



A Risk Lens on Governance

PGEx Workshop, July 3, 2013

A Public Governance Exchange Discussion Paper

Karl Salgo



Institute on
Governance

LEADING EXPERTISE

Institut sur
la gouvernance

EXPERTISE DE POINTE

Introduction

The systematic management of risk is one of many areas of organizational governance, such as internal audit, transparency and increased attention to the responsibilities of directors, whose profile has increased markedly since the 1990s. And as in many of these areas, private sector evolution has inspired changes in public administration. Yet managing risk is hardly a new practice: as pointed out in the *Risk Management Framework for the Government of Ontario*, ancient olive growers who sold their crops at a discount in advance were hedging the risk of a poor harvest.¹

The Geneva-based Organization for Standardization defines risk as “*the effect of uncertainty on objectives*”.² This definition is intended to be neutral – that is, not to characterize risk simply as a threat when it might represent an opportunity. But while this is strictly true, it is not the tenor of most risk management practice. The Government of Ontario’s definition – “the *chance* of something happening that will impact on objectives”³ – implies the element of relative probability. And the Government of Canada’s definition – “the expression of the likelihood and *impact* of an event with the potential to affect the achievement of an organization’s objectives”⁴ – adds the further dimension of the relative severity of consequences. In other words, risk is a kind of vulnerability to organizational goals that is quantifiable in terms of both likelihood of occurrence and severity of impact.

Thus defined, risk of one kind or another is an element of every human enterprise. This point, though simple, needs to be stated explicitly because risk is often perceived as being largely a matter of choice – no doubt because some activities (such as venture capitalism and skydiving) are widely acknowledged to be “riskier” than others and people differ in the levels of aversion to such activities. In fact, for the most part, risk is omnipresent and the key question is how to deal with it.

In the broadest terms the choice is binary: either conscious management or default. Risk management, which the Government of Canada says “*involves a systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions on, and communicating risk issues*”, is essentially a process of being conscious about what is implicit, of attempting to approach on a considered basis what is often done impressionistically.

The IOG’s examination of public sector risk management practices suggests two important tendencies. First, that governance issues constitute a distinct sphere of risk for public sector organizations, particularly the escalation of enterprise-level risks to the

¹ *Risk Management Framework for the Government of Ontario*, p. 14

² ISO 31000

³ *Risk Management Framework for the Government of Ontario*, p. 8

⁴ *Guide to Integrated Risk Management*, Treasury Board of Canada, p. 5



portfolio, government-wide and societal levels. And second, that despite great improvements in public sector risk management practices, the tendency of risk management to focus on the enterprise level means that governance risk may not be recognized and managed as systematically as other risk areas.

A Basic Overview of Risk Management

Differences in taxonomy aside, the basic elements of risk management are widely agreed upon and international approaches to risk management are broadly similar. The Government of Canada definition cited above refers to;

- identifying,
- assessing,
- understanding, making decisions on and
- communicating risks.

The Ontario Ministry of Government Services (MGS)' risk management guidance for agencies sets out the following elements of the Ontario Public Service (OPS) risk management process:

- state objectives,
- identify the risks,
- assess the risks,
- plan and take action, and
- monitor the risks.⁵

The Ontario and Canadian models are consistent with those used by risk management professionals external to government.⁶ Within these and similar frameworks there is scope for a great range of methodologies, and neither the Ontario nor the federal governments specifies a particular methodology for its organizations. However, consistent with most risk management literature, both agree that risk management is not a stand-alone activity but one that must be integrated into broader decision-making structures and processes such as planning, program management, financial reporting and similar key functions.

Explicitly or otherwise, **risk identification** begins with the **identification of organizational objectives**. In a public sector organization, objectives can be challenging to articulate comprehensively, although clearly the organization's formal

⁵ *Guide to the Risk-Based Approach for the Agency Establishment and Accountability Directive, 2010*, Ministry of Government Services, Government of Ontario, February 2011, p. 2

⁶ For example, Orbis Risk Consulting's overview of the Risk Management Cycle includes establishing the context, risk identification, risk analysis, risk evaluation and risk treatment, with monitoring and review and communication and consultation identified as practices employed throughout the cycle.



