By Brian Philbin, Laura Brown, and Lori McKay

Intelligent Risk-Taking

A Methodology to Determine Risk Tolerance in a Non-Financial Environment

TOLERANCE TRADITIONALLY

How does your organization know which risks require attention? And for the risks that it does recognize, how much or how little? We all struggle with the amount of risk exposure we are willing to bear. The "risks du jour" always seem to be the focus of attention. However, should they?

This is what we wrestled with at the Canada Revenue Agency (CRA), which is a large, complex public institution. A methodology was needed to focus senior management's discussions on all enterprise risks—not just on the risks or hot topics of the moment. We wanted to ensure that all risks received the same consideration and were actioned (or not actioned) appropriately.

While there is no single definition for tolerance, the Treasury Board of Canada Secretariat, the department that sets policy and oversees the operations of the federal government, defines risk tolerance as the willingness of an organization to accept or reject a given level of residual risk.[1] This suggests that an organization must clarify the acceptable variance within risks that it can accept in order to achieve its objectives. Essentially, risk tolerance is the amount of risk the organization can afford to take while remaining within its resources in order to achieve expected outcomes.

There are many challenges associated with implementing tolerance in the public sector or any other non-financial environment. There were several key issues that stood out for the CRA. The first was that the definitions of risk tolerance are vague, abstract, and interdependent—which causes difficulty in fully comprehending the concept of risk tolerance. A perpetuation of this is in defining a risk tolerance statement for CRA that will satisfy different perspectives. Second, there is little or no guidance regarding sound methods for implementing risk tolerance. And, lastly, a constantly changing environment makes it difficult to set static tolerance levels.

ORIGINAL INTENT

In spite of all of these challenges, the CRA took on this task to enhance its enterprise risk management (ERM) decision-making process. The mindset was that an organization should aim at formalizing and, if possible, quantifying its tolerance level so that consistency could be applied to all risks. Rather than automatically mitigating the risks with the highest level of residual risk exposure, the focus was to be on risks that could approach or exceed the established threshold. These risks would be based on predetermined criteria in regard to their tolerance in order to proactively address them.

The intention was to capture the varying level of comfort with risk exposure in a systematic, consistent, and justifiable way. A clear reference point would be established against which risk exposure would be monitored. If risk tolerance levels were approached or breached, a discussion and appropriate action would be taken. We wanted a methodology that was scalable so that it could be used at any level—from the business unit to the enterprise. And, also one that was applicable to any type of risk: for example, strategic, business, and operational.

Our research indicated that there was no tolerance model for the public sector or for many other non-financial organizations. Therefore, we built one tailored to the CRA's need and the needs of these types of organizations.

1 Treasury Board of Canada Secretariat. *Guide to Integrated Risk Management.*

INNOVATIVE VISION

In building a tolerance model, the CRA wanted to keep the tolerance methodology simple and user-friendly, but grounded in sound principles. Numerous documents and white papers from leading private sector, public sector, advisory/consultation/research organizations and international tax organizations, laid the foundation for this research. Interviews were conducted with senior management from several public sector organizations to share their leading practices and lessons learned.

The CRA developed a risk tolerance tool to predict the maximum level of exposure that management would be willing to accept. This would be a way to inform the discussion on risk responses. We determined the qualities that tend to contribute to management's level of comfort to risks. These four qualities are described as risk tolerance criteria and, at the enterprise level, currently include:

1. interconnectivity
2. criticality/government priority
3. sensitivity
4. span of control.

Also included is a constant base factor (criterion # 5), which is the same for all risks and reflects the fact that CRA is not fully tolerant of any risk. (It should be noted that different criteria may be more appropriate for more granular or focused areas of risk that are subject to assessment.)

We began to develop the methodology in 2012 using principles of factor analysis and historical data from the 2011 CRA Corporate Risk Profile to determine how influential each of the criteria were in determining the risk response. The result was a specific weighting for each tolerance criteria.

When weighted and combined, these criteria produce an expected value for the residual risk exposure. This expected value represents the point above which the CRA has typically decided to mitigate risks. That is to say, the expected value represents the maximum level of exposure that senior management would be comfortable accepting.

