

## DISCUSSION PAPER PREPARED FOR THE NATIONAL EXECUTIVE FORUM ON PUBLIC PROPERTY

James McKellar, Professor of Real Estate and Infrastructure, Schulich School of Business, York University ([jmckellar@schulich.yorku.ca](mailto:jmckellar@schulich.yorku.ca))

April 15, 2013

### RISK MANAGEMENT: A FRAMEWORK FOR DISCUSSION

**Risk** is the potential that a chosen action or activity will lead to an unintended loss or an undesirable outcome. Risk is defined in many ways depending on the industry or activity to which the risk applies. Managing risk is based on prediction and in the words of the preeminent scientist Niels Bohr:

*Prediction is very difficult, especially if it's about the future.*

Managing risk requires predicting events in the future, particularly unlikely ones that have not previously occurred. Risk management has been with us as long as risk itself, but it is only when massive failure occurs that we are reminded of the impacts of risk and the need to embrace the measurement, mitigation and management of risk. The financial crisis that erupted in 2007 in the US and then spread across the globe, revealed a major gap in prevailing financial risk mitigation systems. This gained the attention of many organizations well beyond the financial sector. In the past decade, organizations, both public and private, have been forced to think more deeply on how to incorporate risk management into their business strategies and execution frameworks.

What is not always understood is that risk management is directly linked to the broad strategic goals of an organization; it is not a compliance function to be delegated to risk professionals in their own silo. Risk management is about identifying, avoiding, and overcoming hurdles that strategy may encounter along the way. Avoiding risk does not advance strategy, but it can remove obstacles and barriers that may impede progress toward a strategic destination<sup>1</sup>.

### CATEGORIES OF RISK

Risk may arise from either internal or external influences and may be more or less under the control of the organization. Risks can be divided into three categories based on their degree of predictability, controllability, management, and most important, on the magnitude of their consequences to the enterprise<sup>2</sup>.

---

<sup>1</sup> Robert S. Kaplan, *Risk Management and the Strategy Execution System*. Harvard Business School Publishing. Cambridge, Mass. 2009.

<sup>2</sup> Ibid

### **Level 3: Routine Operational and Compliance Risk**

These risks arise from errors in routine, standardization, and predictable processes that can expose the organization to substantial loss. These are the “known” risks. Examples include maintaining and updating financial information systems; ensuring data security; protection from employee fraud; or exposure to regulatory liabilities. Through internal controls, standard operating procedures, and internal audits, organizations should strive for zero defects at this level

### **Level 2: Strategy Risk**

No organization can prosper and flourish while pursuing a risk-free strategy: risk brings reward. To manage risk at the strategy level, an organization must identify the major plausible risks inherent in their strategy; attempt to mitigate and manage those risks; and continually monitor their risk exposure. These risks are the “known unknowns”. There is a long list of risks that fall into Level 2 including financial risk, reputation or branding risk, environmental risk, human resource risk, and information technology risk. These risks imply a complex risk management process, usually specific to each type of risk. Risk management at this level should be anticipatory and preventive, not reactive.

### **Level 1: Global Enterprise Risks**

While Level 2 risk management addresses the “known unknowns”, failure can be triggered by the “unknown unknowns”; the unpredictable and unprecedented occurrences that create existential risk. These are often referred to as “*black swan*” events based on the highly popular book by Nassim Taleb<sup>3</sup>. A severe earthquake, strife in some part of the globe, or the unexpected death of a political leader could precipitate this type of risk. In some situations the best approach to managing global enterprise risk is scenario planning around a set of “what ifs”.

## **RISK MANAGEMENT IN GOVERNMENT**

For most governments organizations, Level 2 and 3 risks are what they are expected to plan for. Fraud or theft might be perpetrated by an employee on external contracts; an IT upgrade may be delayed, over budget, or fail to meet objectives; an environmental hazard such as mold may render a structure uninhabitable; or a bridge or elevated highway may collapse from deferred maintenance. Safeguards in these instances require both financial and non-financial control systems that support risk self-assessment, reasonable forewarning of impending risks and timely response schedules. An essential ingredient for risk management is reliable information delivered in sufficient time for management to take the necessary actions and this is where risk management begins to break down.

---

<sup>3</sup> *The Black Swan: The Impact of the Highly Improbable*, by Nassim Taleb, New York, Random House. 2007.

