into the likelihood and impact assessment for each scenario. Scenarios in each of the five threat/hazard categories were assessed during a one-day workshop. Workshops for rating Technological and Accidental risk scenarios were held in November 2011, and workshops for Terrorism/CBRNE, Human Intentional, and Natural scenarios were held in February-March 2012.

Rating process

The rating method used was inspired by the Delphi technique, where structured elicitation of opinions from a panel of experts results in forecasts about quantities of interest. In the standard version, the individual forecasts are provided anonymously. The process continues for a number of iterations and the experts are asked to revise their judgments based on the summary of the other experts' forecasts from the previous round. The reasoning behind it is that, when the "collective knowledge" assembled from individual forecast is fed back to the participants, the range of answers will decrease and the group will "converge" on the "correct" answer. While close implementation of the Delphi process is rarely practical, the principles of the process must be preserved, in order to end up with usable scenario ratings. Feedback from the group and the opportunity to reevaluate are essential in reducing the spread in ratings.

During the workshops, voting was repeated in most cases until at least 50% of participants agreed on an estimate for the quantity rated. At the same time, the use of individual electronic voting devices enabled recording the distribution of ratings across participants, which was useful in the post-workshop analysis of risk data. There were a number of scenarios where 50% "consensus" was not reached, in which case the value with most votes (the mode) was chosen as the estimate for that quantity. In case of a tie (multi-modal distribution), the "worst case" value was chosen.

Concepts and terms

During the workshops for rating Technological and Accidental risk scenarios, participants encountered difficulties when assessing scenarios due to the lack of suitable definitions and guidance on how to apply rating criteria. The remaining workshops for Terrorism/CBRNE, Human Intentional, and Natural scenarios were delayed by a few months as a result. In preparation for the remaining workshops, regional organizers requested assistance in generating definitions and clarification for terms utilized within the risk assessment methodology. Definitions for a number of key terms are included below.

Risk:

- Definition: Potential for an unwanted outcome resulting from an incident, event or occurrence (involving a hazard within a specified timeframe), as determined by its likelihood and its associated consequences

Consequence:

- Definition: Effect of an event, incident, or occurrence

Impact:

- Definition: The extent to which a risk, should it occur, has an effect on population, economy, environment, and critical infrastructure
- Associates a “measurement” to possible consequences of a risk

Likelihood:

- Definition: Chance of something happening, whether defined, measured or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities.
- Frequency estimates – used for likelihood assessment for natural, human accidental and technological risks
- Feasibility of an attack – used as a “proxy” for likelihood of intentional/terrorism risks

Frequency:

- Definition: Number of occurrences of an event per defined period of time or number of trials

Feasibility:

- Definition: Combination of the diffent elements necessary to mounting an intentional/malicious attack, for example a terrorist event.
- Feasibility of an attack such as described in a risk event provides a measure of likelihood.

Likelihood assessment

Different rating methods are employed for likelihood assessment, depending on the threat/hazard scenario category. The rating methods are very briefly described below, with a more detailed description of the rating methodology to follow in a forthcoming more comprehensive technical report.

For the Natural, Human Accidental, and Technological risks, the likelihood assessment is based on frequency estimates derived from historical data. Trends can be captured and can modify historical estimates, through the use of trend modifiers.

Rating scales follow an order of magnitude approach, where the ratio between the magnitude of two events described by consecutive rating levels is √10 (approximately 3)[2]. A trend can be employed to modify an estimate based on historical data if it is anticipated that trends are significant enough to make the event at least approximately three times more (or less) likely. The rating scale goes from 0 to 9.

For Intentional and Terrorism/CBRNE scenarios, the feasibility of the attack is used as a “proxy” for likelihood. This approach assumes that intent is uniform throughout the region

[2] Note that the ratio for two levels difference is 10.

across all scenarios in the category. The capability of malicious actors to mount the attack is also not explicitly assessed, but is implicit in the assessment of the feasibility.

The feasibility rating was based on a combination of necessary components to mount an attack such as described in the scenario: materials, equipment, technical expertise, and knowledge. The rating is qualitative, based on verbal descriptors describing each rating level. Although the rating for each component goes from 0 to 4.5, the aggregated feasibility score follows a 0 to 9 scale, although the mapping of the feasibility scale onto the frequency scale requires additional calibration.

Impact assessment

The impact is assessed across a set of four primary impact categories: People, Environment, Disruption of Critical Infrastructure, and Economic Loss. The People category includes fatalities, severe injuries, and people displaced or without access to basic necessities of life. The Environment category considers the extent of environmental damage, the required level of environmental response, as well as necessary efforts for clean-up and recovery. Disruption of Critical Infrastructure considers the number of people affected by the disruption, as well as the duration and extent of the disruption. Economic Loss includes both direct and indirect losses.

