# National Risk Management

## A Practical ERM Approach for Federal Governments

April 2018

CAS
Canadian Institute of Actuaries
Institut canadien des actuaires
SOCIETY OF ACTUARIES®

# National Risk Management

## A Practical ERM Approach for Federal Governments

**AUTHOR** Sim Segal, FSA, CERA

## ACKNOWLEDGMENTS

The author would like to acknowledge the extensive assistance—in the form of guidance, oversight, insights, commentary and edits—generously provided by the Project Oversight Group, most of whom serve on a volunteer basis. Without their efforts, this white paper would not have been possible.

Project Oversight Group Members:

Jill Knudsen, Chair

Victor Chen

Helmut Engels

Nancy Ning

Shannon Patershuk

Tianyang Wang

Ella Young

David Schraub, SOA staff

Jan Schuh, SOA staff

Ronora Stryker, SOA staff

# CONTENTS

## SPONSORS' PERSPECTIVE

The Canadian Institute of Actuaries, Casualty Actuarial Society, and Society of Actuaries engaged SimErgy to develop a white-paper on the application of enterprise risk management (ERM) at a national government level and examine the potential role of a national risk officer. Although there is considerable literature on the benefits of ERM, it is typically targeted at large, global corporations in the financial sector. An objective of this project is to develop a potential framework for national enterprise risk management to enhance and advance ERM practice and to serve the public beyond its traditional applications in the financial sector.

## AUTHOR'S PERSPECTIVE

**In this white paper, the author, Sim Segal, FSA, CERA, presents his perspectives on a practical enterprise risk management (ERM) approach for national risk management, that is, ERM at the federal[1] government level. This is based on the author's**

- Consulting experience in both the private and public sectors
- Value-based ERM approach—a synthesis of value-based management and enterprise risk management—first introduced in *Corporate Value of Enterprise Risk Management: The Next Step in Business Management,* authored by Sim Segal and published by Wiley in 2011 (ISBN-13: 978-0470882542)
- Research studies conducted separately from efforts supporting this white paper
- Research, including interviews with federal government employees and vendors, conducted in support of this white paper

These views are solely those of the author of this white paper, and do not necessarily represent those of the organizations sponsoring this effort.

# EXECUTIVE SUMMARY

This paper presents a value-based approach to ERM and discusses how federal governments can use it to support risk-reward decision making at the highest levels of government and increase the chances of achieving critical national goals. Value-based ERM provides a key link between risk and reward using a robust yet practical approach that is easier to implement and maintain than current ERM methods widely in use. The paper provides guidance—step-by-step procedures, implementation tips and red-flag cautions—to federal governments on how to adopt this approach.

The first three sections are brief and set the stage by introducing and defining the topic. Sections 4 through 7 discuss the approach, walking through each of the four ERM process cycle stages. Section 8 describes how the ERM program can easily be maintained once it is implemented. The last two sections present comments on the role of a national chief risk officer (NCRO) and some positive trends in national risk management.

# 1 INTRODUCTION

## 1.1 WHAT IS ERM?

ERM is a process that organizations use to identify, measure, manage, and disclose key risks to increase value to stakeholders. When done properly, ERM informs better risk-reward decision making, increases the likelihood of achieving strategic plan objectives and enhances the efficiency and effectiveness of allocating resources.

Though ERM is relatively new, private-sector organizations—corporations as well as non-corporate entities such as nonprofits—have been implementing ERM programs for many years. However, more recently, governments have begun to design and implement ERM programs at both the agency and national levels.

## 1.2 WHY SHOULD ERM BE APPLIED AT THE NATIONAL LEVEL?

To see why ERM is needed at the national level, consider the following question: If you were given the entire national budget and had the freedom to use it any way you wanted, how would you allocate the funds? This question starts you down a path of having to clarify the following additional questions:

1. What are our critical national objectives?
2. What are our key metrics for success (that is, for achieving critical national objectives)?
3. What are the key risks (that impact our key metrics)?
4. What are the quantitative impacts (and likelihoods) of the possible risk scenarios for each key risk?
5. What decisions can we make to increase the likelihood of success?

Once questions 1 and 2 are answered, ERM can help us answer the rest. Using an ERM process to think through and address questions 3 through 5 provides the following benefits at the national level:

1. **Forecasts.** Improves forecasts—baseline as well as confidence ranges around various levels of over- or underperformance—in part by extracting and leveraging information from subject matter experts
2. **Simulations.** Uses a more rigorous simulation tool to enhance ability to understand the integrated impact of potential changes in the national or global situation on critical national objectives
3. **Prioritization.** Improves focus on the most important threats—individual and combination (two or more simultaneous events)—with a quantitative model that captures the full impact of events (including offsetting or exacerbating effects)
4. **Decision making.** Enhances decision making, based on a more robust and integrated picture of potential impacts of decisions—ranging from strategic planning to budgeting to risk mitigation
5. **Success.** Increases the likelihood of achieving critical national objectives

## 1.3 HOW SHOULD ERM BE APPLIED AT THE NATIONAL LEVEL?

Most governments that have begun implementing ERM programs have chosen one of the two most common frameworks—either COSO[2] ERM or ISO[3] 31000—or some adaptation of these as their ERM framework. In terms of how they function in practice, these approaches are not materially different, so for convenience, this paper will refer generally to "the current ERM approach," "current

ERM practices" or something similar. While the current ERM approach has advanced some ERM practices (for example, risk mitigation), the fabric of its design can inhibit ERM programs from achieving their primary goal: to better inform risk-reward decision making.

This paper describes an ERM approach suitable for national government enhancing the most important risk-reward decisions at the highest levels of government. As the sections illustrate the steps to implement this ERM approach, they also compare aspects of this approach to current ERM practices and highlight implementation tips and red-flag cautions involving the critical activities in the ERM process.

## 1.4 NATIONAL ERM VERSUS AGENCY ERM

The primary purpose of this paper is to provide a practical ERM framework that governments can implement at the national level. However, individual government agencies can also apply this approach; implementation is easier at the agency level because there are complexities that apply only at the national level.

A national-level ERM program can be implemented on its own, although if all major government agencies also implement ERM on a consistent basis, the work can be leveraged to support the work at the national level.

## 1.5 ERM FRAMEWORK VERSUS RISK GOVERNANCE

ERM infrastructure comprises risk governance and an ERM framework. Risk governance is concerned with defining the specific roles and responsibilities, organizational and reporting structures, detailed policies and procedures and so on. The ERM framework addresses the questions of what ERM activities should take place, in what sequence, with what inter-relationships and how they should be performed. This paper focuses mainly on the framework—the how-to aspect of ERM. Risk governance is important, but less so than the ERM framework, which correlates more closely with ERM excellence than does risk governance. There are organizations with minimal and informal risk governance structure (particularly, early in their ERM evolution) that have achieved much ERM success; conversely, there are organizations with detailed, formalized risk governance structures, yet with little or no ERM successes. In addition, a strong ERM framework enhances risk governance; only after an organization effectively integrates ERM activities can it properly inform how to shape an effective formal risk governance structure.

## 1.6 PRACTICAL HURDLES

Some practical hurdles should be acknowledged, considered and addressed when applying ERM to government entities, and it is worthwhile to briefly discuss some of the most important obstacles: political forces, silos and vendors.

### 1.6.1 Political Forces

While it can be argued that the near-term heat of political battles often supersedes the kind of decision making informed by an ERM program, there are two main reasons why ERM is nevertheless valuable:

1. There are pockets within a national framework where such forces tend to be less of an impediment. These may include
    a. Government agencies or departments that have relatively stable budgets from year to year and involve more routine and/or less controversial activities
    b. Initiatives with a high level of consensus urgency, such as national defense in times of war or responses to natural disasters

2. Transparent public disclosures of appropriate ERM information can generate the public support needed to overcome resistance to actions.

### 1.6.2 Silos

Often, the scope of government agencies has been limited, by design, to their own stated goals, activities and budgets. This means that (1) they may not be afforded an overarching view of the impact of their actions or risks on the overall national government, and (2) they may have incentives to maintain or increase their budgets by spending all of it each year. These silo structures and incentives can impede the collection of unbiased ERM information. For example, if ERM information might reveal that budgetary funds should be shifted from one agency to another, the agency losing funds might bias the ERM information it provides in a conscious or unconscious attempt to avoid this loss of money/control. These forces are also present (though to a lesser degree) in corporate ERM efforts, and there are techniques embedded in an effective ERM approach that combat this type of bias. One such technique is the documentation and sharing of risk scenarios during the risk scenario development portion of risk quantification; the transparency of this activity reduces bias, because subject matter experts are aware that their risk scenarios will be viewed, vetted and challenged by others.

### 1.6.3 Vendors

Another challenge is present wherever government relies too heavily on vendors as the only subject matter experts in one area. In such situations, it may be difficult to extract the required unbiased information during both risk identification and risk quantification. Additional care must be taken to identify and scrutinize this information during the ERM implementation and review processes.

## 1.7 DEFINITIONS

ERM terminology and definitions vary. In this paper, when we use a term that may have a variety of definitions in the market, we will clarify by defining it. For expediency, we do not point out the other usages, but rather attempt to clarify our intended meaning.

# 2 DEFINING RISK IN AN ERM CONTEXT

Common ERM practice is to define risk as a loss, or downside event, and usually as an extreme loss. This narrows the focus and inhibits the usefulness of ERM efforts. Extreme downside events are only a small part of the day-to-day concerns of an organization. In addition, decisions cannot be made solely based on exposure to extreme downside events.

In an ERM context, *risk* should be defined as any event—upside or downside—that results in a deviation from baseline strategic plan ("Plan") objectives. This is the lynchpin that directly connects ERM to decision making and the day-to-day concerns of the organization; everyone is concerned with achieving Plan goals. This allows ERM to provide information on both sides of the risk-return equation, which is necessary for decision making.

TIP #1: Define risk as any deviation (up or down) from strategic plan expectations to enhance risk-reward decision making.

# 3 THE ERM PROCESS

The ERM process involves the process cycle steps listed below:

- Risk identification
- Risk quantification
- Risk decision making
- Risk messaging

This is a continuous process cycle and is illustrated in Figure 1.

FIGURE 1: ERM PROCESS CYCLE




Sections 4 through 7 will discuss how to implement this ERM approach initially, going through each process cycle step and its activities. Section 8 will discuss how to maintain this ERM approach on an ongoing basis. The bulk of the activities relate to the initial implementation; once set up, the maintenance can be performed relatively easily.

# 4 RISK IDENTIFICATION

The risk identification process cycle step consists of three activities:

- Risk categorization and definition (RCD)
- Qualitative risk assessment (QRA)
- Emerging risk identification

## 4.1 RISK CATEGORIZATION AND DEFINITION (RCD)

At the outset, it is important to develop a risk categorization and definition (RCD) tool. The RCD tool is a list of categories and sub-categories of risks along with their definitions. This tool has many applications throughout the ERM process, but its overarching purpose is to provide a single, consistent language for discussing risk throughout the organization. Typically, risk means many different things to different areas of government and even within agencies or functional areas. The RCD tool brings unification and cohesion to the dialogue which, importantly, translates into a consistent set of ERM activities. This is critical to an ERM program.

### 4.1.1 Level of Granularity

In current ERM programs, risks are sometimes categorized at an inconsistent level of granularity, with some set at too high a level (such as "strategic risk") and some at too low a level (such as "loss of key personnel in area X"). Either can result in failure to identify risks due to the omission of sub-categories either beneath a "too-high" categorization or above a "too-low" categorization. The RCD tool must categorize risks at a consistent level of granularity to avoid these issues.

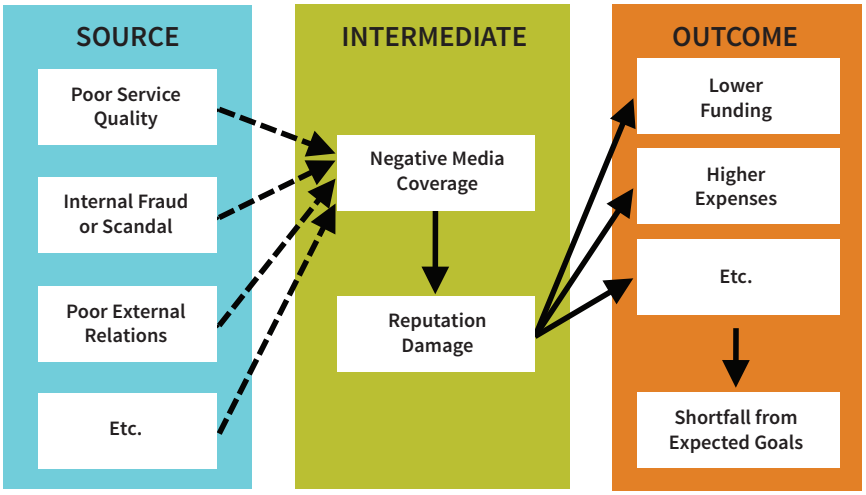
### 4.1.2 Defining Risks by Source

In most current ERM programs, risks are not consistently defined by source; rather, they are defined sometimes by source and other times by outcome. Failing to consistently define risks by source typically causes critical damage to risk identification and risk quantification.