mandate will serve as the starting point. Of particular relevance to governance risks, the MGS guide for agencies notes that “agency objectives will not necessarily be parallel to the ministry’s objectives” and indicates that “competing ministry and agency objectives” should be identified.⁷ At the federal level, the Treasury Board (TB) framework notes that TB policy instruments “should target risks linked to achieving federal government *management* objectives”.⁸ Risk identification can be approached in a variety of ways (e.g., quantitative tools such as forecasting models to qualitative ones such as questionnaires and workshops) and entail varying degrees of staff engagement (e.g., from analysis by specialists to more broadly based like surveys). But even qualitative assessments should rely as much as possible on verifiable information rather than impressionistic approaches. Risk perceptions often fail to survive careful scrutiny informed by hard data (consider the phenomenon of the traveler who speeds to the airport while fretting about the dangers of flight).

Risk assessment can be approached in a variety of ways, though as state in the Treasury Board guidance, “at a minimum, analyzing the risks typically involves assessing the likelihood of the risk occurring and the impact on objectives should the risk occur”.⁹ Even such a minimal assessment would enable the organization to map risks on a quadrant (low risk, low impact; low risk, high impact; high risk, low impact; high risk, high impact) that would assist in prioritizing the risks that need to be the focus of active responses and in assigning responsibility for those risks (e.g., high risk, high impact items would likely be expected to receive active ongoing attention from senior management and the board). There are of course numerous other ways in which organizational risks can be mapped.

A more thoroughgoing assessment process would include explicit analysis of the costs and benefits of addressing the risks in question (a process that will likely take place implicitly even if it is not done systematically). “Costs” will include not only direct outlays such as insurance premiums, but opportunity costs as well as. For example, the organization should consider the kinds of activities the risks are linked to and how fundamental these activities are to organizational objectives. This will help inform the articulation of a considered **risk tolerance** “philosophy” – e.g., certain relatively high risks may be considered tolerable because they are linked to activities fundamental to organizational mandate while lesser risks may not be tolerated because the opportunity costs of forgoing the associated activities are low. It is important that questions of this nature be considered at the senior-most levels in the organization; without leadership and clarity in these matters (both of which require open communication) such issues are likely to be determined largely by default.

⁷ Ibid, p. 3

⁸ *Framework for the Management of Risk*, Treasury Board of Canada, p. 3 (italics added)

⁹ *Guide to Integrated Risk Management*, Treasury Board of Canada, p. 17.



Strategies for **responding to risks** – the centerpiece of risk management – can be variously expressed but will broadly fall into four categories. The US Department of Defense uses the convenient acronym ACAT to describe risk management practices in military acquisition: **Avoid, Control, Accept, Transfer**.¹⁰ **Avoidance** refers to the decision not to engage in an activity because of the associated risks; this is widely perceived to be the most characteristic public sector response. **Control** refers to specific mitigation strategies aimed at reducing the likelihood and/or severity of a negative impact. Physical security and safety measures would be an example of this approach. Typical **transfer** practices include insurance and other hedging practices (e.g., maintenance of a foreign currency account to manage short-term currency risks), although logical purists will point out that the risk is not technically “transferred”, but rather that compensatory arrangements are purchased. **Acceptance** essentially refers to the recognition that a given risk is best absorbed given the relative cost-benefits of active management (the deductible portion of an insurance contract being a straightforward example). Implicit in this characterization is the reality that risk can be over managed – i.e., where overall costs of managing the risk outweigh the likelihood of occurrence and probable severity of impact.

Ongoing **risk monitoring** is a further key element of risk management. Again, this can be done more or less systematically but at a minimum should entail the identification of key indicators, whose progress can be followed through such tools as dashboards and “risk heat maps”. Among the merits of such tools is the potential for effective communication to an appropriately broad audience.

Public Sector Challenges

While most if not all generic risk management principles and practices can be applied to the public sector, public sector institutions also face distinctive risks and a distinctive risk management environment.¹¹

It has been argued that the very mandates of public sector organizations discourage risk management – that, for example, an organization mandated to underwrite risks that the market won’t assume (say deposit or export insurance, small business financing or personal income security) does not readily withdraw from areas where the usual risk management calculus suggests it should. However, when risk is conceived in terms not simply of financial loss but of vulnerability of organizational objectives, there is no contradiction between absorbing societal risks and managing organizational ones. That said, the argument does underscore the fact that public sector

¹⁰ See Defense Acquisition University, *Glossary: Defense Acquisition Acronyms and Terms*, 13th edition, Nov. 2009, p. B-158ff and *Risk Management Guide for DOD Acquisition*, Aug. 2006.