In order to insure a consistent mathematical framework for the impact and risk scores, the rating for each impact category is based on the "magnitude" of the loss in that category. This implies a constant ratio for the increase in severity from one level to the next. As in the case of likelihood, the impact rating uses a ratio of approximately 3 ($\sqrt{10}$) in increased severity from one level to the next. The rating scale goes from 0 to 9[3], similarly to likelihood rating.

Additionally, supplementary categories may be added, which are difficult to include satisfactorily into an overall risk score, but nonetheless add important information necessary for the later development of detailed scenarios, or might be of interest to specific capability areas. For example, the impact of scenarios on companion animals has been considered in all participating regions so far. Lessons learned from Hurricane Katrina have shown that the lack of plans for emergency assistance for affected animals hindered efforts to evacuate their owners, who would not evacuate without their pets.

Risk score

The final risk score is a combination of scores for likelihood and impact. With a logarithmic (order of magnitude) approach, the likelihood and impact scores are added for each impact category; the impact category with highest score will produce the overall risk score. Thus, the overall risk score can have a value between 0 and 18.

Reference iso-risk contours

In order to decide which scenarios to include in the priority set, a "threshold" risk value is needed. A pre-determined value can be chosen, for example, by dividing the 0-18 scale into a number of intervals, and scenarios whose overall risk score fall within the highest

---

[3] Note that a rating of zero does not equal Nil impact. If a category does not apply for a particular scenario, it is rated as Nil. A rating of zero implies a possible, if very small, impact in that category.

interval are selected for further development. In the case of the CRA, a risk threshold of "11" was chosen as a starting point (for non-intentional threat scenario; see discussion below). However, in doing so, scenarios with very close risk scores might end up in different priority groups. Although some degree of arbitrary is unavoidable, looking at the natural "clustering" of scenarios before deciding where to draw the line makes more sense, particularly in light of the inherent uncertainty around any point estimates for risk (see below discussion on sensitivity analysis).

When "drawing the line", it is useful to establish iso-risk contours, which are contours of equal risk on an Impact vs. Likelihood scatter plot. For a logarithmic rating approach, the contour is a diagonal line.

Uncertainty

Uncertainty is generally defined as an inability to exactly determine the values for variables (e.g., likelihood and consequence, or to predict a future state). Uncertainty is inherent in risk.

For the Metro Vancouver regional CRA, differences in likelihood and impact ratings produced by participants were captured, and produced a measure of uncertainty around point estimates for risk.

Agreement

As mentioned, rating for both likelihood and impact was based on "consensus" among participants; the rating process continued until 50% of participants agreed on a score. On an Impact vs. Likelihood scatter plot, this "consensus" rating is shown by a "dot", representing a (likelihood, impact) pair for each scenario.

In practice, in some cases "consensus" was not reached; in those cases, the ratings produced by 50% of participants cover a range around the most "popular" value (the mode) for likelihood, impact, or both, as the case may be. This value – the mode – was recorded in the corresponding cell in the risk assessment template. However, showing only those values amounts to discarding the ratings of all participants who produced a different value, which in some cases meant more than half of the participants.

In addition to the mode, the Impact vs. Likelihood graphs below include ratings produced by 65% of participants, shown as ranges around the most "popular" value (the mode) for both likelihood and impact. Thus, each "dot" is surrounded by a "box", the height (width) of which represents the spread of values produced by 65% of participants around the mode value for impact (likelihood). The smaller the box, the more "convergent" the opinion of participants. The 65% agreement "box" has better chances of capturing the actual risk associated with that scenario than the 50% one. The 65% distribution was chosen by a "trial and error" process, balancing the need to include uncertainty around the point estimates with the need to be able to distinguish between scenarios within different priority groups, as well as the need to be consistent across hazard categories.

Scenario grouping

Scenarios can be characterized by likelihood and impact scores (i.e., general position on an Impact vs. Likelihood scatter plot), as well as overall risk (scenarios with equal overall risk lie along on the same iso-risk line). Depending on the stakeholder/planning needs, the focus for follow on analysis might shift between two broad categories:

- High Impact-Low Frequency scenarios (i.e., EM planners), or
- Low Impact- High Frequency scenarios (i.e., operational community)

Additionally, given the uncertainty in the estimates, due to differences in ratings produced by participants and reflected in having “boxes” instead of “dots”, the sizes of which are related to the level of agreement among the participants, it might be difficult to tell scenarios apart, in terms of overall risk, due to overlap of “boxes”. Risk scenarios that are positioned closely together and that overlap should be treated at the same priority level.