Governments seldom maintain reliable information systems, including historical data sets. This shortcoming is exacerbated by the inability to document performance outcomes as a feedback to both project management programs and strategic risk management. In particular, project-oriented organizations face difficulties in capturing and transferring knowledge and spreading learning across projects. In many cases the risk profile of an organization is heightened by bureaucratic structures, processes, and incentive structures that reinforce the autonomy of project leaders. This inhibits cross-project learning experiences or shared communications which could serve as cost-effective risk mitigation measures.

### **Risk Management at the Project Level**

At the project level, the major steps involved in risk management are risk identification, risk assessment, and the processes of prioritization and response to risk. At the project level, risk identification can be divided into two parts<sup>4</sup>:

- A *qualitative* analysis that focuses on identification, together with the assessment of risk; and,
- A *quantitative* analysis that focuses on the evaluation of the risk.

The elements of risk management can be broke down into three parts<sup>5</sup>:

1. Risk assessment (including risk identification and analysis).
2. Risk management plan (including risk response and controls).
3. Risk monitoring (including monitoring of the risk management plan, controls effectiveness and communication).

The most challenging aspect of project management is the proper management of risk, or the balancing of potential opportunity against possible loss. Major weaknesses that expose an organization to project risk include inadequate controls that signal potential difficulties early and clearly enough; continued incorrect assessment of the remaining potential risks; wishful thinking; and, unwillingness of management to take swift and appropriate corrective action even when the problem is apparent. The best protection against project risk begins with a clear assessment of the project's chances of success before it is launched, including thorough risk identification and assessment.

Research by Bent Flyvbergh<sup>6</sup> underscores the poor record of government in applying risk management at the level of major capital projects.

- 58 rail projects showed an average 44.7% cost overrun

---

<sup>4</sup> Donna Fletcher and Susan Newell. "A *Technical Note on Risk Management*". Richard Ivey School of Business. 2007

<sup>5</sup> Ibid

<sup>6</sup> A Danish economic geographer, Flyvbergh is Professor of Major Programme Management at Oxford University's Saïd Business School and the founding Director of the University's BT Centre for Major Programme Management.

- 33 bridge projects showed an average 33.8% cost overrun
- 167 road projects showed an average 20.4% cost overrun
- Boston's Big Dig: 275% or \$11 billion over budget
- Pentagon Spy Satellite: \$4 billion over budget
- Denver International Airport: \$200% over budget on \$5 billion project
- Channel Tunnel: 80% over budget for construction and 140% over for financing (compare with 10% contingency assumed by lenders)
- Sydney Opera House: 1,400% over budget
- 90% of rail projects overestimate traffic.
- 25 rail project traffic forecasts had average inaccuracy of -51.4% with SD of 28.1.
- 50% of road project traffic forecasts are wrong by >20%.

### **Risk Management at the Organizational Level**

At the organizational level, risks within government may reflect the organizational culture of a particular ministry, department or agency. No government organization can function on a risk-free basis: new drugs must be approved; new aircraft must be certified; new social programs must be implemented; and new buildings and infrastructure must be built. It is the manner in which they carry out their duties and responsibilities that government entities expose themselves, and those they serve, to some level of risk. This risk can have significant external consequences. An example would be a major data loss that places confidential health information in the public realm and places individuals at risk.

The broader view of organizational risk management is referred to as Enterprise Risk Management (ERM). ERM is a systematic approach to managing risk, which means that risk factors and mitigation programs must be considered on an enterprise-wide basis, internally and externally. The Committee of the Sponsoring Organizations of the Treadway Commission (COSO) provides a framework for ERM that views objectives at the entity, division, business-unit, and subsidiary levels, in four key categories: strategic, operations, reporting, and compliance. The framework focuses on eight interrelated components that are integrated with management processes<sup>7</sup>:

- Internal environment (mission, culture, governance policies)
- Objective setting (strategic, operational, reporting and compliance goals and objectives)
- Event identification
- Risk assessment
- Risk response
- Control activities,
- Information and communications
- Monitoring

---

<sup>7</sup> "Enterprise Risk Management – An Integrated Framework". Committee of the Sponsoring Organizations of the Treadway Commission (COSO), Sept 2004.