¹¹ Some of the ideas put forward in this section draw on *Strengthening Risk Management in the US Public Sector*, McKinsey Working Papers on Risk, Number 28, May 2001.



organizations often have multi-faceted missions that can complicate the assessment of objectives and risks.

A closely related concern is that the metrics of success and failure are murkier in the public sector, where the bottom line is almost never the exclusive concern. Yet this is a complicating factor but hardly an insurmountable one. It may require greater reliance on qualitative assessment, but ultimately this is a problem of public sector performance management rather than of risk management per se.

Another purported challenge for public sector organizations is the relatively high level of discontinuity in leadership. The argument has been made that deputy ministerial tenure, at least at the federal level, has been short in recent years by long-term historical standards (systematic comparisons to private sector norms have been less common).¹² Perhaps more significant is that leadership changes at the political level can require a reorientation of organizational objectives (albeit usually within the framework of a statutory mandate). However, this reality is best viewed, not as a roadblock to risk management, but rather as a form of governance risk (policy misalignment) to be managed, as discussed below.

Beyond such specific challenges, a more general argument has been made that public sector “culture” is not well adapted to risk management, at least in part for reasons that have already been noted – e.g., public sector institutions’ own status as instruments of risk management cause them to view government as a natural absorber of risk. Additionally, public servants are often perceived to be more “mission focused” than management focused.

However, to the extent that such thinking was ever true, it appears to be out of date, at least in a Canadian context, given the emphasis in recent years on fiscal restraint, comptrollership and accountability – an emphasis that has to a considerable extent been enshrined in legislation. A casual empiricism suggests that, far from being complacent about risk, public servants tend to be hesitant about confronting it and engaging in the relatively bold calculus needed to agree on and operate within appropriate levels of risk tolerance. Further, while the literature consistently emphasizes the importance of forthright communications about organizational risks and the organization’s risk management philosophy, open communication in this area is not characteristic of core public service culture.

¹² This assertion has been subject to some scrutiny suggesting that the reality is more nuanced than conventional wisdom might suggest. See for example: *Is Deputy Churn Myth or Reality?* Public Policy Forum, November 2007.



A Risk Lens on Governance


In referring to a risk lens on governance, this paper is not concerned with *governance of the risk management function* – that is, with issues such as who is responsible for what (policies versus processes and tools, implementation and monitoring), the establishment of committees and working groups, reporting and accountability and the like. Important as that line of inquiry could be in identifying useful practices, our focus is on *the management of governance related risks*.


In this connection, we start with the observation that there is a range of risks that pertains directly to organizational governance; this includes but goes well beyond risks to the effectiveness of governance structures such as a potential loss of board or senior management capacity. Looking at the risk categories identified in Figure 1 below, policy alignment, accountability, values and ethics, and legitimacy could all be considered governance risks.

Figure 1

How does risk shift? What's material at what level?

Risk/ Level of Government	Financial	Operational	Reputational	Performance	Policy Alignment	Accountability	Values and Ethics	Legitimacy
Division								
Agency								
Portfolio								
Whole of Government								

 Institute on
Governance
LEADING EXPERTISE

 Institut sur
la gouvernance
EXPERTISE DE POINTE



The extent to which governance risks are recognized as such varies. In this respect, Government of Ontario Guidance is more explicit than that of the Government of Canada. Ontario's risk management guidance for agencies specifies "Accountability/Governance" as a risk category, and defines it to include:

*Risk that the organizational structure, accountabilities, or responsibilities are not defined, designed, communicated or implemented to meet the organization's objectives, and/or that culture and management commitments do not support the formal structures. Risk of conflict of interest for board members. Inadequate ethics/codes of conduct. Inadequate definitions of roles and responsibilities. Risk of failure to comply with administrative requirements, such as directives.*¹³

Additionally, Ontario's definition of the "Strategic" risks category includes what could also be considered a major governance risk: "Risks related to implementing (or not implementing) new policies or changes to existing policies (e.g., misalignment of agency policies with OPS policies)".¹⁴