Risks that are not clearly defined by their originating source cause confusion among qualitative risk assessment (QRA) participants and render the results of the risk identification process unreliable. Consider the following example. Many ERM programs have "reputational risk" on their key risk list. This is not a *source* of risk but an intermediate outcome. There are many different independent sources of risk—poor service quality, internal fraud or scandal, poor external relations, and so on—that (in an extreme scenario) can trigger media coverage. This can do temporary or lasting damage to the organization's reputation, which can hurt it through lower funding, higher expenses and so on and can ultimately result in a shortfall from goals (Figure 2). When QRA participants are asked to provide likelihood and severity scores for "reputational risk," they each may imagine a different source of that risk. Such scores should not be aggregated, because they do not reflect the group's impression of a single risk source. Instead, each risk source must be identified and explored separately. Many current ERM programs do not recognize this problem, and as a result, their risk identification process may fail to identify the appropriate set of key risks.

Failure to define a risk by its originating source also subverts the risk quantification process. The risk scenarios developed from an intermediate outcome exclude other streams of impact that flow from the original triggering event (Figure 3). A risk scenario

FIGURE 2: REPUTATION DAMAGE IS AN INTERMEDIATE IMPACT





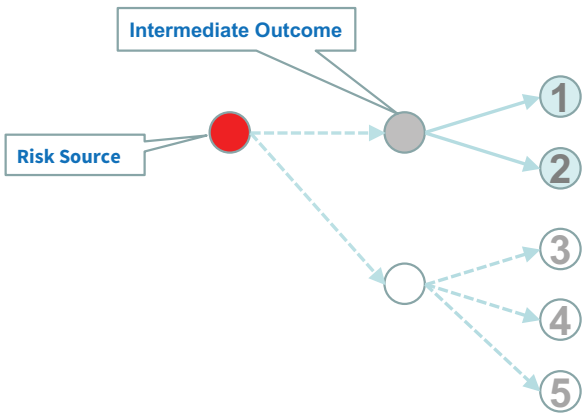

developed from a risk defined by an intermediate outcome may capture impacts 1 and 2 but fail to capture impacts 3, 4 and 5. These additional impacts may be exacerbating or offsetting, but either way, the risk quantification can be dangerously inaccurate, potentially resulting in a failure to prioritize the largest threats.

### 4.1.3 Nomenclature

A question often arises as to whether the RCD tool's risk categories and sub-categories should match those of other organizations. This is not an important issue, because there is no single standard, and each organization must develop a customized RCD tool that is suitable for its needs. However, three guidelines should be followed when creating and using the RCD tool:

1. All categories and sub-categories of risk should be included. It is unimportant, for example, whether the risk of losing a key leader is categorized within "Operational—Human resources" or "Strategic—Governance." What does matter is that the risk is captured. This should not be interpreted as insisting that the RCD tool be a comprehensive list of risks, because that is impossible; many individual risks cannot be known in advance. However, the RCD tool should be all-inclusive in that it must have a category/sub-category for all individual risks that are known to the organization.
2. Internal to the organization, the RCD tool should be used to create a uniform risk language, so there is a consistent enterprise-

FIGURE 3: RISK SOURCE NEEDED TO CAPTURE ALL DOWNSTREAM IMPACTS






TIP #2: Define risks consistently by source for reliable risk identification and risk quantification processes.

wide understanding of risk definition and categorization.

3. When communicating risk-related matters to external stakeholders, the RCD tool should be mapped/translated into the risk terminology used by the external stakeholders to avoid miscommunication.

## 4.1.4 Developing the RCD Tool

The RCD tool is developed by answering—at a high level (the category/sub-category level, not the individual risk level)—the question "What key risks do we face?" This question can only be asked and answered after the following two questions are addressed:

1. What are the critical national objectives?
2. What are our key metrics for success?

It is necessary to address these questions first, because in our ERM approach, we define risk as deviation (up or down) from achieving baseline strategic plan expectations, expressed as projected results in the form or one or more key metrics, for each objective. Our ERM approach can be applied to any entity if, and only if, the entity objectives and associated metrics can be stated clearly. For example, assume that ERM is applied to a government project with an objective of improving economic output, where the key metric is gross domestic product (GDP), and the baseline expectation is a permanent 3.0% annual improvement in GDP. In this example, risk would be defined as any event that could result in the project's achieving less than (or more than) a 3.0% annual increase in GDP (in an ERM context, risk includes both downside and upside deviations).

This is more straightforward for organizations where this information is already clearly defined. For example, some government agencies have objectives that are relatively well defined and may be relatively stable from administration to administration, and their metrics and corresponding baseline values expected for the coming period(s) are also well established in their Plan. Doing this for a nation is arguably among the most complex versions of this exercise due to variations in opinions even about what should be in the scope of the critical national objectives. Though challenging, once we complete this exercise of thinking through how to apply our ERM approach at the national level, this will then more easily instruct simpler applications of the same concepts, such as implementing ERM at individual government agencies.

### *4.1.4.1 What Are the Critical National Objectives?*

Calling the question "What are the critical national objectives?" a challenging one is an understatement. Certainly, this varies by country, but even within a country, the citizenry may have disparate factions with diverging views of the priorities that should be placed on different objectives or even on the appropriate level of federal government involvement. Here, we select a set of critical national objectives merely to allow us to illustrate the application of our ERM approach; readers are encouraged to imagine any set of critical national objectives they deem most appropriate for their country and from their perspective.

We will narrow our focus to an overarching small and manageable set of objectives. The primary reason for this is practicality, to limit the number of corresponding metrics that must be considered in the ERM process. Risks must be assessed—first qualitatively and then quantitatively—in

TIP #3: Limit the number of key objectives to a small and manageable number for practicality and focus.

terms of impact on each key metric. An excessive number of metrics would impede the process. A secondary reason is that a small set of objectives focuses efforts exclusively on key risks, which are those that represent the critical threats (and opportunities) rather than lesser concerns.

For illustrative purposes,[4] we will define the critical national objectives as follows:

1. **Life**—protect lives of citizens
2. **Health**—protect/enhance health of citizens
3 **Wealth**—provide opportunity for citizens to financially support needs/wants
4. **Sovereignty**—maintain/enhance level of independence from foreign influence

Even for these basic four objectives, different countries will have different opinions on both the relative importance of each objective and the level to which the federal government should be directly involved in each objective. For example, there is a high level of consensus among Canadian citizens that the Canadian federal government should support the health objective, whereas the U.S. citizenry is currently divided on how this responsibility should be split between the federal government, state governments, and citizens themselves.

TABLE 1: LOWER-LEVEL OBJECTIVES MAP INTO HIGHER-LEVEL OBJECTIVES

| These Lower-Level Objectives | Map into These Higher-Level Objectives |
|---|---|
| Maintain quality of food and water supply | **Life**—protect against spread of disease that can lead to death<br>**Health**—protect against spread of disease that can lead to illness |
| Maintain air quality | **Life**—protect against pollutants that can lead to death<br>**Health**—protect against pollutants that can damage health<br>**Wealth**—attract foreign talent and investment |
| Maintain demographic balance: working vs. nonworking citizens | **Wealth**—avoid overtaxing working citizenry |
| Maintain favorable national credit rating | **Wealth**—protect against devaluation of the national currency and keep portion of taxes servicing debt to a manageable level<br>**Sovereignty**—maintain ability to borrow in times of war or threat of war |
| Maintain low unemployment | **Wealth**—protect citizenry's ability to find employment to support needs/wants |
| Grow economic output | **Wealth**—increase economic opportunities for citizenry and domestic corporations |
| Negotiate and enforce trade agreements with other nations | **Wealth**—increase economic opportunities for citizenry and domestic corporations<br>**Sovereignty**—increase ability to obtain critical resources unavailable internally |
| Educate the population | **Wealth**—maintain/enhance ability of working population to compete in global market |
| Maintain transportation infrastructure | **Life**—lower number of deaths via enhanced transportation safety<br>**Health**—lower number of injuries via enhanced transportation safety<br>**Wealth**—increase economic output via enhanced flow of commercial goods and human capital |

CONTINUED

TABLE 1: LOWER-LEVEL OBJECTIVES MAP INTO HIGHER-LEVEL OBJECTIVES, Continued

| These Lower-Level Objectives | Map into These Higher-Level Objectives |
|---|---|
| Foster agriculture productivity | **Life**—maintain adequate and affordable food supply to reduce deaths from malnutrition<br>**Health**—maintain adequate and affordable food supply to support nutrition required to maintain health<br>**Wealth**—increase agricultural exports<br>**Sovereignty**—maintain self-sufficiency of food production |
| Natural resources cultivation | **Wealth**—increase national wealth and maintain affordable natural resources (e.g., energy) costs for consumers<br>**Sovereignty**—decrease level of dependence on foreign nations for natural resources (e.g., energy) |
| Cultivate alliances with other nations | **Life**—protect life in times of war by allying forces and in times of peace with deterrent capability of implied ability to muster alliances; sharing of intelligence to detect/prevent terrorist attacks<br>**Sovereignty**—reciprocal defense against foreign invasion or threats |
| Maintain military strength | **Life**—protect life in times of war by allying forces and in times of peace with deterrent capability<br>**Health**—protect/enhance health via military research that protects/enhances health (e.g., countermeasures against biological attacks, enhancements to human performance, advancements in prosthetics)<br>**Wealth**—protect trade routes and investments in foreign nations<br>**Sovereignty**—defend against foreign invasion or threat |

These four higher-level objectives encompass many other lower-level objectives. Table 1 illustrates some examples.

### *4.1.4.2 What Are Our Key Metrics for Success?*

Current ERM practices often have key metrics with a short-term focus, sometimes as short as one year. This often fails to capture the full impact of risk events and can result in wildly incorrect risk assessments. Consider an ERM program with only one-year metrics. As shown in the example, two risk events—A and B—appear to be equally impactful if we examine only a one-year period, yet B is many times more impactful than A.

Current ERM practices often result in underestimating risk, as in the preceding example, but they also can result in overstating impacts. In one corporate case study, a company with a one-year time horizon for ERM metrics had, as a credible worst-case scenario for one of its key risks, an event that would shut down production of a product line for one year. However, when expanding the analysis to include multiyear impacts, this scenario was exposed as being so overstated that it was actually reversed from a downside to an upside: due to certain competitive advantages, the organization's competitors would be impacted to a greater degree and for a longer period of time; this would allow the company to be the sole-source supplier to the local market for a period

| Risk Event | Risk Impact | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Year 1 | Year 2 | Year 3 | Year 4 | Year 5 | Year 6 | Year 7 | Year 8 | Year 9 | Year 10 |
| A | –100 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| B | –100 | –100 | –100 | –100 | –100 | –100 | –100 | –100 | –100 | –100 |

of time after it resumed production. During this time, it would reap higher sales at higher prices, and these gains would more than offset the early-onset losses.

Such inaccuracies in risk assessment inevitably lead to poor decision making. Sometimes, the poor decisions are dangerous in that they inform poor risk-reward decisions or fail to identify and correct vulnerabilities to key threats. Other times, they may lead to wasted resources as time, attention and funding are focused on immaterial "false positives" that function as distractions.

Our ERM approach avoids these problems by using key metrics over a time horizon that is long enough to fully assess risk impacts. This is especially important for a nation. The critical national objectives must be achieved on a sustained basis over a long-term (indefinite) time horizon, and we must measure risk in both the short term and the long term. Projections extending for decades may be warranted, because ERM must inform national decisions, some of which take a full generation to reveal their impacts.

Each key metric must be accompanied by corresponding baseline values that define the target we expect to achieve. National governments may not have explicit baseline values for these key metrics; when this is the case, we assign baseline values that are reasonable and consistent with the overall national agenda. We do so because approximate measurement is superior to none; if no baseline value is designated, then the risk—measured as deviation from baseline values—cannot be evaluated properly. Also, the bulk of actionable ERM information is generated from *changes* in these values—which inform relativities, prioritization and choices—and the change in values has a level of accuracy that is an order of magnitude higher than the accuracy of the value itself.

TIP #4: ERM metrics must capture long-term as well as short-term risk impacts to fully and accurately assess risks and properly inform decision making.