Likelihood calibration for intentional and terrorism/CBRNE scenarios

The CRA did not directly assess the likelihood of intentional threats but rather only the feasibility. However, in order to compare intentional threat scenarios with non-intentional threat scenarios one must convert the feasibility score into a likelihood score. The method chosen was a “calibration” method whereby the highest “feasibility” score across the intentional threat scenarios was anchored to a “likelihood” score (i.e., calibrated) while the remaining “feasibility” scores where mapped to “likelihood” scores based on that anchor value. This approach assumes that “intent” is uniform across all intentional threat scenarios. The method for anchoring the highest feasibility score to a likelihood score was to consider the frequency of similar incidents in North America (Canada and the US only) over the past decade, and to assume that the likelihood for the BC Lower Mainland was about the same on a per capita basis. This assumes that the likelihood within the BC Lower Mainland is approximately the same, on a per capita basis, as what we’ve seen in the past decade across North America. It is possible that this underestimates future likelihood, but, as mentioned under the section on Sensitivity Analysis, this can be addressed by using a lower risk threshold for the inclusion of intentional threat scenarios.

Sensitivity analysis

Sensitivity analysis is one method for reducing the effects of uncertainty on analysis. The goals of sensitivity analysis are to:

- Determine the limitations of the analysis,
- Identify and isolate those factors that contribute the most to uncertainty;
- Ensure that the results are still valid despite uncertainty with respect to the value of factors in the analysis; and
- Provide the decision maker with a better understanding of the problem and effect of uncertainty on decisions.

The recommended approach[4] to sensitivity analysis is to:

- Identify the factors that have the greatest effect on the analysis;

---

[4] NATO Code of best practice for C^2 assessment, Command and Control Research Program, US Department of Defense, October 2002, retrieved from www.dodccrp.org

- Vary the factors across a range of values to see the effects on the results; and
- Focus on the variations in factors that most affect results or decision based on the results.

The decision that results from the CRA is the inclusion or exclusion of scenarios from the "priority" set of scenarios. Two types of errors might results from this decision:

1. The inclusion of low priority scenarios in the high priority set because the group estimates were too high; and
2. The exclusion of actual high priority scenarios from the high priority set because the group estimates are too low.

By using the range of estimates from the group as a proxy for uncertainty and displaying these ranges on the risk plots, one is able to see the risk with the inclusion or exclusion of a scenario from the high priority set. If the reference iso-risk contour passes through the "agreement box" around the "consensus" point estimates for a scenario that's included in the high priority scenario set, there is some risk that this scenario has been erroneously included. On the other hand, if the reference iso-risk contour passes through the "agreement box" of a scenario excluded from the high priority scenario set, there is some risk that the scenario was erroneously excluded. Adjusting the "threshold" iso-risk contour to respect the natural "clustering" of scenarios, particularly in light of the inherent uncertainty around point estimates, is one way to mitigate this risk.

