Risk Management: Moving the Framework to Implementation

Keys to a Successful Risk Management Implementation Strategy

October 2003
# Table of Contents

Acknowledgements

Executive Summary

Introduction

Background and Context

Findings and Observations

First Steps – How Practical Links were Built between Theory and Practice

Conclusion

The Project Team

Contacts for Further Discussion

## APPENDICES

A. Study Methodology
B. Advisory Committee Members
C. Interview Guide
D. Bibliography
E. Sample Templates and Report Formats
F. Questions to Consider
Acknowledgements

The authors would like to thank the members of the Advisory Committee that provided financial support to this project and input and advice throughout the project. Without their support, this project would not have been possible. These include:

- Canadian Food Inspection Agency;
- Alberta Finance;
- British Columbia Ministry of Finance;
- Nova Scotia Department of Finance;
- Ontario Ministry of Finance;
- Human Resources Development Canada;
- Public Works and Government Services Canada; and,
- Royal Canadian Mounted Police.

We are also deeply grateful for the participation and involvement of those representatives of the government organizations with whom we spoke in the conduct of our study.

- Canadian Food Inspection Agency;
- City of Winnipeg, Manitoba;
- Human Resources Development Canada;
- New Zealand Inland Revenue Department;
- Ontario Ministry of Transportation;
- Ontario Ministry of Environment;
- United Kingdom National Savings and Investment;
- United States Department of the Interior – Office of Air Services; and,
- Victoria Department of Sustainability and Environment (Australia).

We trust that we have reflected their views and insights accurately, yet take full responsibility for the conclusions drawn.
Executive Summary

No one is questioning whether or not government should practice good risk management. The challenge is how to get beyond the concept to application. Increasingly, political leaders and senior officials within government need and expect that effective risk management will be part of how public sector organizations conduct their business.

This study of the implementation of risk management in the public sector is a joint venture of The Conference Board of Canada and Deloitte & Touche with the support and guidance of its sponsors. The findings are based on interviews with nine selected public sector organizations from Canada and abroad. The result of this study is a compendium of useful practices to assist other public sector organizations in successfully implementing risk management policies.

The strategic approach that was identified and most important to public sector organizations was that risk management was seen as a total package of risk identification, risk mitigation and risk communication. Implementation of all three elements was essential to its success and to the advancement of risk management as an effective management tool.

The overall findings were that implementation is an incremental process, built on good training and good governance. Implementation is not driven by elaborate frameworks, but rather through experimentation, a recognition by corporate leadership of its necessity, applied leadership and incorporation into how the public sector organization operates. Risk management is not an add-on; it is an “add-into” the way that public sector organizations are managed.

The key learnings, defined in this study as the bottom line, are:

- Expect a **multi-year implementation**, starting with a **pilot approach** and adjust **based upon experience and feedback**, to build understanding and support and to effectively integrate into the normal business cycle.
- Effective leadership means **hands on leadership** throughout the organization dealing with both implementing risk management practices and managing risks as an integral part of doing business.
- The **right competencies** (business acumen, facilitation skills, sound judgment) at the **right levels** (adequate authority and influence) must be accessible and available to guide risk management efforts.
- It is critical to **keep communicating** and reinforcing the key benefits and goals of risk management as one of the management tools to help meet organizational objectives.
- Risk management is inextricably aligned to the organization as a going concern. **Link risk management** into how the organization makes decisions and sets priorities, providing a mechanism in which risks come to a collective table for assistance, validation or acceptance.
- **Educate and involve stakeholders** in the organization’s risk management practices so that they understand the business’s trade-offs.
- Use the same **sound judgment** in establishing and communicating risk issues as you otherwise would in conducting the business of government.
- Setting **risk tolerances** is a normal part of management that must be both **qualitative and quantitative**. While there is a tendency to want absolute clarity, this is difficult – and potentially harmful – in the face of many public policy issues.
- Like all elements of good management, sustaining and nurturing effective risk management takes **continuous effort**. The tools and discipline must be in place to assess and refine the practices.