For each critical national objective, we must incorporate metrics that capture both the actual and the perceived level of success. If the public misperceives the level of success toward any of these objectives, it may champion for and achieve changes to policies that, in the longer term, will be revealed as having been counterproductive. Though it can be argued that any material deviations between perceived and actual progress are usually temporary, near-term discontinuities can produce real political consequences that can derail progress (in addition to causing personal risk to individual careers). In this context, ethically based efforts to identify and combat such misperceptions serve a legitimate and important purpose. Another reason to include metrics capturing public perception is to capture the emotional impact of disproportionate events that, though they may not materially change the actual level of success, are meaningful intrinsically. For example, a serial murderer at large may not materially change national statistics on life safety, but an entire region of the country may be terrorized and feel a significant decrease in life safety.

For each national critical objective, we attempt to focus on metrics related to areas that are most likely to be under the purview of a national government (as opposed to provincial/state/local government). This varies by country, but we attempt here to include what may be the most common metrics under a national government's purview. Consider the life metric. A metric related to deaths of citizens due to local crime would likely be a local government matter. However, local murders related to the activities of a nationwide organized crime syndicate (such as a drug cartel) would be a national government responsibility.

The specific key metrics (and sub-metrics) proposed are merely examples. Rather than proposing a definitive solution, the intent here is solely to illustrate how to apply our ERM approach—the sequencing/flow of the approach, the process steps involved and the type of thinking/choices needed to implement and maintain it. National government ERM leaders and team members, as well as those of individual government agencies, are encouraged to visualize the analogous metrics or sub-metrics that may more appropriately represent their unique situation.

**4.1.4.2-1 Life metric.** The life metric could be composed of the following sub-metrics:

- Deaths caused by war/terrorism
- Deaths caused by large-scale crime/negligence
- Deaths caused by transportation
- Deaths caused by natural disaster
- Perception of life safety

**Deaths caused by war/terrorism.** This sub-metric could be defined as the number of annual deaths caused by acts of war or terrorism.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* military (deterrent), intelligence (information that enables pre-event mitigating actions), diplomacy (reduction of tensions that may lead to conflict) and strategic alliances with other nations (deterrents and sources of additional intelligence)
- *Lowering the severity of risk event impact:* law enforcement (halting of acts in progress, apprehension of criminals), judicial system (incarceration), military (defense), intelligence (information that enables event-in-progress mitigating actions), diplomacy (reduction or end of conflict) and strategic alliances with other nations (military and intelligence assistance)

**Deaths caused by large-scale crime/negligence.** This sub-metric could be defined as the number of annual deaths caused by acts such as the following:

- Poisoning of air or water or contamination of land, either by illegal polluting (such as dumping of toxic waste) or by accident
- Civil unrest
- Organized crime

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* criminal laws and regulations (deterrent), law enforcement (deterrent), judicial system (deterrent), military or national guard (deterrent against civil unrest), intelligence (information that enables pre-event mitigating actions against civil unrest), outreach to protest groups (reduction of tensions that may lead to civil unrest) and monitoring of air and water quality (early detection of pollutants)
- *Lowering the severity of risk event impact:* law enforcement (halting of acts in progress, apprehension of criminals), judicial system (incarceration), military or national guard (restoration of law and order during civil unrest), intelligence (information that enables event-in-progress mitigating actions against civil unrest), outreach to protest groups (reduction or end of civil unrest) and cleanup of toxic sites

**Deaths caused by transportation.** This sub-metric could be defined as the number of annual deaths caused by transportation over roads, rail, waterways and by air.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* transportation regulation such as safety features

for cars (for example, rear brake lights), trains (for example, auto-braking) and ships and airplanes (for example, collision detection systems); operator safety training standards (for example, pilot training); and standards for roads (such as lower speed limits to enable prevention), bridges (such as inspections) and airports (air traffic control standards)

- *Lowering the severity of risk event impact:* transportation regulation such as safety features for cars (for example, seat belts, safety glass), buses (for example, emergency exits) and ships and airplanes (for example, life vests); operator emergency-response training standards (for example, flight attendant training); and standards for roads (such as lower speed limits to decrease lethality) and airports (on-site emergency response requirements)

**Deaths caused by natural disaster.** This sub-metric could be defined as the number of annual deaths caused by natural events such as earthquakes, tsunamis, tornadoes, hurricanes, wildfires, rainstorms, windstorms, electrical storms, pandemics, drought, crop disease, mudslides, volcanic eruptions, solar flares, and so on.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* forestry regulation/management (against wildfires), infectious disease management (against pandemic) and agriculture regulation (against crop disease)
- *Lowering the severity of risk event impact:* storm shelters, emergency action plans, emergency services, disaster relief funds (minimization of impact of natural disasters post-event) and insulation of electrical grid (minimization of impact of solar flares on electrical grid)

**Perception of life safety.** This sub-metric could be defined based on a public-opinion survey. Perceptions may change independent of the actual level of life safety achieved; for example, foreign propaganda could decrease the public's perception of life safety although there is no change in the actual level. Also, two different events that result in the same actual change in life safety may impact perception in very different ways. For example, a single corporate criminal act that results in the loss of 10 lives might not cause the perception of life safety to change significantly, whereas the same loss of life due to a deranged citizen shooting people at a mall might have a material negative impact on perceived safety.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* pre-event mitigation of particularly terrorizing events, such as intelligence services identifying and infiltrating hate groups to detect and prevent terror acts
- *Lowering the severity of risk event impact:* post-event mitigation of particularly terrorizing events, including national alert systems such as Amber alerts (child abduction) and national weather alerts for early warning of dangerous weather to allow citizens to take shelter (A post-event activity that can mitigate the impact on the perception of life safety is to identify, implement and publicize any enhanced mitigation against future recurrences.)

**4.1.4.2-2 Health metric.** The health metric could be composed of the following sub-metrics:

- Life expectancy
- Perception of health safety

**Life expectancy.** A variety of metrics, such as obesity rates, smoking rates and percentage of the population with at least one chronic illness,

capture different aspects of health. However, they all encapsulate parts of the puzzle more succinctly captured by a single health sub-metric with which they are typically correlated: life expectancy. This sub-metric could be defined as the period life expectancy at birth, which is the average lifespan of those born in the current year and exposed to future mortality equal to the current year's mortality rates for each age of life.[5]

Some examples of related federal government responsibilities:

- Providing equitable health care access for all (such as Canada's Medicare) or a portion (such as the U.S. Medicare) of the population
- Setting standards for clean air and water
- Establishing "sin taxes"—additional taxes on items such as alcohol, sugar and tobacco—intended to deter usage and help fund the additional expected health care costs
- Educating the population on a healthy lifestyle

**Perception of health safety.** This sub-metric could be defined based on a public-opinion survey. Perceptions may change independent of the actual level of health safety; for example, false research findings could create a public perception that water or air quality has become unsafe, when in fact no change has taken place. Also, two different events that result in the same actual change in health safety may impact perception in very different ways. For example, an increase in breast cancer rates that results in a certain decrease in actual health safety might impact the perception of health safety more than an increase in diabetes rates that produces an identical impact, merely due to the higher level of public awareness of, and popularity of social efforts to combat, breast cancer.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* federal regulations setting standards for published health-related research
- *Lowering the severity of risk event impact:* actively identifying potentially misleading public-health research and resulting media coverage, combatting misperceptions with public service announcements and inhibiting further misleading efforts via litigation or court action

**4.1.4.2-3 Wealth metric.** The wealth metric could be composed of the following sub-metrics:

- Ability to cover expenses
- Perception of wealth security

**Ability to cover expenses.** Traditional economic metrics, such as unemployment rate and GDP growth, are commonly used to measure the health of the economy. Yet, these metrics do not correlate well with the wealth of citizens. The unemployment rate can improve when economic status of the citizenry is decreasing, such as when the unemployed stop looking for work (the unemployment rate metric excludes such individuals), and when the unemployed stop looking for work comparable in pay to their former employment and accept lower-paying jobs ("underemployment"). Similarly, GDP growth can increase while the average standard of living decreases; this has been evident in recent years, when productivity gains reaped by employers (such as those due to advancements in robotics/automation) have not translated into gains for employees.

Instead of traditional economic metrics, our wealth sub-metric is more directly correlated with the level of wealth of individuals and addresses a question that is more to the point: "Can people pay their bills?"

This sub-metric could be defined as the number of months of expenses a family has in capital. The specific metric could be the average ratio:

$$\frac{\text{Family}^{6}\text{ net worth (assets less liabilities)}}{\text{Monthly living expenses}}$$

This metric captures movements such as a portion of the population moving further into debt (or gaining in equity) as people become less (or more) able to cover their expenses.

Some examples of related federal government responsibilities:

- Public education system
- Monetary policy (such as managing inflation or the money supply) to support a strong economy
- Economic infrastructure—including transportation, sanitation, communications, safety and laws/regulations—necessary to support a strong economy
- Tax laws and regulations to provide incentives for a strong economy

**Perception of wealth security.** This sub-metric could be defined based on a public-opinion survey. Perceptions may change independent of the actual level of wealth security; for example, political campaign rhetoric could create a public perception that the current economic situation is worse than it is. Also, two different events that result in the same actual change in wealth safety may impact perception in very different ways. For example, people may be more sensitive to an increase in federal taxes than to an identically impacting increase in inflation of living expenses.

Unlike the life and health perception-based sub-metrics, public misperceptions of wealth security can do more damage and impact the economy directly, such as when the public acts to invest/spend less than it otherwise would due to unwarranted underconfidence in the economy.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* publishing easily comprehensible, credible and unbiased economic data
- *Lowering the severity of risk event impact:* actively identifying potentially misleading public statements about the economy and issuing public service announcements to counteract these statements

**4.1.4.2-4 Sovereignty metric.** The sovereignty metric could be composed of the following sub-metrics:

- Self-generated critical resources
- National wealth
- Military strength
- Perception of national sovereignty

**Self-generated critical resources.** This sub-metric could be defined as the extent to which a nation has, or can provide/produce, its own critical resources, such as energy, food and essential technologies. The specific metric used could be the percentage of a set of defined critical resources that are available or produced independently. This captures the ability of a nation to self-sustain its critical subsistence and infrastructure. The higher the percentage of self-reliance, the more independent the country. When this percentage falls below a critical threshold, a nation is vulnerable to losing its sovereignty entirely.

Some examples of related federal government responsibilities:

- Laws and regulations supporting sustainable and affordable domestic sources of energy
- Laws and regulations supporting sustainable and affordable domestic agriculture

**National wealth.** This sub-metric could be defined as net national wealth, which is national assets minus liabilities, where national refers to the collective wealth owned by the nation's citizens. This captures the ability of the nation to purchase critical resources that are not self-generated. The more wealth a nation has, the more flexibility and ability to purchase these items.

Some examples of related federal government responsibilities:

- Trade policies to protect/enhance employment opportunities and national wealth
- Immigration policies that attract/retain a globally competitive level of talent and innovation

**Military strength.** This sub-metric could be defined as the relative ranking of national military power versus that of other nations. An alternate sub-metric could be the relative ranking of the combined military power of the nation and its closest allies versus the analogous ranking of its current top adversary. The specific metric, for either of these alternatives, could be the size of the annual military budget. This captures the ability of a nation to defend itself from (1) military threats and (2) intrusions into its key alliances and interests, particularly regarding transportation and trading routes (land, sea, air and space) and relationships with partner trading nations. Generally, the higher the level of relative military strength, the more independent the country. Above a certain threshold, the benefits diminish; similarly, falling below a certain threshold represents a critical threat to sovereignty.

Some examples of related federal government responsibilities:

- Military strength
- Budgetary policies to maintain military strength
- Maintenance/enhancement of strategic military alliances

**Perception of national sovereignty.** This sub-metric could be defined based on a public-opinion survey. Perceptions may change independent of the actual level of national sovereignty. Some examples include the following:

- Foreign intrigue might create a public misperception that there is an excessive level of dependence on an allied nation; this could lead to a counterproductive cooling of relations between the two allies.
- Corporate lobbyists could create a public misperception that obscures the fact that there is an excessive level of dependence on another nation; this could lead to passage of legislation profitable to corporate entities but potentially damaging to national sovereignty.
- Military vendor lobbyists could create a public misperception that the nation has insufficient military capabilities; this could lead to unnecessary spending on military projects.

Some examples of related federal government responsibilities:

- *Lowering the likelihood of a risk event:* gathering and acting on intelligence (information that enables pre-event mitigating actions)
- *Lowering the severity of risk event impact:* actively identifying potentially misleading information related to national sovereignty and providing public information to counteract misperceptions

### *4.1.4.3 Identifying Key Risks*

Now we have answered the questions about critical national objectives and key metrics for success. Once projected baseline values are assigned for each key metric, we can return to our initial question, "What are the key risks?"