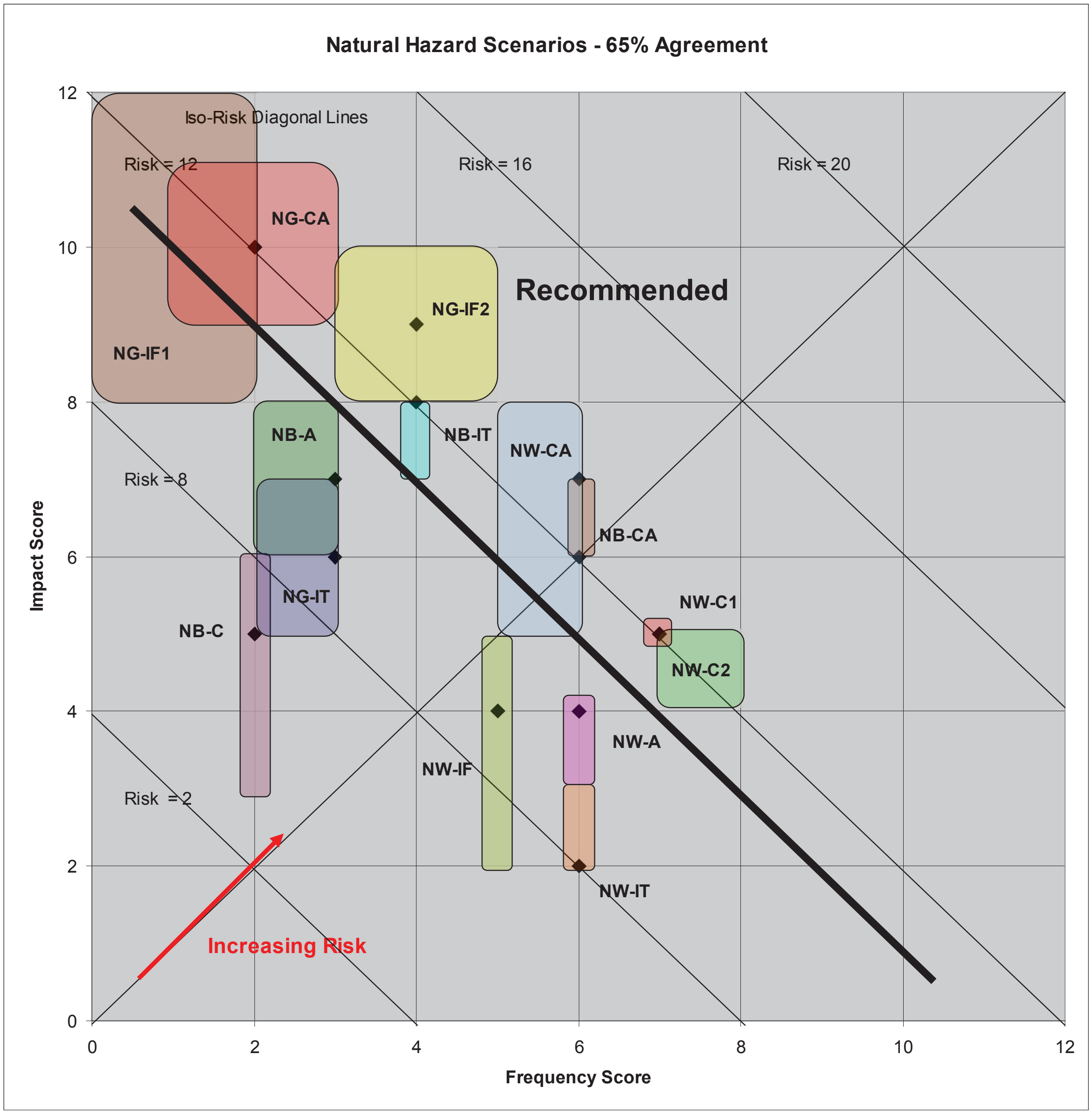
The conversion of feasibility for "intentional threat" scenarios into likelihood is an additional way to introduce errors in the scenario selection. Risk cannot be directly computed from a "feasibility" score but must be converted to "likelihood". The analysis documented here uses a "calibration" method to do the conversion. Regardless of the method used for converting "feasibility" scores into "likelihood" the high degree of uncertainty associated with the "intent" of potential threats must be taken into account when identifying which "intentional threat" scenarios should be included in the high priority scenario set. A prudent approach would be to include "intentional threat" scenarios with a lower risk threshold. In the case of the CRA, a risk threshold of "11" was chosen for non-intentional threat scenario. If this threshold risk value were chosen for the intentional risk scenarios, none of these scenarios would have been included in the high priority scenario set. The next suitable threshold risk value that does not pass through the middle the uncertainty ranges of many scenarios is a risk threshold value of "8" which represents a risk 30 times greater than that associated with a risk threshold score of "11", it is not an unreasonable prudent choice given the unpredictability of threat intentions.

Next steps

Starting with the priority set of scenarios selected through the process summarized in the present Annex, the next step in the Capability Based Planning process is the analysis of capabilities and gaps. Depending on the stakeholder/planning requirements, scenarios in the priority set must undergo further evaluation, with the goal of developing full-spectrum scenarios to aid the capability assessment across the full spectrum from prevention, protection, mitigation, through to response and recovery.