Above all, this is not about being risk adverse or risk takers: it is about the management of risks that so that the public sector organization can achieve its goals, can equip its political leadership with the information and solutions it needs and can allocate resources effectively in high risk
areas. Implementation success hinges on the features noted above: integration to the culture, leadership, use as a management tool, inclusion in the business management suite that the organization must have. It is not the flavour of the month, nor is it the magic solution. It is part of the sound modern management of government.

The key to implementation is to move beyond policy and frameworks with a plan and leadership that suits the organization and its needs. There is no single step-by-step formula. However, common elements to implementation are: policy, governance, accountability, integration, training and design flexibility. This study established that many organizations use risk management as one of the management tools to achieve their ends. They engaged staff and stakeholders in the process so that they took on ownership, became more comfortable with the use of the risk language and concepts, and helped add value to its final character in the organization. Political leaders are both users and beneficiaries of good risk management tools.

No one started with risk management as part of the management cycle – they each had to learn what risk means in their organization, establish a foundation, and then integrate risk management into existing management processes as promptly as possible. What became clear in retrospect is that their management cycle was enriched and improved by the use of risk management.
Introduction

“The need for more affordable and effective government combined with trends towards revitalizing human resources capacity and redesigning service delivery are dramatically affecting the structure and culture of public organizations. The faster pace and need for innovation, combined with significant risk-based events from computer failures to natural disasters, has focused attention on risk management as essential in sound decision-making and accountability.”

(Integrated Risk Management Framework, April 2001 – Treasury Board of Canada Secretariat)

Government’s changing policy and operating environment and the increasing expectations of stakeholders are driving the requirement to better anticipate and actively manage organizational risks. Unique to the public sector, however, are the political and public implications of practicing risk management.

The essence of our conclusions after many interviews is that the old saying – ‘risk is risky’ in government – needs to be replaced by a new one that has been proven true only too often recently: ‘Disregarding risk is even riskier’. Increasingly public sector organizations are challenged to answer “What did you know and when, and what did you do about it?” questions on difficult issues. Implicit in those questions is another one: “How do you know? What tools do you use to effectively bring forward operational and administrative risks and then do something about them?” That is risk management.

Integrating with the prevailing culture is essential to help that culture grow and move forward. Many public sector organizations are in some stage of reform and modernization: risk management should be a tool of such changes and part of the overall process, not an aside or add-on.

We learned that the value of risk management as part of the way of doing business is an organic process, one where learning and integrated staff involvement at all levels and across organizational boundaries create synergies that force the risk management approach to develop on a continual basis to meet the needs of the organization. That means that the processes need continual support in terms of training, internal champions, and consistent leadership at the corporate, technical and operational levels. Without this holistic approach and preparedness to stick to it over the long term, risk management can be seen as another flavour of the month and augment staff and stakeholder cynicism.

Building in flexibility to permit corrections and refinements to the risk management process and practices based on learning from experience and engagement of staff and stakeholders was cited as critical to effective risk management implementation.

In some cases, we found a direct connection between risk management practices and resource allocation and planning processes. In cases without this direct link, we found a strong connection to the operating culture or to the use of customized risk management tools to build internal understanding of management priorities. In other words, risk management implementation appears to help in achieving the priorities of the organization. So-called full integration was not readily measurable and it is doubtful that one size would fit all in the final analysis.

Our study also concluded that it is naive and possibly dangerous to use strictly numerical forms of risk tolerance in discussing risk management in public sector organizations. On most public sector issues, risk tolerances cannot be easily established. Often setting such tolerances is a matter of political judgment. The public has a key role to play here. So too does the way in which information is gathered and assessed, often demanding that public sector organizations react
quickly with only minimal information. On the other hand, we found that risk management procedures as part of ‘the way we do business’ enabled organizations to arrive more clearly at a better appreciation of the tolerance landscape on issues. They also permitted both internal and external dialogues about risks and risk tolerances as never before, thereby providing as much guidance to staff as possible, even when the situation was ambiguous.