We first answer this question at the *sub-category* level to create the risk categorization and definition tool. The RCD tool is developed by thinking through the following question: "What types of risk events, each defined by its originating source, might cause us to deviate (either up or down) from achieving the baseline values for our key metrics?" The RCD tool is provided to qualitative risk assessment (QRA) participants as part of the QRA advance communication for the following purposes:

- A catalyst to trigger their thinking about the types of risk to consider
- An illustration of how, in an ERM context, risk is defined
    - As an event that causes a significant deviation from expected/baseline results
    - By originating source (not by outcome)
    - At a consistent level of granularity

In the upcoming step—the qualitative risk assessment itself—we will answer the question "What key risks do we face?" at the *risk* level.

The RCD tool is developed by considering each key metric/sub-metric, one at a time, and imagining what types, or sub-categories, of risk sources could cause it to significantly deviate—up or down—from its expected/baseline values. Risk sources often include events that impact multiple key metrics/sub-metrics, so as we identify risk sources for our key metrics/sub-metrics, we conveniently find that some of the risk sub-categories are already on the list. For example, in considering the life sub-metric "deaths caused by war/terrorism," an obvious risk source is "war—new conflict" (unexpected outbreak of war). However, should a risk within this sub-category occur, it can impact not only the life sub-metric, but also those for health, wealth and sovereignty. Therefore, as we progress in our exercise, when we arrive at the health, wealth and sovereignty sub-metrics and consider war as a risk sub-category, we will find it is already on the list.

Once the risk sub-categories are developed, the risk category labels are assigned. These are less important, because they serve only to group similar risk sub-categories and there are varying definitions of risk categories. The risk categories used here are strategic, operational and financial, and they are defined as follows:

- **Strategic**—a category of risks related to items of strategic importance (often, these are differentiators of success/failure versus competitors)
- **Operational**—a category of risks related to items of routine operations (typically, these include human resources, technology, processes and disasters)
- **Financial**—a category of risks related to external markets and prices (such as economic environment, stock market, bond market and commodity prices)

A partial illustrative example of an RCD tool appropriate for our chosen set of national key metrics is shown in the Appendix. Consistent with our definition of risk in an ERM context, the definition of each risk sub-category is expressed as a deviation from expectations/baseline.

## 4.2 QUALITATIVE RISK ASSESSMENT (QRA)

Now that we have the RCD tool, we can begin the qualitative risk assessment (QRA) process, which involves the following steps:

1. Identify participants.
2. Provide advance communication.
3. Interview participants. (This will occasionally be referred to as Interview #1 to distinguish it from a second interview conducted during the risk quantification process.)
4. Score likelihood/severity.
5. Select key risks.

### 4.2.1 Identify Participants

The first step is to identify the QRA survey participants who will be interviewed in step 3. The total number should be large enough to involve those with the widest range of knowledge of potential key risks and small enough to be manageable. Examples of potential candidates include the following:

- Key leadership, such as heads of departments or agencies, or their direct reports who may be closer to the operations and risks
- Executive risk owners (EROs), who are individuals with expertise in a known key risk and/or with official responsibility to lead efforts related to a key risk
- Some staff valued for their long service, understanding of government workings and/or expertise
- Some key stakeholders with risk insight

### 4.2.2 Provide Advance Communication

Participants should be provided with an advance communication, the primary goal of which is to prepare them for the interview. It should convey the following:

- Benefits that ERM provides
- An overview of the ERM process
- The critical importance of the QRA to the ERM process
- Key information participants should be prepared to provide during the QRA interview
- Risk categorization and definition
- Likelihood and severity scoring criteria
- How the information they provide will be used

The key information participants will be asked to provide during the interview includes the following:

- List of potential key risks
- Credible worst-case scenarios
- Likelihood and severity scores

#### *4.2.2.1 List of Potential Key Risks*

QRA participants should be prepared to provide a list of potential key risks, where key risks are defined as events that

- Span all categories and sub-categories of risks, such as those listed in the RCD tool, which is included in the advance communication sent to QRA participants
- Impact any part of the government (not necessarily limited to the participant's area of responsibility)
- Are defined by their originating source (not outcome), also illustrated in the RCD tool
- Have the potential to cause at least one of the key metrics to have results that materially deviate from its baseline (strategic plan goal) expectations[7]

Having a scope that includes all categories and sub-categories of risks is a critical characteristic of successful ERM programs. Often, ERM programs limit the scope of risks considered; a typical category they ignore is strategic risk, which routinely accounts for the largest number of key risks in an ERM context.[8] Ignoring risk sources can subvert the entire purpose of ERM, which is to better understand and inform decisions about significant known volatility that can impact the organization.

QRA participants should only be asked to provide a small number (such as three to five) of potential key risks. Requesting only a small number serves multiple purposes:

TIP #5: Risk identification must include all sources of risk to provide as complete a picture of significant known volatility as possible, which is critical for risk-reward decision making.

- It focuses participants on the most important key threats.
- It avoids unsettling participants who may only be able to offer the minimum number requested. Those who have more than the maximum number requested tend to bring their full list anyway and this can be collected during the interview.
- It leads to an appropriate number of potential key risks collected, in aggregate, once all QRA participant interviews are completed.

#### *4.2.2.2 Credible Worst-case Scenarios*

For each potential key risk, QRA participants should be prepared to provide a single credible worst-case scenario that describes a specific (deterministic) manifestation of the risk, how it initiates and how it plays out. A *credible worst-case scenario* is defined as an event that is rare and severe yet still possible (as opposed to an Armageddon scenario).

Most ERM programs ask participants merely to provide a broad description of the risk, which tends to lower the quality of the QRA results to a point that should be considered unusable. When QRA participants provide scores on the aggregate risk list (produced by consolidating the risks gathered during the QRA interviews), the vagueness of a broad description results in confusion and the possibility that each participant may be scoring different events. Each risk can manifest in a variety of risk scenarios, and each participant may be imagining a different one when providing his or her likelihood and severity scores. In our ERM approach, for consistency in scoring, we request that a specific credible worst-case scenario be provided for each risk. For example, for the risk of a data breach, a credible worst-case scenario might be "a data breach involving the most sensitive information within an agency, stolen by our leading adversary nation." This affords the QRA participants a more consistent vision of what the event is—and can help them form clear opinions on its likelihood and severity more easily—than would a broad risk defined merely as "data breach."

TIP #6: QRA scoring must be conducted using well-defined risk events, such as credible worst-case scenarios, to avoid confusion and inconsistent scoring results.

At this stage of our ERM process, we only use the single downside of a credible worst-case scenario to evaluate potential key risks. There are two reasons for this. First, this scenario tests whether a risk is truly a potential key risk; often, QRA participants believe a risk to be important until they are asked to try and imagine a specific credible worst-case scenario and then score it, only to realize that it has an immaterial impact. If even a credible worst-case scenario does not generate materially high severity scores, then the risk is not a key risk. Second, our ERM approach captures both upside and downside volatility, but this is done in a subsequent stage (risk quantification, Interview #2) where multiple risk scenarios are developed for each confirmed key risk. Attempting to explore a full range of scenarios for each potential key risk is unnecessary, and more important, not feasible.

#### *4.2.2.3 Likelihood and Severity Scores*

For each credible worst-case scenario, QRA participants should be prepared to provide a single likelihood score and one or more severity scores—one for each key metric/sub-metric impacted.

Scoring criteria must also be defined in the advance communication to QRA participants. The scoring criteria should clearly define the metrics. For example, the likelihood scoring criteria should specify the range

of likelihood percentages and the corresponding time horizon. Each severity metric should similarly indicate the range of absolute or percentage deviation from baseline results (in our ERM approach, risk is measured as deviation from baseline plan expectations). Here is an illustrative scoring criteria example for likelihood and a single key metric:

| Likelihood Score | Chance of Occurring (risk event begins within next 3 years) |
|---|---|
| Very high | ≥20% |
| High | ≥10% but <20% |
| Medium | ≥5% but <10% |
| Low | ≥2% but <5% |
| Very low | <2% |

| Severity Score | Key Metric #1 War/Terrorism Deaths in Excess of Expected (total over all future periods) |
|---|---|
| Very high | ≥1,000 |
| High | ≥250 but <1,000 |
| Medium | ≥100 but <250 |
| Low | ≥10 but <100 |
| Very low | <10 |

### 4.2.3 Interview Participants

Many ERM programs gather input from QRA participants using questionnaires. This typically produces a low-quality set of information and should never be used as the primary method. QRA participants often initially provide risks that are not suitable as key risks; for example, the risks are not defined by source or do not have the potential to be materially impactful. With questionnaires, it is not feasible to iteratively contact participants, reinstruct them, have them resubmit responses and so on. Personal interviews are superior to questionnaires. In an interview, these corrections are made instantly by providing guidance, feedback and Socratic inquiry. Some ERM programs use open-group discussions. These should also be avoided as a primary method, because they are often biased by groupthink and/or a dominant individual's influence, or some information is withheld by individuals unwilling to share risks on the record. The preferred method is one-on-one anonymous interviews, which resolve the issues that arise with questionnaires and open-group discussions.

TIP #7: Anonymous, expert-led, one-on-one interviews should be used in the QRA process to provide the most robust and high-quality list of risks.

**RED FLAG #1** This interview (Interview #1) is the first of the three most critical activities in the ERM process. Any failings in this step have a cascading and multiplying negative effect on the entire ERM process, because all subsequent steps are predicated on this one. In addition, this is a key moment to either gain or lose stakeholder buy-in. Finally, although this may seem like a straightforward interview to conduct, a lack of ERM experience on the part of the interviewer tends to produce suboptimal results, and the difference of what has been missed may not be apparent. The ability to provide proper guidance on defining risks by source, defining risks at an appropriate level of granularity, differentiating key risks from non-key risks, connecting ERM to interviewee goals and so on are often subtle conversations, and expertise in both ERM and communication skills are required for an effective interview.

### 4.2.4 Score Likelihood/Severity

After the QRA participant interviews have been conducted, a list of potential key risks (stated in credible worst-case scenario form) is created by aggregating and consolidating those provided by each participant. This consolidated potential key risk

list is sent to the QRA participants, who then provide likelihood and severity scores for each item. Average severity scores may be calculated by assigning numerical scores to each qualitative score; average probabilities may be assigned to each qualitative likelihood score.

A ranking methodology may be developed to convert the scoring results into a single ranking result. One approach is to assign weights to each key metric/sub-metric to collapse it into a single severity metric/score that can then be multiplied by the weighted-average likelihood to obtain a single number. This number is then ranked.

### 4.2.5 Select Key Risks

In the final step of the QRA process, a consensus meeting is conducted with all QRA participants to decide collectively on the separation of the potential key risk list into key and non-key risks. The key risks will advance to the risk quantification ERM process step. The non-key risks will be relegated to the monitoring known risks portion of emerging risk identification.

Before making this decision, the group examines, discusses and (anonymously) revotes on some highly ranked risks whose scores exhibit a high level of dispersion.[9] Participants find this to be among the most valuable exercises. This discussion affords an opportunity to share information and perspectives on risks and results in a higher level of understanding and consensus. This is one of the activities that advances risk culture and leads to ongoing productive dialogue between colleagues about risk.

The number of key risks selected should be a manageable number, typically in the range of 20 to 30. ERM focuses on the largest volatility items. Organizations have limited time, attention and resources, and a larger number of key risks results in a slow and cumbersome process that cannot be practically implemented or maintained, so it soon falls under its own weight. Many government ERM programs attempt to include too many risks in the key risks list and fall victim to this problem.

## 4.3 EMERGING RISK IDENTIFICATION

Emerging risk identification has two components. The first is monitoring known risks, which involves developing and tracking key risk indicators (KRIs) for each non-key risk identified in the QRA process. If a KRI, which is a leading indicator, suggests that one of the non-key risk's likelihood and/or severity scores is likely to rise above a certain threshold in the short term, then the non-key risk is elevated to the key risk list, where it is subject to more scrutiny.

The second component is environmental scanning for unknown risks, which is relatively straightforward. This involves collecting information from available sources—such as industry committees, published research and articles—to identify potential risks that may emerge in the future.