ANNEX B – WORKSHOP RESULTS

NATURAL HAZARD RISK SCENARIOS



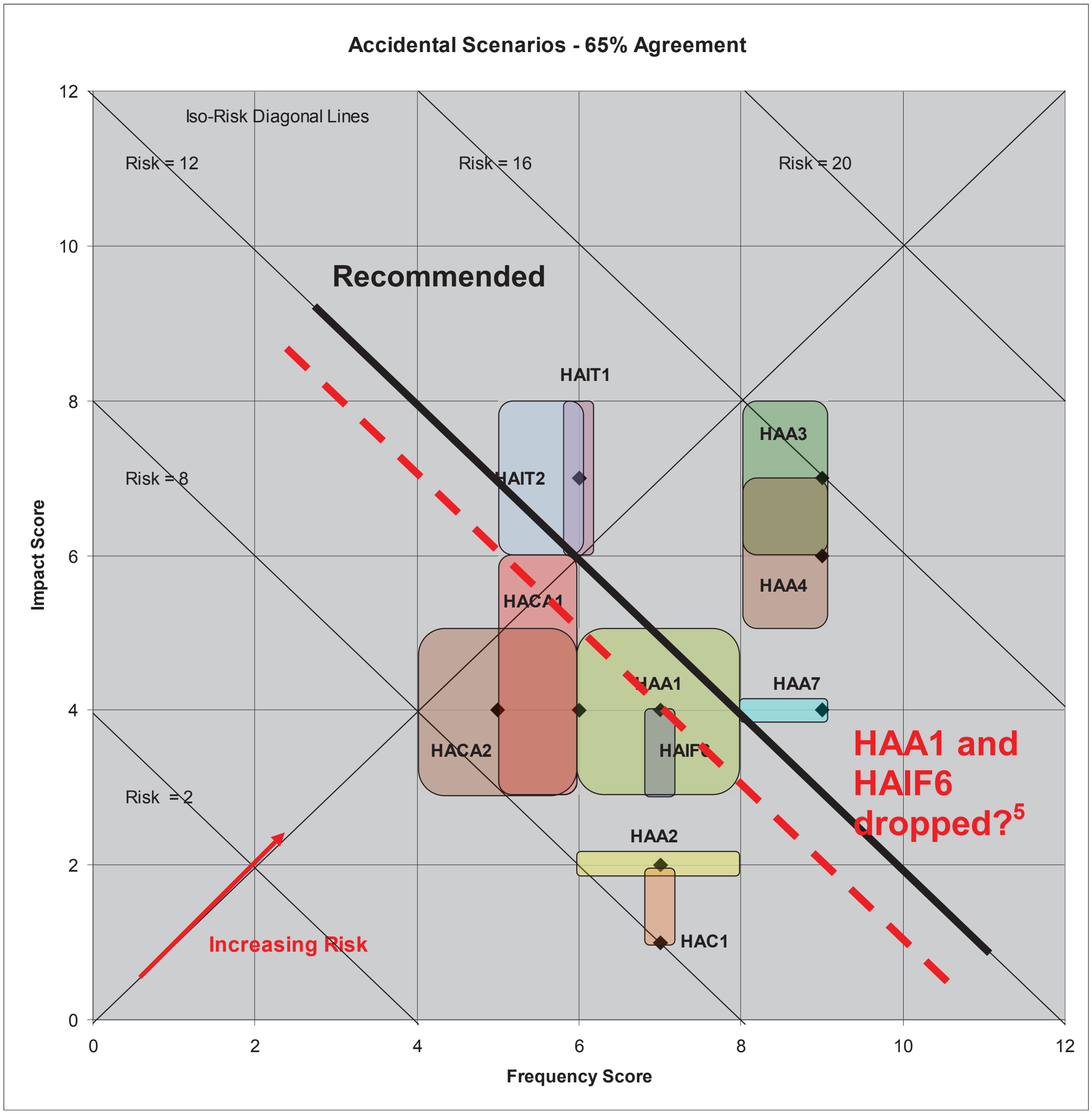
High

- NW-C1: Wildfire
- NW-C2: Extreme Rainfall
- NG-CA: Strait of Georgia EQ
- NG-IF1: Strait of Georgia EQ (IF)
- NG-IF2: Flood
- NB-CA: Severe Influenza
- NB-IT: Cascadia EQ
- NW-CA: Extreme Wind

Moderate

- NW-A: Extreme Heat
- NW-IF: Extreme Cold
- NW-IT: Extreme Snow
- NG-IT: Rock Slide on S2S
- NB-A: Cattle Disease
- NB-C: Kendall Fault EQ

HUMAN ACCIDENTAL RISK SCENARIOS



---

5 Based on the "clustering" of scenarios, the iso-risk reference line should be adjusted upwards; stakeholders should review the HAA1 and HAIF6 scenarios and decide whether they should still be included in the high priority set or dropped.

Extreme

- HAA3: Manufacturing Goods from Imported China
- HAA4: RV Fires Catches on Fire on the Upper Hwy