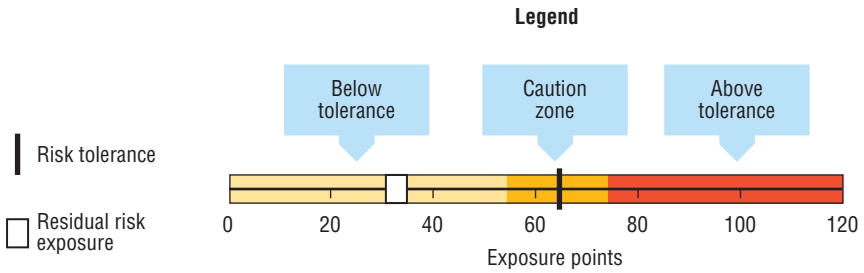
Once the risk tolerance level (expected exposure value) is established, the residual risk exposure (actual exposure value) can be compared to it (both based on 120-point scales). If the level of residual risk exposure is above the risk tolerance level, the risk will be recommended for mitigation. Conversely, if the level of residual risk exposure is below the risk tolerance, it will be recommended that the risk is accepted and the environment monitored for significant changes. If a risk is well below the tolerance threshold, it may be a candidate for taking additional, intelligent risk-taking in the form of, say, increased innovation. Exhibit 1 depicts the relationship between risk tolerance and residual risk exposure.

To ensure tolerance levels remain accurate, all levels are re-evaluated at least every two cycles. As well, if there are changes in the operating environment impacting one or more of the risk tolerance criteria, an ad hoc reassessment would be conducted. The simplicity of the tool allows tolerance levels for a given risk to be reviewed at any time.

INTO PRACTICE

Tools aren't made to sit on the shelf or be concealed in the toolbox. We wanted to test the tolerance model, perfect it, and incorporate it into our risk management process. That said, we piloted it through the corporate risk profile exercise the following year. The expected and actual residual risk exposure values for each risk were calculated in the evaluation phase of the risk assessment.

Exhibit 1
Essence of Risk Tolerance



Source: Enterprise Risk Management Division, Canada Revenue Agency.

Table 1
Risk Tolerance Calculation

Interconnectivity (10 exposure points) • Scoring is based on risk interconnectivity.	• High (10 points)—risk has seven or more interconnections • Medium (5 points)—risk has four to six interconnections • Low (10 points)—risk has three or fewer interconnections
Criticality/government priority (30 exposure points) • Scoring is based on critical services and Government of Canada (GoC) priorities	• High (0 points)—risk directly relates to critical services or GoC priorities • Medium (15 points)—risk indirectly relates to critical services or GoC priorities • Low (30 points)—risk does not relate to critical services or GoC priorities
Sensitivity (30 exposure points) • Scoring is based on the potential level of sensitivity of the general public and media, if the risk was to materialize.	• High (0 points)—risk is of a highly sensitive nature • Medium (15 points)—risk is of a somewhat sensitive nature • Low (30 points)—risk is not of a sensitive nature
Span of control (30 exposure points) • Scoring is based on the level of control the organization has over the risk.	• High (0 points)—risk is mostly within the organization's span of control • Medium (15 points)—risk is partially within the organization's span of control • Low (30 points)—risk is mostly beyond the organization's span of control
Base factor (20 exposure points) • Scoring is consistent for all risks and is based on the fact that the organization is not fully tolerant to any enterprise risks.	• All risks receive 0 points out of 20

Source: Enterprise Risk Management Division, Canada Revenue Agency.

For the expected value, each risk began with zero points. And, using the risk tolerance criteria identified above, we added points based on the scoring outlined in Table 1. A 120-point scale was used: the lower the points, the lower the tolerance.

The actual residual risk exposure is then calculated. This was determined by combining the residual risk exposure (likelihood x impact) and trend in risk exposure scores for a maximum of 120 exposure points. The determination of both these scores is defined in the Table 2. Thus, the actual calculated residual risk exposure score is compared with the risk tolerance score using comparable scales. An example can be found in the table in Appendix A.