# 5 RISK QUANTIFICATION

The risk quantification process cycle step consists of the following three activities:

- Projecting baseline values
- Individual risk scenario quantification (IRSQ)
- Calculating enterprise risk exposure (ERE)

## 5.1 PROJECTING BASELINE VALUES

The first step to quantifying risk is to project the baseline values, because in our ERM approach, risk is measured as deviation from expectations/baselines. There are five key concepts to building a proper ERM model to do this:

1. Practical modeling
2. Projecting key metrics/sub-metrics
3. Projecting over appropriately long time horizon
4. Making the model dynamic to value/risk drivers
5. Projecting values with appropriate granularity

### 5.1.1 Practical Modeling

For ERM, it is both appropriate and critical to engage in practical modeling. The model must be robust enough that we can rely on it for decision making, yet it must include only the level of detail needed to accomplish the task and no more. Practical modeling is appropriate because ERM involves future projections involving numerous assumptions. This limits the accuracy possible in the ERM model and therefore obviates the need for a highly detailed and complex model. Practical modeling is critical; without it, ERM calculations are inhibited, the ERM process becomes cumbersome and/or model complexity results in a lack of stakeholder buy-in. The ERM model must calculate quickly enough to handle simulations of risk combinations, which are needed to calculate enterprise risk exposure. In addition, the number of ERM model inputs must be limited to a manageable number to enable a nimble process of keeping the assumptions current and relevant. Finally, practical modeling allows the transparency needed to make key stakeholders comfortable enough to rely on the ERM information for decision making; decision makers tend not to rely on information for key decisions unless the basis for the information generated is transparent.

TIP #8: ERM models must strike just the right balance: robust enough that they can be relied on for decision making yet practical and transparent enough to generate buy-in.

The importance of practical modeling cannot be overstated. Overly complex or inflexible ERM models often derail the ERM process.

### 5.1.2 Projecting Key Metrics/ Sub-metrics

The baseline values for each key metric/sub-metric must be projected separately within the model. These are the basis of risk measurement—any deviation in results from these baseline values is the quantitative measure of an individual risk or of a simulation involving multiple simultaneous risks.

### 5.1.3 Projecting over Appropriately Long Time Horizon

To be useful for ERM purposes, the ERM model must project the key ERM metrics over a long enough time

horizon to fully measure the impacts of risk. For the federal government, this is likely to be decades long, because many federal government decisions take a full generation to reveal their full impact. Most federal government projections that involve such long-term time horizons do not include projections of the kind of key metrics needed for ERM purposes (to be fair, they were not designed to do so). Here are two examples:

- The Canadian Finance Department has a 50-year forecast,[10] which is certainly a sufficiently long time horizon. However, it does not include the projection of key metrics needed for ERM purposes; rather, it projects the federal budget revenues and expenses, relying largely on aggregate measures. Even its shorter-term (six-year) forecast projects the fiscal outlook based on estimates of future aggregate economic variables (such as GDP, unemployment and interest rates) taken from an opinion survey of banking executives. The nonpartisan Canadian Parliamentary Budget Office (PBO) runs independent long-term projections to estimate the impact of proposed bills; however, these projections are analogous to those of the Finance Department.

- The U.S. nonpartisan Congressional Budget Office (CBO) has a 10-year forecast[11] of the federal budget and economic outlook and a 30-year forecast[12] of the federal budget, both of which are used to estimate the impact of proposed bills. However, the projection basis and metrics are inconsistent with ERM needs and only focus on federal revenues and expenses.

### 5.1.4 Making the Model Dynamic to Value/Risk Drivers

The ERM model must be designed to project baseline values of key metrics in a dynamic way, one that easily adjusts to reflect changes. When a risk—either upside or downside—occurs and results in changes in one or more variables, the model design must easily accommodate the input of the new/changed assumptions and dynamically project the change in key metrics. This is how risk is quantified. When designing the ERM model to project the baseline values, supporting the next step—risk quantification—must be considered. In keeping with our concept of practical modeling, the dynamism in the model should be chosen carefully and limited to those variables informed by the RCD tool initially and, when available, the specific key risks and corresponding scenarios. For example, if one of the key risk scenarios is a significant worsening of eating habits in a portion of the population that results in a specific change in that group's mortality or morbidity, then the model must be able to change these assumptions easily for that portion of the population and project the new key metrics, including the health sub-metrics: life expectancy and perception of health safety.

### 5.1.5 Projecting Values with Appropriate Granularity

The baseline values for each key metric/sub-metric must be projected with enough granularity to capture the impacts on each key constituent group. The ERM model must be able to distinguish between a risk that has the same impact across all citizens versus one that has a disproportionate impact on only a portion of the citizenry. In keeping once again with our concept of practical modeling, we must carefully select only those constituent groups that are likely to have materially different impacts for the key risks on our list. For example, an economic downturn will impact variables such as unemployment, spending habits and wealth metrics in ways that vary by socioeconomic group, industry sector, job level, geographic area and other demographics.

This level of granularity achieves three goals. First, it produces more accurate projections. Second, it allows us to identify risks that can result in crises for certain constituent groups, where such risks might not otherwise register as critical on a national (aggregate)

level. Third, a federal government decision intended to target a specific constituent group can more accurately assess the likely level of success in achieving the desired results. For example, the impact of a bill passed with the intention of improving the health and wealth metrics/sub-metrics for an impoverished portion of the citizenry can be more accurately assessed in terms of its likelihood of succeeding.

A side benefit to building the ERM model to perform a baseline projection is that it also serves as model validation. Lower-level, detailed models that already exist in the organization can be leveraged for their projection methods and data/assumptions. The process of leveraging these disparate, pre-existing models and coalescing them into a new form—the ERM model—acts as model validation. The ERM model puts an enterprise-level picture together (often for the first time), identifies potential discontinuities and affords opportunities to correct them.

**RED FLAG #2** Building the ERM model is the second of the three most critical activities in the ERM process. Models that are not properly constructed for ERM are often the misstep that impedes the entire ERM process. The ERM model must be built with the key concepts outlined here and with attention toward its suitability to the activities and decisions the model will support in later ERM steps. In addition, modelers sometimes fall into the trap of thinking that "more is better" and add unnecessary model infrastructure to the point of unworkability. This is another area where a lack of specific experience (in ERM modeling) tends to produce suboptimal results.

## 5.2 INDIVIDUAL RISK SCENARIO QUANTIFICATION (IRSQ)

Once the key risks are identified and the ERM model is constructed, the first step in quantifying risks is to quantify the one-at-a-time occurrence of specific scenarios under each key risk. These are the building blocks of our ERM approach. By the time we have reached this step, we have already done much of the quantification-related work; the following have all formed the foundation that enables quantifying individual risk scenarios:

TIP #9: ERM models should be constructed by those with ERM modeling experience to produce a practical, working model that can properly support ERM activities and decision making.

- Identifying the critical national objectives (high-level goals)
- Identifying the key metrics/sub-metrics that represent success (specific metrics for projection)
- Developing the RCD tool (sources of potential key risks that can change the baseline values for key metrics/sub-metrics)

There are two steps to individual risk scenario quantification:

1. Developing individual key risk scenarios
2. Quantifying individual key risk scenarios

### 5.2.1 Developing Individual Key Risk Scenarios

For each key risk, we must now identify the subject matter expert (SME) most appropriate to interview for developing the corresponding risk scenarios. While more than one SME may be brought in to flesh out the risk scenarios that were developed initially, it is advisable to involve a single SME to lead the efforts for the interview (Interview #2), during

which the skeletal structure of the risk scenario is mapped out (as opposed to collecting every item needed to complete the risk scenarios, which can be done in later follow-up meetings with other SMEs). In contrast to the QRA interviews (Interview #1), the risk scenario development interview (Interview #2) is not anonymous; it is important that colleagues throughout the organization see that the SME recognized for his or her expertise with the risk is the one whose opinions were collected for that risk. Each risk scenario developed during the interview must describe the source—originating event—that triggers the risk, its likelihood and a description of how it is likely to play out in the real world, including management actions and all downstream consequences, comprising a description of the shocks, or changes, to the ERM model variables (risk and value drivers). The result of the interview is a handful of risk scenarios that represent the major inflection points of the risk and include a range of downside scenarios and, when warranted, upside scenarios.

For each risk, asking the SME to estimate the likelihoods for the identified deterministic risk scenarios (that is, the events that represent deviations—up or down—from the baseline) forces him or her to acknowledge the likelihood of the baseline itself (since they all must add up to 100%). This process generates healthy discussions that (1) socializes the baseline strategic plan, making colleagues more aware of the organization's commitments; (2) makes explicit some baseline assumptions that were otherwise hidden/implicit; and (3) reveals which assumptions are soft (those with which the organization lacks confidence) and provides opportunities to better align these assumptions. This is one of the ways that our ERM approach strengthens the strategic planning process itself.

The individual risk scenarios should be developed using deterministic SME-based realistic scenarios. Stochastic (randomly generated) risk scenarios are often used in developing risk scenarios. In our ERM approach, we recommend that only deterministic risk scenarios—those developed using failure modes and effects analysis (FMEA) interviews with SMEs—be used directly with the ERM model, because they have the following advantages:

- **By source.** The FMEA approach is one that guides SMEs to identify risks by their originating source and then to follow this downstream to capture all resulting consequences. This approach was selected because it serves one of our guiding risk principles: identifying risks by source.
- **More accurate.** SME-based risk scenarios are more accurate, because they leverage the intelligence, knowledge, judgment and intuition of those closest to the operations and the risk itself. The SMEs are free to review all available information—such as stochastic outputs, prior occurrences in the organization or elsewhere, industry studies, research—but then filter it for themselves to arrive at an opinion. When data is combined with human intelligence, the projections are superior to those based on data alone.
- **More robust.** Interviewing SMEs allows them to think each deterministic risk scenario all the way through, capturing more information on the most likely way it would initiate and play out in the environment as well as the organization's likely responses (such as mitigation).[13]
- **Fully dynamic.** Stochastic scenarios often rely in whole or in part on industry indexes. Risk exposures often change based on an organization's

decisions or internal environment, and when that occurs, such stochastic scenarios cannot reflect the change because the indexes have not changed. In contrast, our deterministic scenarios can quickly be updated for any change in exposure, even one based solely on internal changes, by reconnecting with the SMEs.

- **Transparent.** Rather than trying to explain the esoteric math formulae that generate stochastic scenarios, our approach results in one-page documents for each risk scenario that are transparent and easy to review and understand. This results in a high level of buy-in from key stakeholders, who are then comfortable relying on the information for decision making.
- **Fewer errors.** Because deterministic risk scenarios are easy to document and share—both vertically and horizontally in the organization (to the extent appropriate)—others are able to offer input that enhances the scenarios, including identifying and correcting errors.
- **Enhanced risk culture.** A stochastic approach typically involves only a handful of modeling individuals, whereas a deterministic approach engages far more people in the process. ERM is more about getting people involved, building their ERM knowledge and looking at risk-reward decisions in a more sophisticated, disciplined and consistent manner. In addition, a deterministic approach enhances consensus by extracting information previously unsolicited from SMEs and sharing it throughout the organization; this shared knowledge—once corrected/vetted by others' input—results in a tightening of consensus on key risks.

**RED FLAG #3** This interview (Interview #2) is the last of the three most critical activities in the ERM process. The individual risk scenario quantification is the lynchpin of the ERM process. Failure to properly develop individual key risk scenarios results in inaccurate individual risk scenario quantification—either under- or overestimation—and even more dangerously, this can occur without the knowledge of the ERM team. In addition, all subsequent steps—calculating enterprise risk exposure, defining risk appetite and so on—will be negatively impacted as well, because individual risk scenario quantification provides the building blocks on which they rely. This interview is particularly tricky, because the interviewer must build a bridge between (1) the information the SME is able to provide from his or her business perspective, knowledge and nomenclature, and (2) the inputs required by the model. This must be done on the fly during the interview. In addition, the interviewer must convey a connection between this exercise and how it will help support the SME in pursuit of his or her business goals. Finally, as with Interview #1, this interview is another opportunity to either gain or lose stakeholder buy-in, in part because many of the SMEs were not QRA survey participants and are being exposed to ERM for the first time. As a result, this interview—which on its face may seem straightforward—involves many subtleties, and an interviewer with expertise in both ERM and communication skills is required for an effective interview.

### 5.2.2 Quantifying Individual Key Risk Scenarios

For each key risk, the individual key risk scenarios

TIP #10: The individual risk scenario development FMEA interview with SMEs (Interview #2) should be led by an expert to protect the quality of the lynchpin in the ERM process: individual risk scenario quantification.

are quantified by entering the shocks (changes to the model variables), as recorded from the FMEA risk scenario development interviews, into the ERM model, which produces the impact (change) in the key metrics. The ERM model should be constructed in such a way that all key risk scenarios can be entered, and coding can be created to handle the mechanics of the shocks cleanly and practically. The result is a one-page document for each key risk scenario that is suitable for sharing vertically and horizontally in the organization (as appropriate) and contains a summary of the risk scenario event, its likelihood, shocks and its impact on key metrics. These one-page reports will be collectively referred to as IRSQ reports.

The IRSQ reports are shared with the SME(s) who contributed to the FMEA interviews for reasonability checks. Following that, the reports are shared vertically and horizontally throughout the organization (as appropriate), both to socialize the information and to vet it, whereby the ERM team can receive input, opinion and commentary that improves the risk scenarios.