Unfortunately, many organizations move forward with measuring operational risks before they contemplate strategic risk<sup>8</sup>. Research indicates that even among the more advanced practitioners of ERM, the focus on enterprise risk management rarely encompasses more than financial, hazard, and operational risks (or those risks that can be quantified)<sup>9</sup>. Most managers avoid systematically addressing strategic risks that can often be a much more serious threat to an organization.

There is a clear link between project risk management and strategic risk management. Project risks can only be effectively ameliorated if risks inherent in the management processes are linked to broader strategic goals<sup>10</sup>. This means learning from past experiences or situations in which risks were mitigated and embedding lessons learned in the organizational culture of the organization itself. Unfortunately, the autonomy with which projects are often executed isolates each experience from the broader organizational context, and can undermine risk management practices.

Kaplan<sup>11</sup> advocates the use of a risk scorecard to link strategic objectives to risk events. While he admits that the development of a risk scorecard is more conjecture and concept than actual fact, he does see this approach as being anticipatory and preventative, not reactive. The scorecard identifies for each strategic objective the primary risk events that would prevent the objective from being achieved. For each risk event, metrics are selected that would lead to early warning or leading indicators of when a risk event might occur.

#### EXAMPLE OF A RISK SCORE CARD <sup>12</sup>

##### Likelihood of the Event

Score Rating	5	4	3	2	1
	Virtually Certain	Likely	Even odds	Unlikely	Remote
Probability of the event occurring within 36 months	95%	75%	50%	25%	5%

##### Magnitude of the Event's Consequences

Score	5	4	3	2	1
Consequence	Highly adverse	Adverse	Moderate impact	Some impact	Little impact

*For each identified risk, managers estimate the likelihood of an event's occurrence and the magnitude of its consequences, usually on a 1-5 scale.*

<sup>8</sup> Stephen Gates and Ellen Hexter, "From Risk Management to Risk Strategy". Conference Board Research Report. No. R\_1361-05-RR, 2004.

<sup>9</sup> Adrain Slywotsky and John Drzik, "Countering the Biggest Risk of All". Harvard Business review, Vol. 83, No. 4, 2005. pp 78-88.

<sup>10</sup> Donna Fletcher and Susan Newell, "A Technical Note on Risk Management". Richard Ivey School of Business. 2007

<sup>11</sup> Robert S. Kaplan, *Risk Management and the Strategy Execution System*. Harvard Business School Publishing. Cambridge, Mass. 2009.

<sup>12</sup> Ibid.

As an example of his Score Card, Kaplan uses risk associated with the skills, experience and knowledge of professionals required to achieve strategic job readiness in an organization. In his score card, this objectives would typically have a metric “percentage of employees in strategic job families rated as ‘very good’ or ‘excellence’ for relevant skills, experience and knowledge”; a target of 90% or higher; and strategic initiatives involving in-class and on-the-job training, a pay-for-knowledge incentive plan, and planned job rotations. The risk events that could threaten this objective could include high employee turn-over or retirements, staffing budget cuts, ineffective training programs, or lack of career mobility.

This is where data and information become important if risk management is to be anticipatory and preventative, and not reactive. On the basis of good historical data, management should be capable of estimating which risk events are the most likely to occur and could have the most adverse consequences to the strategic objectives of the organization. Insurance companies must estimate the probability of events they insure against; financial firms must forecast the likelihood of mortgage defaults in their loan portfolio; and contractors must estimate the impact of future commodity prices in their bid prices.

## **Risk Mitigation**

Governments, by their own admission, have not been effective practitioners of risk management at the project level, and less so at the strategic level. The origins of the dilemma can be traced to many sources, some of which include:

- The diverse range of services governments deliver for which the performance of service delivery cannot be easily measured;
- Mandates that require actions beyond the capability of the existing organization;
- Optimism bias;
- Inability to acquire the required professionals skills and knowledge at prevailing market rates;
- Budgeting systems that simply defer risks well into the future, in return for expediency;
- Lack of information, historical data, or institutional memory;
- Mandated employment practices; or
- Unwillingness to admit to risk (bad connotation), let alone quantify these risks and their consequences, often for political reasons.

In some situations, governments are looking at risk transfer or risk sharing with the private sector to address risks that, by their own admission, they are not capable of managing. This has implications at the project level and for the organization as whole.