Through our research, the organizations we talked to that had effectively implemented risk management focused on bringing their people along through training and engagement, building a system of internal champions, benefiting from early wins, maximizing the leadership's desire for good management and integrating with existing business planning.

No one started with risk management as part of the management cycle – they each had to learn what risk means in their organization, establish a foundation, and then integrate risk management into existing management processes as promptly as possible. What became clear in retrospect is that their management cycle was enriched and improved by the use of risk management.

Few organizational environments are more active and subject to so many forces of change and adjustment as the public sector. A challenge, therefore, of effective risk management is to continuously learn and refine.

**Background and Context**

For governments around the world, the risk bar has been raised significantly in the past few years. Broad public understanding of emerging risks to health and safety, that have no respect for national boundaries, has increased. Personal and national security issues have risen to the top of organizations’ agendas. Along with that has come the expectation that governments need to respond in more effective ways than they have done in the past.

The issue today is not why government should practice good risk management. The issue is how. Increasingly, political leaders and senior officials within government need and expect that effective risk management will be part of how public sector organizations conduct their business.

**Beyond Having a Policy**

Many governments have established government-wide risk management policies and frameworks. Now the challenge is to implement those policies at a time when the need has never been greater. Recently, issues, factors and influences have emerged which support the need to more effectively identify and manage risks as an integral part of how public sector organizations function. These include:

- A more sensitive political and economic global environment in managing risks to health and safety, and increasing vulnerability of key infrastructures to threat or malfunction.
- Issues of accountability and performance for the effective use of government funds.
- Issues of organizational ethics, governance and accounting practice where financial loss is a threat.
- The emerging security agenda and public concerns demand a focus on risk identification, risk management and risk communication.
- A growing demand that public sector organizations put in place tools to anticipate and mitigate risks.

Taken together, these trends represent a demand for a series of improvements in government risk management practices. As governments continue to develop various approaches to risk management, it is important to learn from each other’s experience. It is also important that governments be equipped with effective and practical risk management tools in order to address these issues.
Objective of the Study

The purpose of this study was to build a reference that senior government leaders can use to implement successful risk management strategies. It reflects how selected government organizations in Canada and abroad are responding to the increased risk challenges they face. Its objective was to identify ways for senior government leaders and public sector risk management champions to:

- Move from having risk policies to implementing them;
- Address the unique features of public sector management that present unique challenges to risk management;
- Integrate risk management tools and approaches into the policy and program framework of the organization;
- Improve risk management skills within the organization; and,
- Apply tools and practices that have worked in other public sector organizations.

The result of this study is a compendium of useful practices to assist other public sector organizations in successfully implementing risk management policies.

Risk Definitions

In general, the study accepted the various definitions used by the organizations under study. Because of the variety of public sector objectives, our study participants' definitions of risk varied somewhat. However, in general, they tended to cite the risk of an organization or program failing to achieve its goals as a central operating concept. Some also specifically included missed opportunity or innovation in their risk definition. The study avoided detailed examination of either the definitions used or the quality of the policy direction or framework. The same approach applied to the definition of risk management. Most definitions included provisions for a systematic approach to effectively identify, assess, treat and report the risks of the organization. The focus was on the tools and practices of implementation.
Findings and Observations

Implementing risk management is a continuous process of experimentation of practice, learning and adaptation. Through our research and investigation, we found that those organizations that believed that they had successfully implemented risk management saw the need for its continuous improvement as a tool of management.

In an effort to identify common practices that may be useful and relevant across governments, we spoke to organizations from a variety of jurisdictions delivering a range of programs. We limited the number of study participants in order to focus our research efforts and more fully understand their experiences to gain meaningful insights. As we focused on how these organizations successfully implemented risk management, several commonalities became evident. Although no two organizations followed identical processes to bring formal risk management to their organizations, they all experienced a number of similar successes and challenges along the way.