Even at this stage of the ERM process—before the quantification phase is completed—the IRSQ information is valuable. The individual key risk scenarios that produce the largest impact to each of the key metrics can be identified. Every time the author has seen this performed, the following three things happen:

1. **Surprises.** Some risks that were not considered to be a big threat are shown to produce the highest ranking impacts; conversely, other risks that were thought to be large threats are shown not to have as large an impact as expected. These surprises arise from leveraging the power of SME insights and quantifying them in a rigorous, consistent and comparable way in the ERM model.

2. **Enhanced prioritization.** A prioritization of focus on risks emerges that is different from, and superior to, that generated in the QRA process. This happens for three reasons:

   - IRSQ is based on SME estimates. These are better than estimates by QRA survey participants, who typically have a broader level of knowledge regarding most key risks.

   - IRSQ develops a full range of risk scenarios, whereas the QRA focuses on one (credible worst-case) scenario.

   - IRSQ provides point-estimate quantification, whereas the QRA qualitative score represents a broad range of metrics (for example, “medium” may be anywhere from 5% to 10% impact).

   This is particularly alarming, because most ERM programs do not perform the risk quantification step this way; instead, they rely solely on the QRA prioritization to inform decision making. The implications are that such decisions are flawed, because the IRSQ prioritization can differ dramatically from that of the QRA.

3. **Decision making.** It is generally advisable to wait for risk quantification to be completed (all the way through calculating enterprise risk exposure) before integrating ERM information into decision

TIP #11: Relying on QRA prioritization to directly inform decision making can be disastrous because it is far less accurate than the IRSQ prioritization.

making. However, it is common for organizations to take some action immediately on seeing the IRSQ results. This occurs for two reasons. First, some risk exposures, once revealed, demand action (that is, it is immediately clear that the exposures are beyond acceptable limits, without having to wait to formally define risk limits). Second, the ERM information generated in our approach is precisely in the language of what the organization cares about: the key metrics. Once it is clear how much one or more of the key metrics is at risk, this results in action.

## 5.3 CALCULATING ENTERPRISE RISK EXPOSURE (ERE)

Enterprise risk exposure (ERE) is a probabilistic representation of how the key risk scenarios can play out in the real world. This involves simulations of risk scenarios—not just one-at-a-time risk scenarios, but multiple combinations of scenarios. Many ERM programs do not examine the quantitative impacts of multiple risk combinations. This is dangerous, because the majority of organizational devastation/failures result from two or more risk events occurring at the same time.[14]

While it is not feasible to calculate the volatility from all possible combinations due to run-time considerations, it is also unnecessary. Including the volatility of the most important simulations (such as those that include, at most, three-at-a-time non-baseline risk scenarios and/or comprise risk scenarios that exceed certain materiality likelihood/severity thresholds) is more than enough to generate a simulation set with a robust representation of key volatility (this approach routinely results in simulations in the hundreds of thousands).[15]

ERE is a distribution representing organizational volatility that is calculated as follows:

1. Define simulation set (as already described).
2. For each simulation, calculate its impact—the change in key metrics—by entering its shocks to the key variables directly into the ERM model.
3. For each simulation, calculate its likelihood as the product of the likelihood of each individual risk scenario represented (including baseline and non-baseline risk scenarios) multiplied by all relevant correlation adjustment factors (CAFs). CAFs are subjective adjustment factors to any/all pairs of risk scenarios where the likelihoods are materially non-independent (CAFs are used to increase or decrease the likelihood).[16]
4. The ERE distribution is the collection of impacts and their corresponding likelihoods.

Unlike the IRSQ information, ERE information is not intuitive in its generic form. No person can look at a distribution—either in data form (which is massive) or in graph form—and understand what actions are needed. Instead, we must translate this information into a readily digestible form, and that form is expressed as pain points. A *pain point* is a threshold for which the organization wants to keep the likelihood of crossing it to a low level.

The ERE distribution can be expressed as the likelihood of crossing one or more selected pain points over the desired projection period. Examples of plausible federal government pain points might include one or more of the following:

1. A *x*% or more decrease in average of life sub-metrics (1–4)
2. Perception of life safety at or below critical level *x*
3. Health sub-metric "life expectancy" at or below critical level *x*
4. Perception of health safety at or below critical level *x*
5. The ability of a constituent group to cover expenses at or below critical level *x*
6. Perception of wealth security at or below critical level *x*
7. A *x*% or more decrease in average of sovereignty sub-metrics (1–3)
8. Perception of national sovereignty at or below critical level *x*

For whichever pain points are selected, the ERE calculation provides the current estimate of the likelihood that these thresholds will be crossed at some point over the projection period; the likelihoods can also be calculated over a shorter time horizon, as desired. This provides a natural way to express and discuss the overall current-state volatility of the organization.

# 6 RISK DECISION MAKING

The risk decision-making process cycle step consists of the following three activities:

- Defining risk appetite and risk limits
- Integrating ERM into mitigation decisions
- Integrating ERM into routine decision making

## 6.1 DEFINING RISK APPETITE AND RISK LIMITS

Most organizations have risk appetite statements that are somewhat vague, largely qualitative and mostly contain information that predates ERM and adds little or no value in an ERM context. The risk appetite statement should be an explicit quantitative expression of the acceptable limits on organizational volatility. The reason that most risk appetite statements are vague is that the majority of ERM approaches do not produce a quantitative expression of organizational volatility; this makes it virtually impossible to define risk appetite quantitatively. Our approach does produce a quantitative expression of organizational volatility: this is enterprise risk exposure (ERE). With our approach, risk appetite can be defined by stating the maximum acceptable level for the likelihood of one or more pain points. For ease of illustration, imagine that a federal government ERM program decides to express its ERE solely in terms of a single pain point: the perception of wealth security at or below critical level ***x***. Assume the ERE calculation shows that the current-state likelihood (weight-averaged across all constituent groups) of crossing this pain point threshold (over the time horizon chosen) is 5.7%. In examining this information, the leadership decides to define risk appetite as follows: "The likelihood of crossing this pain point threshold must never be higher than 10%." Risk appetite is expressed on the same basis and with the same terminology as ERE, which makes defining risk appetite (and managing ERE to its optimal level in relation to risk appetite) relatively straightforward.

Risk limits are analogous to risk appetite, but instead of a limit on ERE they are limits on sub-enterprise exposures. Risk limits are the "inner fence" added as extra protection within the "outer fence" of risk appetite. They can be defined as limits on risk coming from a single government agency, a single source of risk or any other number of allocation bases. Continuing the preceding example, in addition to defining a risk appetite at the country level, a federal government ERM program might define a risk limit at a lower level as follows: "The likelihood of 50% of constituent groups with perception of wealth security at or below critical level *x* must never be higher than 25%."

Non-government ERM programs should explicitly define risk appetite quantitatively. Government programs can do the same, but a legitimate alternative is to consider doing it implicitly, by selecting the key pain points on which to prioritize focus and then stating the following: "The funding level provided for in the federal budget, as well as its strategic allocations, implies a risk appetite (at least) equal to current-state ERE levels." In other words, "For the level of funding we have, ERE expresses the current-state volatility of key national metrics, and we can infer that this level of risk is 'acceptable,' because it is the natural consequence of the funding." This alternative may be less politically fraught than explicitly defining risk appetite independent of funding levels, which implies that a given level of poverty or sickness or death or loss of sovereignty is "acceptable," which is not necessarily the case.

## 6.2 INTEGRATING ERM INTO MITIGATION DECISIONS

We are now armed with the information we need to manage the level of overall enterprise risk, or organizational volatility. We have a quantitative expression of current-state volatility (ERE) and a quantitative expression of its desired limit (risk appetite). If ERE is within its optimal range below risk appetite, and if sub-enterprise exposures are within optimal ranges below their corresponding risk limits, then no change in mitigation-related actions is indicated. However, if either ERE or sub-enterprise exposures are too high or too low, then a change in mitigation-related actions is indicated. It may be apparent why an exposure level that is too high must be lowered through additional mitigation; however, it may not be as readily apparent why an exposure that is too low may need correction. There are situations where higher risk exposures allow us to improve our baseline expectations and overall chances of achieving our goals. The ERM model and process can help sort this out. These instances are examples of where taking on more risk yields more reward/return. One example is when a higher-risk battle strategy may increase the chances of winning a war.

Other mitigation-related actions may be warranted when different combinations of mitigation—within the constraint of a constant budget and resources—produce better results, that is, better key metrics under the baseline plan expectations and/or a higher likelihood of achieving plan goals and/or lower ERE or sub-enterprise exposures. The ERM model and process can be used to identify such possibilities.

The ERM model and approach assist in making any mitigation-related decision by allowing a robust, integrated set of information on both a pre- and post-decision basis. The information provided includes the critical bases for any decision: risk and reward information.

Risk:

- Individual risk scenario exposures (absolute and in relation to risk limits)
- ERE (absolute and in relation to risk appetite)

Reward:

- Baseline projection of key metrics

A mitigation decision is adopted if it provides a more favorable risk-reward tradeoff than the current state.

## 6.3 INTEGRATING ERM INTO ROUTINE DECISION MAKING

While keeping risk exposures within acceptable limits is the most commonly recognized purpose of ERM, our approach supports a far more expansive and important mission: integrating ERM into routine decision making, such as strategic planning, strategic and tactical decisions and transactions.

The ERM model and approach assist in making any routine decision by allowing a robust, integrated set of information on both a pre- and post-decision basis. The information provided includes the critical bases for any decision: risk and reward information.

Reward:

- Baseline projection of key metrics

Risk:

- Individual risk scenario exposures (absolute and in relation to risk limits)
- ERE (absolute and in relation to risk appetite)

A routine decision is adopted if it provides a more favorable risk-reward tradeoff than the current state.

This approach for routine decision making is virtually identical to that used for mitigation-related decisions. They both involve evaluating the risk-reward tradeoffs, which is the most rigorous basis for any decision. The only difference is that for routine decision making, we first examine the reward side of the equation (because the primary intent of the decision is to improve expected results), and after that, we examine the risk side (to verify that this is within limits and therefore acceptable). In contrast, a mitigation-related decision's primary impetus is to manage (up or down) the risk exposure level, and therefore we examine the risk side of the equation first (to verify that it is moving as desired); after that, we examine the impact on the reward side of the equation.

In addition to providing the infrastructure and process to support decision making, throughout this paper, we have highlighted characteristics of our ERM approach that also facilitate the ability to support decision making. We provide a brief recap of some of these points here:

- Defines risk as any event—upside or downside—that results in a deviation from baseline strategic plan objectives. This is the lynchpin that directly connects ERM to decision making, because this allows ERM to provide information on both sides of the risk-return equation, and everyone is concerned with achieving Plan goals.
- Includes all sources of risk to provide as complete a picture of significant known volatility as possible, which is critical for risk-reward decision making
- Has transparent building blocks—one-page risk scenario documents—that are easy to review and understand, and that generate a high level of buy-in from key stakeholders, who are then comfortable relying on ERM information for decision making
- Provides a more robust and integrated picture of potential impacts of decisions, ranging from strategic planning to budgeting to risk mitigation
- Has an ERM model that
  - Is constructed by those with ERM modeling experience to strike just the right balance: robust enough to be relied on for decision making yet practical and transparent enough to generate buy-in (without which decisions do not occur)
  - Projects key metrics—and the risk impacts to these metrics—over a long-term time horizon, fully assessing risk and allowing ERM information to inform national decisions, some of which take a full generation to reveal their impacts
  - Has fully dynamic risk exposures that can rapidly be changed to reflect changes in the environment or internal decisions

# 7 RISK MESSAGING

The risk messaging process cycle step consists of two activities:

- Internal risk messaging
- External risk messaging

These activities involve a high degree of customization for each federal government and will not be explored in great depth in this paper.

## 7.1 INTERNAL RISK MESSAGING

Internal risk messaging involves integrating ERM information into performance analytics and incentives. The way in which this is done will conform to the rules, guidelines and culture of the specific government. However, ERM information provides a better lens through which to evaluate and reward performance, and it should be leveraged to do so. For example, where balanced scorecards are used for performance management, ERM can better inform the setting of the relative weights of each metric within the scorecard, because the ERM model can calculate the relative impact of enhancements to each of these metrics. (This is ironic, because the balanced scorecard is fundamentally "unbalanced" in that the weights are often set arbitrarily and result in a lack of appropriate balance of focus, or prioritization, of efforts.)

Internal risk messaging also involves integrating ERM information into internal reporting within the federal government. Again, the way in which this is done will correspond to the specific reporting culture. However, ERM information provides better alignment throughout federal government efforts and should be socialized, most likely slowly over time, until it gains traction and shifts from supplemental information to more prominent usage and reliance.