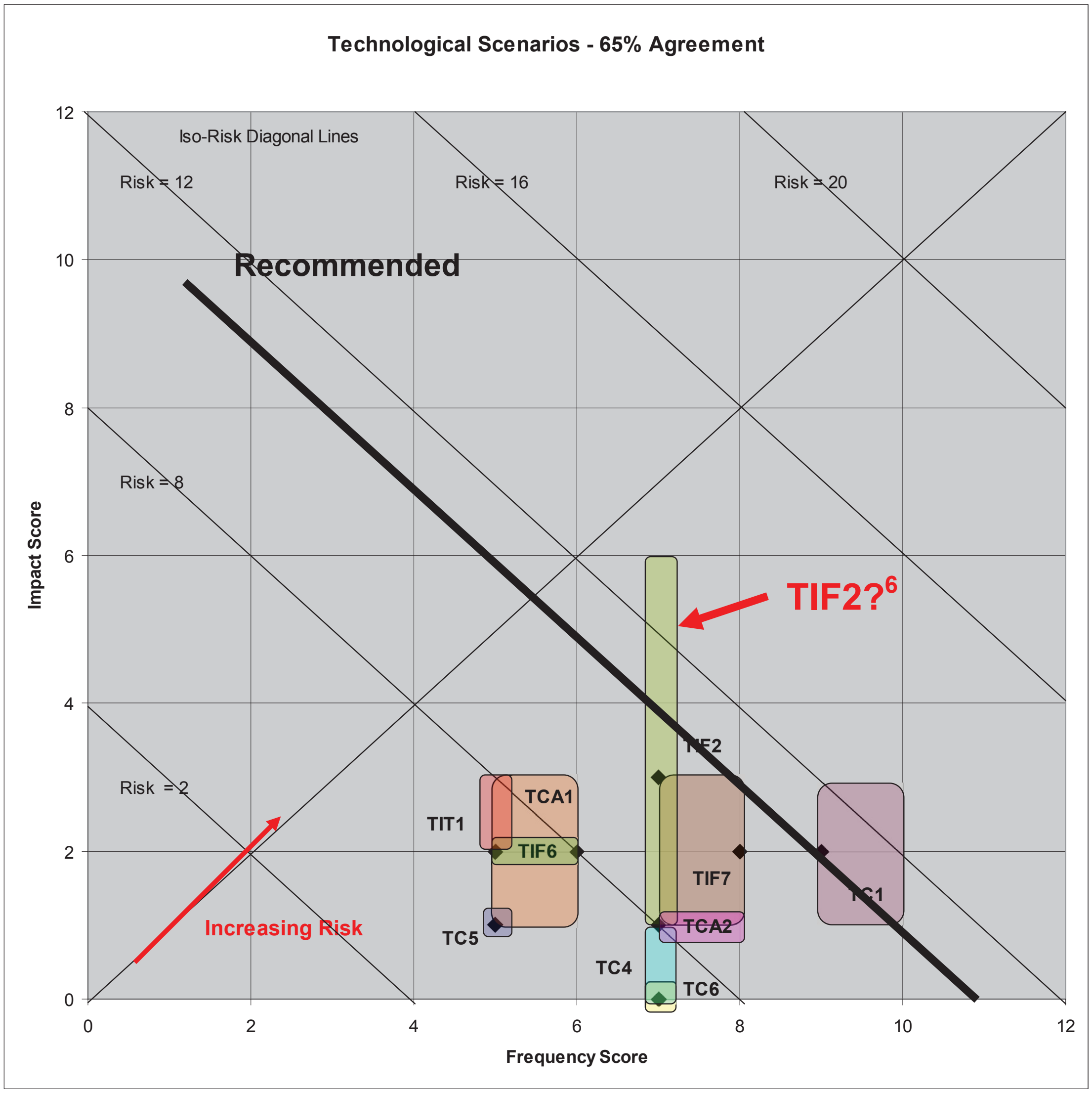
High

- HAA1: Poultry Farm Contamination with Dioxin
- HAA7: Avian Flu
- HAIF6: Release of Mercaptan from a storage facility
- HAIT1: 747 Airplane Crash
- HAIT2: Grounding of a Vessel near Lions Gate Bridge

Moderate

- HACA1: Accidental release of chlorine from a chemical plan
- HACA2: Train Derailment in Port Coquitlam
- HAA2: Lettuce Contaminated by E.Coli
- HAC1: Fire in a Main Switching Room

TECHNOLOGICAL RISK SCENARIOS



---

6 The iso-risk reference line cuts through the 65% agreement "box"; stakeholders should review the TIF2 scenario and decide whether it should be included in the high priority set.