Risk transfer or sharing implies two things:

- Added costs in the form of risk premiums and the increased cost of capital where debt is involved. The benefits must be shown to offset the costs involved and this requires the ability to identify, price, and compare the costs of risk mitigation alternatives.

- Ability to attract private partners who have the proven capability to manage the risks to be transferred or shared. Also, private partners must have the confidence in the public's capacity to manage strategic risk as these arrangements are typically long-term.

Risk transfer is based on the premise that risk should be managed by the entity best suited to manage the risk, and at a transfer price that makes the sense in a risk/reward relationship. Examples of project risks that might be transferred or shared include<sup>13</sup>:

- construction price certainty
- scheduling, project completion and delays (phased completion)
- site conditions and contamination
- development approvals
- construction financing
- commissioning and readiness
- activity protocols
- change order protocol
- lifecycle repair and renewal

Risk transfer can be also effective in mitigating risks that occur in situations where there is no integration between capitals costs (CAPEX) and operating costs (OPEX). This is typical of most traditional procurement approaches for capital projects that some refer to as the "Design-Build-Forget" model. Traditional procurement often assumes 0% probability of risk occurring, despite the overwhelming evidence to the contrary as evidenced by the research of Flyvbergh. Empirical evidence shows a much higher probability that risks will occur, particularly in the absence of risk management protocols.

This shortcoming has given rise to the PPP model for capital works that is rapidly gaining popularity in many countries. This universal model is built on highly sophisticated risk transfer model, at the heart of which is the ability to quantify and price risk, assign risk, and sufficiently motivate and reward those who manage and mitigate risk.

---

<sup>13</sup> Infrastructure Ontario; Design, Build, Finance and Maintain Risk Analysis and Risk Matrix, 2007

Infrastructure Ontario adopted a model for pricing risk that was developed in the UK and is the basis of I/Os Value-for-Money exercise. The model serves as an excellent example of the rigours of identifying and quantifying project risks<sup>14</sup>.

In the example, for a \$240 million capital project the public agency would retain \$4.3 million of design coordination/completion risk under a Traditional Procurement model, and transfer this risk entirely under a DBFM model. However, the transfer involves a cost and the potential return from accepting this risk must offset the cost involved.

### Expected Value of Risk Transfer

**EV = cost base x probability x impact**

**Probability can include a statistical distribution of the arisen risk**

Risk Category	Cost Base		Design Build Finance Maintain Model (DBFM)						Traditional Model					
	Portion of DBFM	Value	Probability %	Impact			Risk Quantified		Probability %	Impact			Risk Quantified	
				10 th perct	Typical	90 th perct	Government	Shared		10 th perct	Typical	90 th perct	Government	Shared
Design Coordination/ Completion	Design and Construction	\$240 million	90%	0.5%	1.0%	5.0	\$0	%0	90%	0.5%	2.0%	5.0%	\$4.32 million	\$0

<sup>14</sup> Ibid. Page 9.



## **In Conclusion**

Risk management has pre-occupied and focused business and government leaders since the start of the financial crises in 2007. This crisis brought down some of the best known global private brands including General Motors, Ford, Merrill Lynch and Lehman Brothers. Subsequently, it devastated the economies of Ireland, Greece, Spain, and Portugal. While private organizations focused on shareholder value, revenue and growth, productivity, cost control and quality, few of them, it seems, explicitly incorporated risk. For different reasons, but often with similar consequences, governments also avoided acknowledging risk. What both sectors seemed to enjoy, with unintended consequences, was the high-octane environment of low interest rates where debt accumulation was seen as a risk-free venture.

Today we have the potent reminders of the failures to manage risk: the impact of the Tsunami on a nuclear power plant in Japan; significant infrastructure failures arising from deferred maintenance, or the reputation of an entire government agency being tarnished by leadership that condones a culture of excess. It is now imperative that organizations, both private and public, explicitly account for risk when formulating strategies, and then follow through with processes and procedures to monitor and manage the risks they are willing to assume.

For governments in particular, they must come to grips with the notion that project risk can only be effectively managed, and the risks mitigated, if risk management is linked to the broader strategic goals of the entity. This implies critical links between project and organizational levels, a link that has proven difficult to forge within governments. Above all, effective risk management takes strong leadership and a belief that risk management is a core function in any organization.