## 7.2 EXTERNAL RISK MESSAGING

External risk messaging involves integrating ERM information into communications with external stakeholders. Examples include oversight committees and any independent or semi-independent governance structures.

Another key stakeholder is the public. Federal governments should select the information most suitable for sharing; for example, they may wish to report to the public on enhancements to selected key metrics and also some information on mitigation initiatives launched to enhance projected key metrics. They would likely not share information on most key risks and scenarios.

# 8 MAINTAINING THE ERM PROGRAM

Section 3 pledged to first discuss how to initially implement our ERM approach and how to maintain it on an ongoing basis. We have now completed the discussion of the implementation and will move on to maintaining the ERM program.

The critical quantitative ERM information—the key risks (those that are part of the risk quantification) and/or key risk scenarios (the deterministic scenarios that describe the key risks: the events, the shocks and their impacts on key metrics and their likelihoods)—is updated with changes in the environment or internal decisions. Whenever there is a material change in either the environment or internal decisions that potentially impacts the key risks or key risk scenarios, the head of the ERM program—typically the chief risk officer (CRO)—does the following:

1. Reviews the list of key risks and, for those that are potentially impacted, contacts the subject matter expert(s) with whom the failure modes and effects analysis (FMEA) risk scenario development interviews (Interview #2) were conducted, and discusses what changes, if any, are needed.[17]
2. Reviews the list of non-key risks and, for those potentially impacted to an extent that would elevate them to key risk status, identifies relevant subject matter expert(s) and conducts FMEA risk scenario development interviews.
3. Considers whether any new key risks should be added and, if so, identifies relevant subject matter expert(s) and conducts FMEA risk scenario development interviews.
4. Enters any changes to key risks and key risk scenarios in the ERM model to calculate updated outputs: baseline projection of key metrics, individual risk scenario quantification and enterprise risk exposure.

These steps are easily and rapidly completed, allowing the ERM model and process to support decision making. In terms of mitigation-related decision making, the newly updated risk exposures can be reviewed to confirm that they are still within their risk limits (enterprise risk exposure within risk appetite and sub-enterprise exposures within risk limits). More important, from a routine business decision-making perspective, we essentially have a dynamic strategic planning tool: we can produce, on a virtually real-time basis, the updated baseline strategic plan (baseline projection of key metrics) as well as the likelihood of achieving it (as expressed in the ERE pain points).

# 9 POSITIVE TRENDS IN NATIONAL RISK MANAGEMENT

In recent years, there has been a trend to advance ERM practices in government. The following are some examples of these positive trends:

- In May 2014, the Organisation for Economic Co-operation and Development adopted a recommendation ("Recommendation of the Council on the Governance of Critical Risks"[18]) that all participating countries should implement national risk management.
- In July 2016, the U.S. Office of Management and Budget revised its Circular No A-123 on "Management's Responsibility for Enterprise Risk Management and Internal Control,"[19] requiring all executive agencies of the federal government to implement and maintain an ERM program and encouraging all non-executive agencies to do the same. Some of the elements of this directive that represent a step forward are as follows:
  - Defines risks as upside (positive "opportunities") as well as downside (negative "threats")
  - States that ERM should be "coordinated with strategic planning and strategic review process"
  - Defines risk management as "activities to direct and control challenges or threats to achieving an organization's goals"
  - States that effective risk management is part of decision making, including effectively prioritizing resource allocations to ensure successful mission delivery
  - Requires development of a risk profile—a type of key risk list—and specifies that it will be used to inform changes in strategy, policy, operations and the President's Budget
- In September 2017, the COSO ERM approach—widely used in government—was overhauled. The new version attempts a shift toward a value-based ERM approach in two ways: (1) it defines risk as a deviation from strategic plan goals, and (2) it defines risk by its originating source.

# 10 THE ROLE OF A NATIONAL CHIEF RISK OFFICER

A national chief risk officer (NCRO) is essential for a national ERM program to be successful. The NCRO serves three main types of functions:

1. Leads activities
2. Maintains consistency
3. Builds buy-in

## 10.1 LEADS ACTIVITIES

The NCRO and staff must lead the activities required to implement and maintain the ERM program. The NCRO is responsible for leading a wide range of ERM activities, which were described in this paper and are summarized here:

- ERM framework
  - Developing, implementing and maintaining the ERM framework itself, which delineates the approach as well as the individual process steps and activities and how they interrelate
- Risk governance
  - Determining key ERM roles and responsibilities and organizational structure; developing, maintaining and implementing ERM policies and procedures
- Risk identification
  - Developing a risk categorization and definition (RCD) tool
  - Qualitative risk assessment (QRA)
    - Conducting QRA interviews (Interview #1)
    - Facilitating a QRA consensus meeting
  - Emerging risk identification
    - Monitoring known non-key risks with key risk indicators (KRIs)
    - Coordinating environmental scanning for unknown risks
- Risk quantification
  - Developing baseline ERM models to dynamically project baseline key metrics associated with critical national objectives and to support individual risk scenario quantification (IRSQ) and the calculation of enterprise risk exposure (ERE)
  - Conducting failure modes and effects analysis (FMEA) risk scenario development interviews (Interview #2) with subject matter experts to develop, for each key risk, multiple deterministic individual risk scenarios that capture holistic/realistic events, multiyear impacts on key metrics and likelihoods
  - Quantifying individual risk scenarios
  - Quantifying ERE
- Risk decision making
  - Providing information to support mitigation-related decisions
    - Facilitating a risk appetite consensus meeting to quantitatively define risk appetite (maximum acceptable level of ERE) and risk limits (maximum acceptable level of selected sub-enterprise risk exposures)
    - Supporting decisions to manage ERE to within risk appetite

    - Supporting decisions to manage sub-enterprise risk exposures to within risk limits
  - Providing information to support routine decisions
    - Integrating ERM information into strategic planning, budgeting and other routine decisions
- Risk messaging
  - Internal: Integrating ERM metrics into performance measurement and management
  - External: Developing reports for external stakeholders, such as oversight bodies, the public and allied nations

The scope of the preceding activities should make it apparent that a dedicated leader (NCRO) is needed to lead these efforts. However, as noted along the way, there are also subtle complexities to performing many of these activities. Orchestrating a successful ERM implementation requires an NCRO with knowledge, experience and skill in a variety of areas, such as the following:

- Enterprise risk management
- Risk measurement and management, with preferred expertise in at least one of the following:
  - Strategic risk, such as strategy development risk, strategy execution risk, competitor risk, regulatory risk, supplier risk, governance risk
  - Operational risk, such as human resources risk, technology risk, natural disasters (for example, pandemics and extreme weather events), manmade disasters (for example, war and terrorism), process risk, compliance risk
  - Financial risk, such as market risk, credit risk, liquidity risk, commodity price risk, currency risk, economic risk
  - Insurance risk, such as unexpected changes in morbidity, unexpected changes in mortality/longevity
  - Demographic risk, such as unexpected changes in reproductive and working-life patterns, unexpected changes in emigration/immigration
- Modeling, including dynamic projections of multiple interacting variables over extremely long time horizons
- Development of credible assumptions suitable for both near-term and long-term projections
- Leadership through gaining buy-in from key stakeholders
- Management, including project management and coordination of a disparate set of personnel with both formal and informal reporting relationships
- Communication
  - Expertise in the Socratic method and understanding of unconscious and cognitive biases needed for the QRA interviews (Interview #1) and FMEA risk scenario development interviews (Interview #2)
  - Ability to interact with a diverse range of stakeholders of varying levels of authority
  - Ability to comprehend, and be understood by, a range of technical professionals

For ERM information to be credibly received, the NCRO must also have and exhibit the highest degree of ethical integrity. This is critical for ensuring that he or she will maintain an honest, unbiased and agnostic approach to the analysis and interpretation of the information produced, as well as its messaging to both internal and (as feasible) external stakeholders such as oversight bodies, the public and allied nations.

A final consideration is that the NCRO role should have independence to protect against undue influence by internal stakeholders. This can be achieved in various ways, such as appointment by the president (or equivalent most senior executive branch member) and/or long-term appointments that can only be terminated for cause.

## 10.2 MAINTAINS CONSISTENCY

A key tenet of ERM is that activities are performed in a consistent way. An NCRO is needed to act as a focal point to corral efforts and ensure consistency of approach, language, methods, tools and techniques across all ERM activities. Without this consistency, it is impossible to look across the organization and get a cohesive view: metrics are not calculated on a consistent basis, reliable comparisons and prioritizations cannot be made, measurements cannot be aggregated, information cannot be effectively reported and optimal risk-reward decisions cannot be achieved. The need for consistency is such a central aspect of ERM that, when an organization lacks a single CRO function, this is a clear signal that true ERM is not taking place.

## 10.3 BUILDS BUY-IN

Like any other change management effort, it is paramount that key stakeholders buy into the ERM approach for its implementation to be successful. An NCRO is needed to champion efforts to generate a critical level of buy-in. Our ERM approach has several design features (described in this paper) that make buy-in easier to achieve. However, it is not enough to have an effective approach. An effective messenger is also needed. An NCRO builds direct relationships with key stakeholders, explains how the ERM program supports each stakeholder's goals, builds the bridges between information accessible to stakeholders and that needed by the ERM program, and over time builds the trust needed to support decision making at the highest levels.

# APPENDIX

RISK CATEGORIZATION AND DEFINITION (RCD) TOOL (PARTIAL AND ILLUSTRATIVE ONLY)

| Risk Category | Risk Sub-category | Description |
|---|---|---|
| **Strategic** | | **A category of risks related to items of strategic importance (often, differentiators of success/failure versus competitors)** |
| Strategic | Budgeting—Strategy | Federal budget strategy not as viable as expected (e.g., flawed assumptions in budgeting process) |
| Strategic | Budgeting—Execution | Federal budget strategy not implemented as expected (e.g., funds approved/allocated insufficient to fund critical national objectives) |
| Strategic | Governance | Governance not functioning as expected (e.g., no productive working relationship between governing powers/parties) |
| Strategic | Executive branch—Performance | Performance of executive branch not as expected (e.g., failure to deliver on campaign promises) |
| Strategic | Legislative / regulatory—Strategy | Legislative/regulatory strategy viability not as expected (e.g., laws or regulations not aligned with desired outcomes) |
| Strategic | Legislative / regulatory—Execution | Legislative/regulatory strategy not implemented as expected (e.g., failure to pass intended laws or regulations in the form expected) |
| Strategic | Border control agencies—Strategy | Strategy for controlling borders not as viable as expected (e.g., suboptimal investments and/or location of border control personnel, infrastructure and technology) |
| Strategic | Border control agencies—Execution | Execution of border control strategy not as expected (e.g., inability to intercept illegal goods at expected level) |
| Strategic | Defense agencies—Strategy | Military strategy viability not as expected (e.g., choices of investments in human capital and equipment/technology not suited to emerging threats) |
| Strategic | Defense agencies—Execution | Military effectiveness not as expected (e.g., new training or equipment not as effective as expected) |
| Strategic | Intelligence—Quality | Quality of intelligence information not as expected (e.g., failure to gather and analyze data as expected) |
| Strategic | Intelligence—Availability | Availability of intelligence information not as expected (e.g., failure to share information within nation or between allied nations) |
| Strategic | Terrorism | Unexpected change in terrorist strategy and execution effectiveness, including both armed and cyberconflicts (e.g., unforeseen methods) |
| Strategic | War—Strategy | Viability of strategy for existing war, including both armed and cyberconflicts, with other nation(s) not as expected (e.g., suboptimal choice of approach, usage of military branches and weaponry, targets) |
| Strategic | War—Execution | Execution of existing war, including both armed and cyberconflicts, with other nation(s) not as expected (e.g., inability to effectively execute strategy) |