High

- TC1: Problems connecting to Internet sites

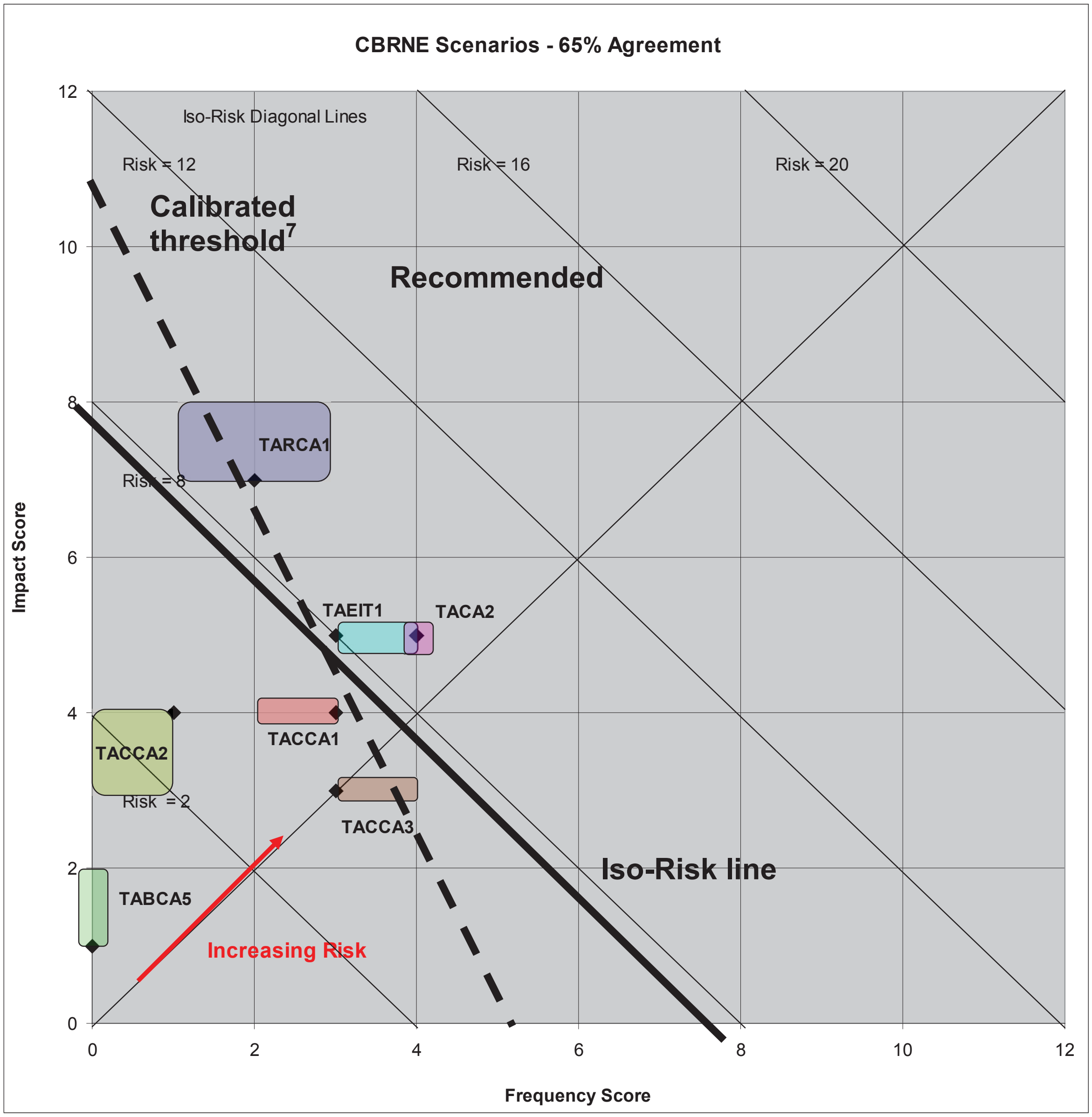
Moderate

- TCA1: An extreme weather event disrupts power to the SCADA system causing a major sewage lift station to fail.
- TIF2: Failure of the SCADA system reported inaccurate water levels
- TIF6: A processing error causes a release of chlorine gas from a plant storage tank
- TIF7: Failure of a redundant power system causing bypass of untreated sewage
- TIT1: An engine failure in a tug boat pulling a barge, impacts the rail bridge
- TC4: A piece of flawed software affects the process control system of a SCADA system
- TC6: A hardware failure to a banking processing center

Low

- TCA1: Fire downtown in a substation
- TC5: A control system failure at a liquid natural gas site

TERRORISM/CBRNE RISK SCENARIOS



[7] This represents the threshold based on impact and ***feasibility*** scores. When the feasibility score is converted to likelihood, the contour is no longer a diagonal iso-risk line. Therefore, the solid iso-risk line is used instead as a reference for selecting priority scenarios.

High

- TACA2: Feed supply mill contaminated with cyanide
- TARCA1: Explosion of a van during rush hour downtown
- TAEIT1: VB Incendiary Device, multiple attacks on major bridges in Lower Mainland