A significant feature of this methodology is that it can be modified depending on the organization's needs. It is scalable and can be utilized at any level, from the enterprise to the program or project level. As well, any set of relevant criteria can be used to reflect differing environments, and the weights of each criterion can be calibrated individually and modified over time.

The benefits of the results obtained were numerous. Appropriate risk response recommendations can be made to senior management for each risk. Our logic was based on evidence rather than a subjective reaction to current events. We did not automatically mitigate the highest risks, but did mitigate risks that were approaching or beyond the established tolerance threshold, based

Table 2
Residual Risk Exposure Calculation

Residual risk exposure • Scoring is based on the level of exposure of the organization given the current preventative and remedial controls.	• For each risk, the residential risk exposure is calculated as the product of the residual risk likelihood and the residual risk impact (converted to a scale of 100) as assessed by management.
Trend in risk exposure (±20 exposure points) • Scoring is based on the anticipated change in residual risk exposure over the next 12 to 18 months if controls are maintained at their current levels.	• For each risk, scoring is calculated leveraging the assessment of trend in risk exposure conducted by management: – (-20 points) to risks whose residual risk exposure is expected to *decrease* over the next 12 to 18 months – (+20 points) to risks whose residual risk exposure is expected to *increase* over the next 12 to 18 months – (0 points) to risks whose residual risk exposure is expected to *remain stable* over the next 12 to 18 months.

Source: Enterprise Risk Management Division, Canada Revenue Agency.

on predetermined criteria. In fact, certain risks that would not have received management's attention based solely on risk exposure were addressed when their tolerance level was taken into account. The knowledge of CRA's tolerance level allows us to have sound conversations around the risks whose exposure is approaching or beyond its tolerance level.

This structured approach to enterprise risk tolerance promotes consistency in decision-making. Unless there are important changes in the environment, risk tolerance levels should remain fairly stable over time, which creates an understanding throughout the organization. Employees thus have tangible grounds to better understand the Agency's approach toward risks, which reinforces a risk-aware culture and informed, intelligent risk-taking.

DRIVING INTO THE FUTURE

A successful pilot phase led to implementing the tolerance methodology into our risk management process. Still, it didn't stop there. Knowing that this tool was fairly unique, we shared it as part of the ERM program's vision: "ERM for the broader CRA community." Tailored risk tolerance models have been developed for major projects and programs within the Agency for the past four years and guidance material is available on the CRA's intranet. The tool also provided value in helping to determine risk-based resource allocation decisions to avoid over-investing in adequately controlled areas (or to engage in additional innovation). This allowed resources to be directed to risks that may be approaching unacceptable levels. In addition, we have had consultations and discussions on the methodology with other government departments and international partners.

Being innovative is at the core of what we do. We intend to evolve and refine our methodology further by, in particular, focusing on measurable indicators to determine both risk tolerance and exposure, which will contribute to even greater intelligence in risk management.

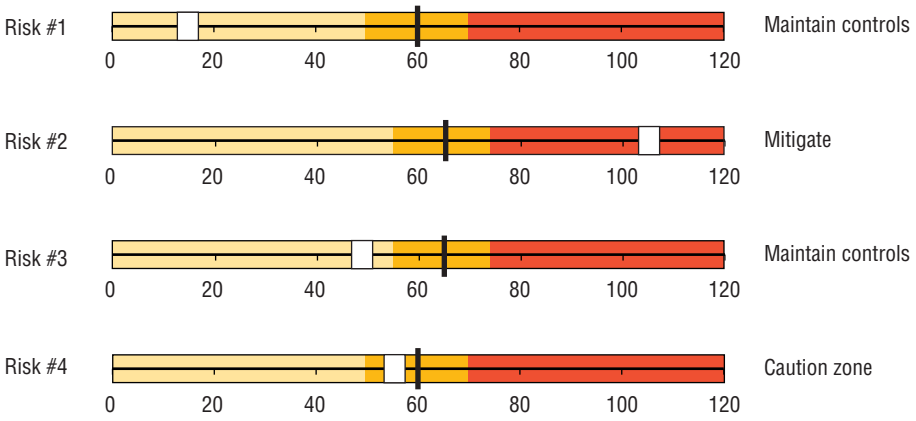
BIBLIOGRAPHY

Treasury Board of Canada Secretariat. *Guide to Integrated Risk Management*. Government of Canada, n.d. www.tbs-sct.gc.ca/tbs-sct/rm-gr/guides/girm-ggirpr-eng.asp.