CONTINUED

| Risk Category | Risk Sub-category | Description |
|---|---|---|
| Strategic | War—New conflict | Unexpected outbreak of war, including both armed and cyberconflicts, with other nation(s) (e.g., unexpected attack by adversary) |
| Strategic | Agriculture/food agencies—Strategy | Agriculture strategy not as viable as expected (e.g., suboptimal selection of regulatory incentives) |
| Strategic | Agriculture/food agencies—Execution | Agriculture strategy not implemented as expected (e.g., regulatory incentives not as effective as expected) |
| Strategic | Health care agencies—Strategy | Strategy for national or market-based health care system not as viable as expected (e.g., flawed assumptions in health care strategy) |
| Strategic | Health care agencies—Execution | Execution of health care strategy not as expected (e.g., regulatory incentives fail to enhance access and/or reduce costs) |
| Strategic | Health care—Access | Unexpected change in citizenry access to health care system (e.g., increase in health care costs) |
| Strategic | Health care—Quality | Unexpected change in quality of health care practices/ technology (e.g., new more effective treatments) |
| Strategic | Lifestyle habits | Unexpected change in citizenry lifestyle habits, such as nutrition, smoking, drinking, and drug usage (e.g., higher-calorie diets or increase in drug use) |
| Strategic | Economic policy agencies—Strategy | Economic strategy not as viable as expected (e.g., flawed approach to stimulating economy due to misinterpretation of emerging economic conditions) |
| Strategic | Economic policy agencies—Execution | Economic strategy not implemented as expected (e.g., failure of economic stimuli to produce desired economic growth) |
| Strategic | Monetary policy agencies—Strategy | Monetary policy strategy not as viable as expected (e.g., suboptimal choice of actions based on misinterpretation of emerging economic conditions) |
| Strategic | Monetary policy agencies—Execution | Monetary policy strategy not implemented as expected (e.g., failure of actions to produce expected employment, inflation and interest rates) |
| Strategic | Trade policies—Strategy | Trade policy strategy not as viable as expected (e.g., suboptimal choice of trading partners) |
| Strategic | Trade policies—Execution | Trade policy strategy implementation not as expected (e.g., failure of trade agreements to produce expected level of trade balance with trading nations) |
| Strategic | Trade competition | Unexpected change in level of foreign competition for national exported goods/services or trade routes |
| Strategic | Tax revenue agencies—Strategy | Tax revenue strategy not as viable as expected (e.g., suboptimal tax structure based on misinterpretation of emerging taxpayer behavior) |
| Strategic | Tax revenue agencies—Execution | Tax revenue strategy not implemented as expected (e.g., failure to get passage of expected changes to tax structure) |
| Strategic | Labor agencies—Strategy | Labor strategy not as viable as expected (e.g., suboptimal choice of policies based on misreading future employment needs) |
| Strategic | Labor agencies—Execution | Labor strategy execution not implemented as expected (e.g., failure of policies to produce expected level of employment) |

CONTINUED

| Risk Category | Risk Sub-category | Description |
|---|---|---|
| Strategic | Immigration agencies—Strategy | Immigration strategy not as viable as expected (e.g., suboptimal choices of number of immigrants and/or types of skills based on misinterpretation of emerging market needs) |
| Strategic | Immigration agencies—Execution | Immigration strategy not implemented as expected (e.g., inability to attract desired number/type of skilled workers) |
| Strategic | Energy agencies—Strategy | Energy strategy not as viable as expected (e.g., suboptimal choice of mix of energy sources and investments) |
| Strategic | Energy agencies—Execution | Energy strategy not implemented as expected (e.g., failure of investments to yield expected energy production levels) |
| Strategic | National alliances agencies—Strategy | Viability of national alliances strategy not as expected (e.g., suboptimal choice of alliances) |
| Strategic | National alliances agencies—Execution | National alliances strategy not implemented as expected (e.g., inability to form desired strength of alliances) |
| Strategic | Diplomacy agencies—Strategy | Diplomacy strategy viability not as expected (e.g., suboptimal choice of diplomatic approach) |
| Strategic | Diplomacy agencies—Execution | Diplomacy strategy not implemented as expected (e.g., inability to effectively engage in desired diplomatic activities) |
| Strategic | Treason | Individual act of treason (e.g., individual revelations of national secrets damaging to national security) |
| Strategic | Cyberattack by non-nation-state | Unexpected cyberattack by non-nation-state (e.g., cybercriminal organization or hacktivist attack) |
| Strategic | Propaganda—Foreign | Dissemination of biased/false information by a foreign nation, organization or individual that skews public perception (e.g., foreign nation propaganda falsely claiming that nationally produced goods are of poor quality) |
| Strategic | Propaganda—Domestic | Dissemination of biased/false information by a domestic organization or individual—political, corporate, or special interest group—that skews public perception (e.g., domestic security company propaganda falsely claiming high crime rate) |
| Strategic | Etc. | Etc. |
| **Operational** | | **A category of risks related to items of routine operations (typically, including human resources, technology, processes and disasters)** |
| Operational | Law-enforcement agencies—Strategy | Law-enforcement strategy viability not as expected (e.g., suboptimal investment in personnel, training, tools/techniques, and technology) |
| Operational | Law-enforcement agencies—Execution | Law-enforcement strategy not executed as expected (e.g., inability of law enforcement to keep crime level within expected parameters) |
| Operational | Civil unrest | Unexpected change in level of civil protests (e.g., masses of citizens gathering in sustained violent protests) |
| Operational | Organized crime | Unexpected surge in organized crime (e.g., drug cartel) |
| Operational | Piracy | Unexpected change in level of piracy of ships |
| Operational | Corruption | Corruption in executive, legislative or judicial branch officials or staff (e.g., elected official who takes bribe to subvert legislation that would have benefited the public) |

CONTINUED

| Risk Category | Risk Sub-category | Description |
|---|---|---|
| Operational | Fiduciary or ethical breach | Breach of ethical or fiduciary responsibilities by a government official, employee or contractor (e.g., elected official favors a special interest over the citizenry) |
| Operational | Fraud | Internal or external fraud (e.g., theft of government funds) |
| Operational | Federal courts—Effectiveness | Judicial system effectiveness not as expected (e.g., failure of court system to handle volume of cases expected) |
| Operational | Infrastructure agencies—Strategy | Infrastructure strategy not as viable as expected (e.g., suboptimal type or location of investments based on a misinterpretation of future needs for roads, bridges, tunnels, airports, etc.) |
| Operational | Infrastructure agencies—Execution | Infrastructure strategy not implemented as expected (e.g., inability to achieve the expected level of improvements in infrastructure) |
| Operational | Transportation agencies—Strategy | National transportation strategy not as viable as expected (e.g., suboptimal investments based on incorrect assumptions about emerging transportation needs) |
| Operational | Transportation agencies—Execution | National transportation strategy not implemented as expected (e.g., inability to rebuild roads/bridges at expected cost) |
| Operational | Transportation innovation | Innovation in transportation (vehicles or infrastructure) that results in unexpected change in safety level (e.g., self-driving vehicles) |
| Operational | Telecommunication agencies—Strategy | Telecommunications strategy not as viable as expected (e.g., suboptimal investment in technology due to misinterpretation of future needs) |
| Operational | Telecommunication agencies—Execution | Telecommunications strategy not implemented as expected (e.g., failure of policies to regulate telecommunications effectively) |
| Operational | Education agencies—Strategy | Education strategy not as viable as expected (e.g., suboptimal emphasis of public education curriculum) |
| Operational | Education agencies—Execution | Education strategy not implemented as expected (e.g., failure to achieve desired level of education in general public) |
| Operational | Human resources—Execution | Unexpected change in ability to maintain human resources required (e.g., inability to attract/retain key talent) |
| Operational | External relations | Unexpected changes in relationships with external stakeholders with public voices, such as the media or advocacy groups, or directly with the public (e.g., inability to maintain desired relationship with a key special-interest group) |
| Operational | Technology | Unexpected change in technology (e.g., emergence of new tools that increase likelihood/severity of cyberattack) |
| Operational | Environmental protection agencies—Strategy | Environmental protection strategy viability not as expected (e.g., choices of investments in human capital and equipment/technology not suited to emerging threats) |
| Operational | Environmental protection agencies—Execution | Environmental protection strategy not implemented as expected (e.g., failure of emissions standards to produce desired air quality) |
| Operational | Air/water quality | Unexpected change in air/water quality (e.g., unexpected decrease in air quality due to collective legal pollution) |

CONTINUED

| Risk Category | Risk Sub-category | Description |
|---|---|---|
| Operational | Illegal disposal of toxic waste | Illegal disposal of toxic waste causing pollution to air/water or land contamination |
| Operational | Industrial accident | Accidental pollution of air/water or land contamination (e.g., nuclear reactor core leak) |
| Operational | Crop disease | Unexpected change in frequency/severity of crop disease |
| Operational | Drought | Unexpected change in frequency/severity of droughts |
| Operational | Earthquake | Unexpected change in frequency/severity of earthquakes |
| Operational | Hurricane | Unexpected change in frequency/severity of hurricanes |
| Operational | Pandemic | Unexpected change in frequency/severity of pandemics |
| Operational | Solar flares | Unexpected change in frequency/severity of solar flares |
| Operational | Tsunami | Unexpected change in frequency/severity of tsunamis |
| Operational | Emergency response agencies—Strategy | Emergency response strategy viability not as expected (e.g., choices of investments in human capital and equipment/technology not suited to emerging threats) |
| Operational | Emergency response agencies—Execution | Emergency response strategy not implemented as expected (e.g., new training or equipment not as effective as expected) |
| Operational | Etc. | Etc. |
| **Financial** | | **A category of risks related to external markets and prices (e.g., economic environment, stock market, bond market, and commodity prices)** |
| Financial | Economic | Unexpected change in the economy (e.g., severe economic downturn) |
| Financial | Commodities | Unexpected change in price or availability of commodities (e.g., sudden decrease in availability of non-self-generated critical national resources) |
| Financial | Exchange rates | Unexpected changes in exchange rate (e.g., shift in exchange rates that decreases national exports) |
| Financial | Equity markets | Unexpected changes in equity markets (e.g., stock market crash) |
| Financial | Interest rates | Unexpected changes in interest rates (e.g., sustained low-interest-rate environment) |
| Financial | Credit markets | Unexpected changes in credit markets (e.g., drying up of credit availability) |
| Financial | Counterparty | Unexpected change in creditworthiness of a counterparty (e.g., major national debtor no longer able to repay loans) |
| Financial | Etc. | Etc. |

# ENDNOTES

1. Though some countries do not use a federated system, the concepts explored in this paper are applicable to other national government structures.

2. Committee of Sponsoring Organizations of the Treadway Commission.

3. International Organization for Standardization.

4. We make simplifying assumptions for the sake of illustrating the steps involved in implementing (and maintaining) our ERM approach rather than attempting to advocate for any specific set of key objectives, key metrics, and so on.

5. The life expectancy at birth (LEB) is one of the key metrics used by the Organisation for Economic Co-operation and Development (OECD) to compare population health outcomes between countries (*http://www.commonwealthfund.org/publications/issue-briefs/2015/oct/us-health-care-from-a-global-perspective*).

6. Includes families comprising a single individual.

7. Any deviations, such as downside losses, that are already accounted for in the baseline strategic plan are not considered risks in our ERM context.

8. Industry studies routinely show that strategic risks are the most prevalent (representing about two-thirds of key risks), followed by operational risks and then financial risks. One such study, conducted by the author, Sim Segal, is "Front-Page Risks: Risks Commonly Occurring and Reported in the Canadian News," Joint Risk Management Section, Apr. 2015, *https://www.soa.org/research-reports/2015/research-2015-04-front-page-risks*. A one-year Globe & Mail study: strategic, 65%; operational, 22%; financial, 13%. In addition, all the author's client work has confirmed this same relative importance of risk sources.

9. Simply put, this means that the individual scores did not indicate a consensus—such as might be evident from a normal bell curve of responses—but rather disparate or bipolar results indicating two or more schools of thought.

10. *http://www.fin.gc.ca/pub/ltefp-peblt/report-rapport-eng.asp.*

11. *https://www.cbo.gov/publication/52370.*

12. *https://www.cbo.gov/about/products/major-recurring-reports#2.*

13. It is advisable to have each risk scenario initiate in its earliest possible time period, which is typically within the first projection year (the impacts captured should, of course, include all downstream impacts occurring in all years—in the initiating year as well as all future years).

14. See research study "Disarming the Value Killers," by Deloitte Research: *http://deloitte.wsj.com/cfo/files/2014/05/DisarmingTheValueKillers.pdf*.

15. Another limitation that is nearly universally adopted is that although individual risk scenarios (along with all their potentially multiyear impacts) can recur in future projection years, simulations should be restricted to multiple risk scenarios in which each initiates solely in its earliest possible time period. This is primarily because doing otherwise would result in an exponentially increasing number of convolutions for each successive time period in the projection.

16. In this white paper, the term *correlation* is given its common usage as opposed to its technical usage. Here it denotes a recognition that some pairs of risk events are more or less likely to occur together than their independent likelihoods might suggest. A common approach to adjusting for correlations is to attempt to do so at the risk level. This is flawed, because risk scenarios near the mean are correlated differently than those at the extremes of the risk distribution ("tail" events), and attempts to compensate with further adjustments are ineffective. In our approach, we address correlation at the risk scenario level, which are more accurate, and also reject math-based adjustments in favor of human insight, which, as stated earlier, enhances the accuracy of assumptions.

17. Changes can also include the removal of one or more key risks.

18. *http://www.oecd.org/gov/risk/recommendation-on-governance-of-critical-risks.htm.*

19. *https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-17.pdf.*