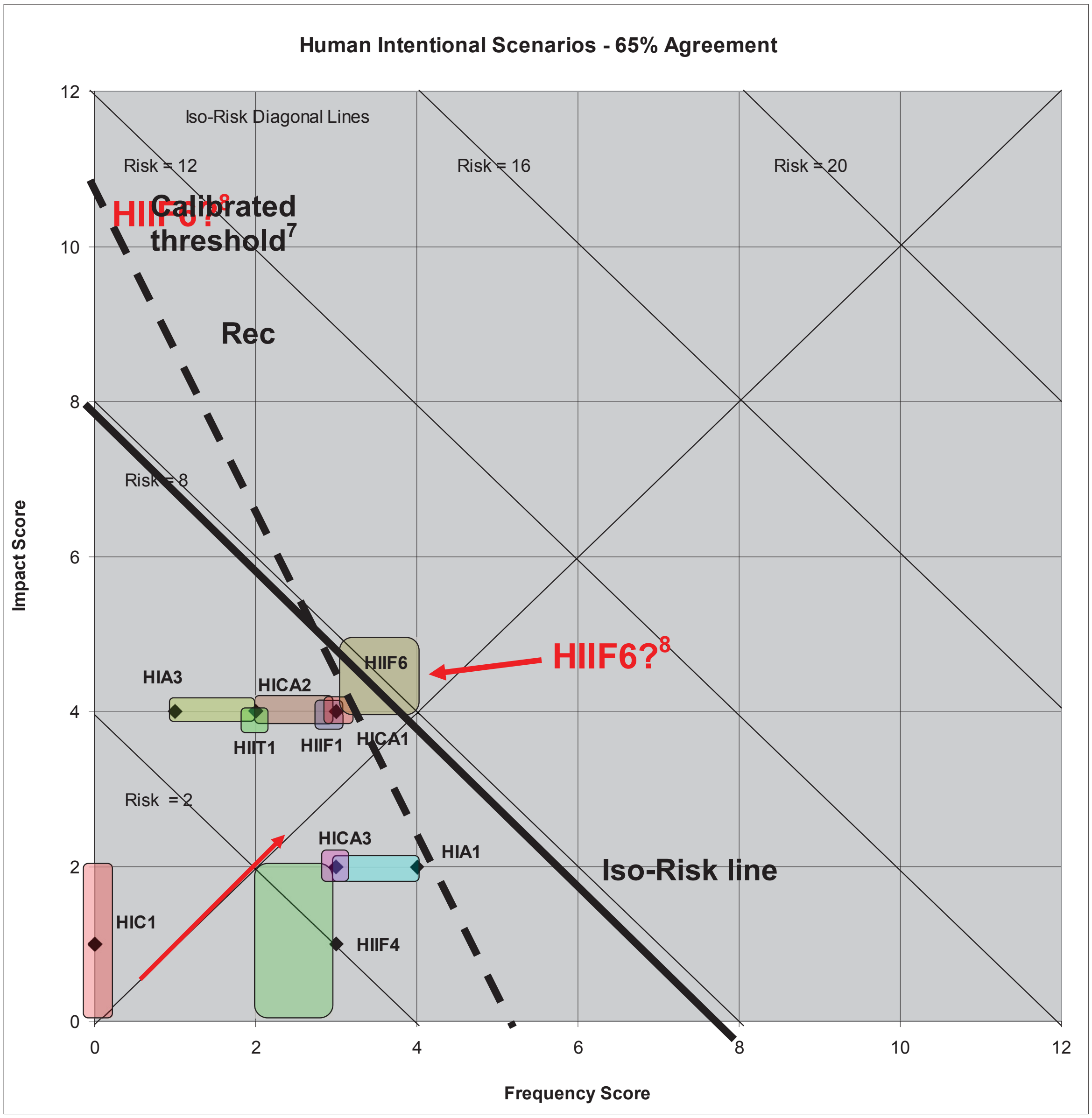
Moderate

- TACCA1: Unknown person enters YVR food court
- TACCA3: Lone wolf disperses turpentine throughout a hotel

Low

- TACCA2: Sarin released in a HVAC system at a hotel
- TABCA5: Mail containing anthrax

HUMAN INTENTIONAL RISK SCENARIOS



[8] The iso-risk reference line cuts through the 65% agreement "box"; stakeholders should review the HIIF6 scenario and decide whether it should be included in the high priority set.

Moderate

- HICA1 : An ex-spouse disseminates ricin at a restaurant
- HICA2: Off gassing through an entire neighborhood toilet system
- HICA3: Chemical Endosulfan was seeded at local parks
- HIA1: A competitor has contaminated the produce of a vegetable farmer selling his products with a rodenticide and/or pesticide
- HIIF1: Citizens walking through a Park discover an abandoned vehicle and report it
- HIIF4: The bulk milk tanks at several dairy farms are contaminated at night several hours before regular milk tanker pickup
- HIIF6: A disgruntled driver intentionally releases gasoline from two trailer tankers onto the street
- HIIT1: An individual with a personal agenda disengages the safety features
- HIC1: Copper thieves break into a manhole

Low

- HIA3: Disgruntled farm workers infect their employer's chicken farm

ANNEX C – RECOMMENDED SCENARIO SET

- **Natural Hazards**

Risk = 13
Earthquake (combined NG-IF1, NG-CA, NB-IT)
Extreme Wind (NW-CA)
Risk = 12
Flood (NG-IF2)
Severe Influenza (NB-CA)
Extreme Rainfall (NW-C2)

- **Human Accidental**

Risk = 16
Imported Insect Infestation (HAA3)
Risk = 15
Wildfire (combined HAA4, NW-C1) [Note: Also, a natural hazard scenario]
Risk = 13
Avian Flu (HAA7)
Plane Crash (HAIT1)
Vessel Grounding at Lion's Gate (HAIT2)

- **Technological**

Risk = 11
Internet Problems – DNS Disruption (TC1)

- **CBRNE**

Risk = 9 (calibrated score)
Explosive Dispersal of Radioactive Material (TARCA1)
Contamination of Feed Supply Mill (TACA2)
Risk = 8 (calibrated score)
Vehicle Borne Incendiary Device – Multiple Attacks (TAEIT1)