APPENDIX A

Table 1
Risk Tolerance Illustration

	Risk tolerance criteria						Residual risk criteria			
Risk name	Interconnectivity 10 pts	Criticality government priority 30 pts	Sensitivity 30 pts	Span of control 30 pts	Base factor 20 pts	Total risk tolerance score (expected value) 120 exposure points	Residual risk exposure[1] 100 pts	Trend in risk exposure ± 20 pts	Total residual risk score (actual value) 120 exposure points	Recommendation
Risk #1	0	30	30	0	0	60	16	0	16	Maintain controls
Risk #2	5	30	30	0	0	65	86	20	106	Mitigate
Risk #3	5	30	30	0	0	65	70	-20	50	Maintain controls
Risk #4	0	30	0	30	0	60	55	0	55	Caution zone



Source: Enterprise Risk Management Division, Canada Revenue Agency.

Risk #1 has high interconnectivity resulting in zero exposure points. It is not a critical service or a government priority, so we assign 30 exposure points. The level of sensitivity is low, which allocates another 30 exposure points. The span of control is mostly within the organization's control. Therefore, zero exposure points are added. Taking into account the base factor, the expected value of the total risk tolerance is 60 out of 120. The organization's actual residual risk score is calculated by adding the residual risk exposure, which is 16, to the trend in risk exposure. In this case, it is zero as this risk is expected to remain stable over the next 12 to 18 months, which totals 16. Comparing these two values informs us that the actual residual risk exposure is significantly below the acceptable risk tolerance. Therefore, the recommendation would be to maintain current controls and monitor the environment.

Brian Philbin
Assistant Commissioner,
Audit, Evaluations, and Risk
Branch, and Chief Audit
Executive
Canada Revenue Agency

Brian Philbin is the Assistant Commissioner of the Audit, Evaluation, and Risk Branch, and the Chief Audit Executive for the Canada Revenue Agency (CRA). He is responsible for providing strategic advice and executive oversight with respect to horizontal and integrated enterprise risks. Brian also directs a robust, independent, internal audit and program evaluation function across the CRA. In addition, he plays a key role in supporting major strategic and change management initiatives within the Agency. Brian Philbin is a chartered professional accountant with over 25 years of public and private sector experience in enterprise and operational risk management, internal and external audit, finance, operations, technology, strategic planning, compliance, and governance.

Laura Brown
Assistant Director, Corporate
Risk Management, Enterprise
Risk Management Division
Canada Revenue Agency

Laura Brown is the Assistant Director of the Corporate Risk Management section within the Enterprise Risk Management Division at the Canada Revenue Agency. She is responsible for supporting the effective management of enterprise risks and the use of sound risk intelligence at the enterprise level through the development of the CRA's Corporate Risk Profile (CRP). This includes supporting the development and monitoring of the implementation and performance of enterprise risk action plans; reporting to the key stakeholders on the status of enterprise risks; and working with key corporate stakeholders to ensure that the CRP informs the CRA's planning and reporting processes. Laura holds a MA in sociology with a concentration in quantitative methods and a professional certificate in risk management. She has over 10 years of public sector experience in risk management, project management, business planning, and corporate policy.

Lori McKay
Analyst, Enterprise Risk
Management Division
Canada Revenue Agency

Lori McKay is an Enterprise Risk Management Analyst in the Corporate Risk Management section within the Enterprise Risk Management Division at the Canada Revenue Agency. She is responsible for the development of the CRA's Corporate Risk Profile; monitoring and reporting on the status of risk action plans; sharing and developing risk management best practices through engagement and relationship-building with other tax jurisdictions; and analyzing social, economic, and other relevant statistics and data pertaining to planning, risk management, and performance measurement. Lori also contributes to the development of corporate position papers, briefings, and presentation materials for senior executives in the Agency on matters relating to risk management. Lori holds an MBA from Queen's University. She has over 16 years of public sector experience in risk management, strategic planning, and program analysis.