Without an explicit risk taxonomy, there is a danger that governance risks will not be addressed in the most appropriate way or will go unrecognized altogether. For example, most organizations will attempt to identify "strategic" risks, but at an enterprise level "policy misalignment" (i.e., misalignment with broader government policy objectives) will not necessarily figure among them, especially if the organization looks principally to private sector risk management models. Other risks, such as legitimacy (or loss thereof), will not necessarily even make it onto the radar screen at the enterprise level, despite the fact that organizational legitimacy is a key element of sound public sector governance and one that can be diminished or lost altogether in the context of a controversy or scandal of comparatively limited financial or operational significance. (Recent developments the Canadian Senate providing a conspicuous example.)

Our concern here about the adequacy (or inadequacy) of conducting public sector risk management exclusively at the "enterprise level" is critical. One of the key findings PGEx has made in applying a risk lens to public sector governance is that **enterprise or agency level risk management in the public sector tends not to take sufficient account of the individual institution's potential to contribute to broader systemic risks.**

Individual institutions develop their own culture and language that impacts heavily on their view of risk. The resulting diversity of perspectives constitutes a major governance challenge in a public sector context. This is so because a great deal of public authority

¹³ *Guide to the Risk-Based Approach for the Agency Establishment and Accountability Directive, 2010*, op-cit. p. 8.

¹⁴ *Ibid.*, p. 9.



is delegated to bodies that have varying degrees of independence (distributed governance bodies or DGOs) and often relatively narrow mandates but which are nonetheless part of a larger government organism for which ministers and governments retain overall accountability.

For example, in the private sector, hiring consultants is not necessarily perceived as a risk of any kind, and in any case not in the way that it may be in the public sector. When a DGO is mandated to operate at least partly on commercial terms and is significantly influenced by private sector norms, its enterprise-level assessment is unlikely to view the risk the same way that the portfolio department might, and in the absence of a distinct “governance” lens framework, its assessment is unlikely to go beyond enterprise level concerns. By the same token, the responsible department or ministry needs to support and foster portfolio-wide and whole-of-government thinking, or, differently put, to consider various kinds of misalignment by DGOs among its own risk areas and to manage them accordingly.

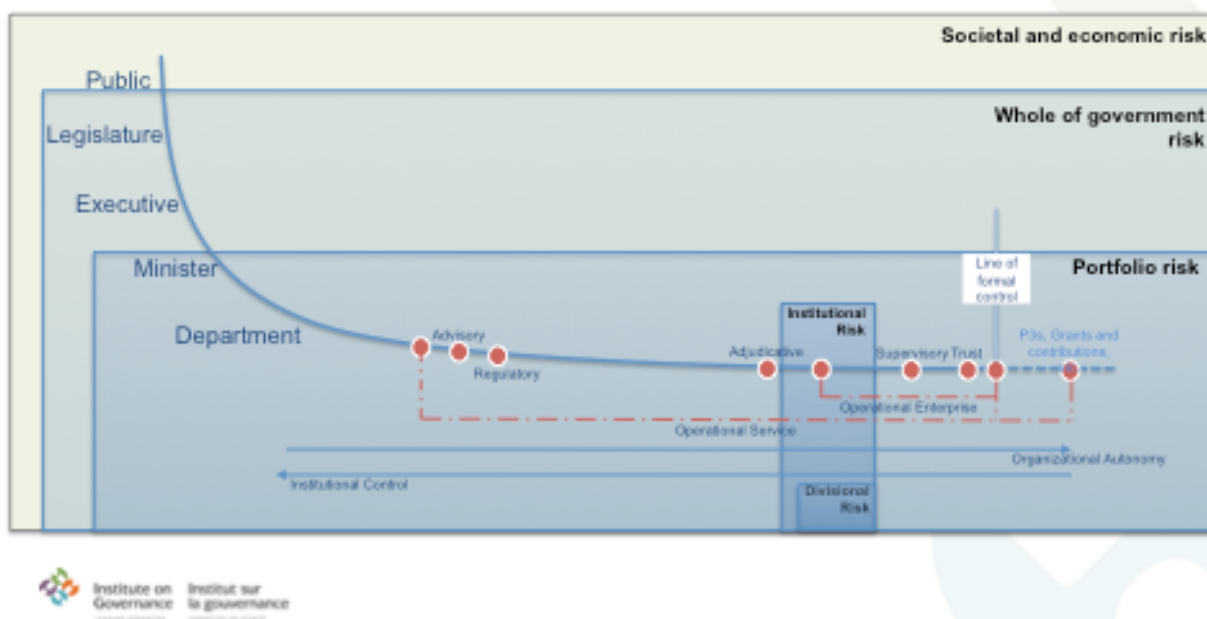
The failure to engage in this kind of risk analysis at the enterprise level was arguably one of the issues plaguing eHealth Ontario, possibly with a corresponding failure to manage risk at the ministry level. While this could also be characterized as an oversight failure, it could equally be said that (1) oversight failure is itself a governance risk and (b) oversight is typically understood in terms of compliance, and risks of this sort are not necessarily about the failure to comply with formal requirements.

Financial issues rightly receive a lot of attention in risk management, but not necessarily as governance risks. Yet financial matters have a particular potential to escalate from the enterprise level. Expenditure practices with almost no materiality at the level of organizational budgets and no *direct* capacity to interfere with operational effectiveness or mission objectives can become serious reputational issues at the departmental/ministry level and even the whole-of-government level. In doing so, they can rebound back to the organization as legitimacy issues and, in extreme cases, have a societal impact as the organization loses capacity to deliver on its mandate.

Figure 2 illustrates the potential escalation of issues from the enterprise (and indeed divisional) level through the societal level, including the fact that this escalation entails a corresponding escalation of the level of accountability – from organizational CEO to Department/Ministry and Minister, to the whole of the executive and the First Minister, and potentiality to the legislature.

Figure 2

Different Levels – Different Risks



This shifting of risk is not one-directional – it is not simply a matter individual organizational activities escalating “upwards”. Clearly, decisions made at the ministerial and government-wide level – and not perceived as risks at all at that level – can constitute serious risks for individual organizational objectives. For example, at the ministerial/government level, a large reduction in organizational appropriations is more likely to be seen as a decision furthering objectives than as a risk, though plainly it would factor as a risk at the enterprise level. Thus if one were to map specific potential occurrences on the table in Figure 1, it is entirely possible that they would be differently described at different levels.

Conclusion: Implications for Practice

As already noted, it is useful to identify governance risks as such, starting with the development of a governance risk taxonomy, as the first step in managing these risks. But the distinctive feature of governance risks is their connection to inter-organizational relationships: they flow at once from (1) the autonomy that characterizes a majority of public sector organizations and corresponding potential for misalignment of objectives

at different levels, and (2) the simultaneous interconnectedness of organizations as part of a larger whole, with a single ultimate locus of accountability. This means that any conscious management of governance risk has to be to some extent coordinated beyond the enterprise level. And while the kind of guidance provided by the Government of Ontario at least forces conscious consideration of such issues, their effective management would require not only assurances of due diligence at the agency or enterprise level, but also systematic collective engagement.

Risk management literature and public sector guidance devotes a great deal of attention to the importance of open communications about risk and the full (albeit differentiated) engagement of everyone in the organization in its active management. However, it is far from clear that this kind of communication and engagement is actively practiced throughout the public sector. As a minimum starting point there would be value in ensuring that new entrants into the senior ranks of agency management (particularly those drawn from outside the public sector) receive clear orientation in the area of governance risk.

Issues for Discussion

1. Is risk openly discussed in your organization and is everyone engaged in its management consistent with their level of responsibility? Do you think there are cultural or other systemic obstacles to this in the public sector?
2. Does your organization identify governance risks as such? Do you think that risk areas such as values and ethics, policy alignment and escalation are managed as systematically as other risks to organizational objectives such as financial risks? Are they capable of the same kind of management?
3. How do governance risks differ from a departmental/ministry perspective versus the perspective of a distributed governance organization? Are departments/ministries as vulnerable to governance risks, or is their main concern the effective management of such risks in DGOs?
4. What kinds of practices might improve portfolio-wide and whole-of-government risk management without impeding on DGO autonomy?
5. What if any role do different organizational cultures play in creating or intensifying governance risks? How can cultural differences be managed?