We saw eight practices common to all. Through this study we have been able to draw useful practices from the way these organizations have implemented their risk management processes. These practices are:

1. **Plan to Adapt and Learn**: Develop and refine the implementation process through experimentation, real organizational learning and the engagement of staff and stakeholders.
2. **Provide Leadership Support**: Demonstrate visible and continuous senior leadership.
3. **Adequately Resource and Manage**: Ensure the right mix of skills at the right levels.
4. **Make It Real**: Keep risk management pragmatic and relevant to day-to-day operations.
5. **Integrate**: Incorporate risk management in existing planning and decision-making processes.
6. **Engage Stakeholders**: Include and communicate with stakeholders early in the process.
7. **Make It Transparent**: Build transparency into the risk management design.
8. **Establish Risk Tolerances**: Provide a forum for people to discuss risks and to come to common understanding of thresholds.

What we provide in the subsequent sections are observations taken from the experiences of the government organizations we studied. They are designed to provide practical guidance and insights for other governments currently planning or in the midst of implementing risk management.

1. **Plan to Adapt and Learn**: Develop and refine the implementation process through experimentation, real organizational learning and the engagement of staff and stakeholders.

   Rather than develop a single, comprehensive project plan, virtually all of the organizations we spoke with had a strong preference for experimentation as they implemented risk management. Working within a general risk management framework, many achieved success by “leading the people gently” or taking an “unofficial” approach to implementation. This approach was taken in part because they recognized the difficulties that would arise if they tried to plan what the managers and staff may see as yet “another flavour of the month initiative.” One consistent message that we received is that risk management has to be treated as a management tool and that the level of its use would reflect how the organization does business.

But while the approach may have been unobtrusive, it certainly was deliberate. The organizations took measured steps and adapted the risk management plan and process as the organization and its people evolved and practiced increasingly formal risk management. In order
to be deliberate, we saw that organizations in some instances made a policy decision to proceed with implementation and clearly assign responsibility for the implementation within their executive structure. In other cases, the chief executive mandated improvements in risk management. In others, formal political agreement was reached to move forward.

Most of our study participants began their implementations by testing the concept under a pilot approach. Finding friends in the enterprise who would serve as early adopters and champions of risk management allowed the organization to showcase quick wins and to refine their approach based on this pilot experience. At the end of each pilot phase, one organization conducted sessions with key pilot participants to understand the strengths and weaknesses of the pilot implementation. Adjustments were made to the subsequent pilot plans as well as to the risk management process, framework, training and tools to reflect their experiences and evolution. There was flexibility in how risk management was rolled out to different business units, but the core information and messaging were consistent throughout. Successful implementers of risk management paid attention to and learned from any criticism they received. Not presuming to know the ultimate solution and expecting the process to evolve and mature affords the sponsors opportunity to improve the process over time.

Some organizations piloted their risk management implementation by business line. Others by geography. Others by project or by process. The key was to start small or with a specific program because it was easier to implement risk management in a defined arena and the benefits were easier to see and then to communicate. After more people had a better understanding of risk management and its value, they rolled out the process to other areas across the organization. All successful implementers told us it is most effective to implement a risk process that included risk identification, risk assessment and risk mitigation action planning. Risk assessment is a critical step in the process but it cannot be confused with the broader risk management process. In fact, we heard that risk identification and assessment on its own can be disastrous, particularly in the public and political environment. In the transparent public environment those affected by risk expect answers on how those risks are going to be resolved. We noted that several organizations deliberately involved their political leadership, alerting them to the process of implementation, getting direction on preoccupations and design features and ensuring that no risk identified be left unanalyzed or unresolved.

Few of our study participants implemented successful IT solutions designed specifically to support their risk management efforts. In addition to the significant financial considerations, most in our study decided a major IT solution would unnecessarily complicate the risk initiative and potentially compromise success at this stage of their progress. Most organizations developed simple templates to facilitate the risk management process. Others also made adjustments to their existing reporting systems to incorporate risk information. As risk management practices continue to mature, some organizations indicated that they may investigate IT solutions in the future.

With “risk management” front-page news and the number of theories and methodologies abounding, it is easy to get caught up in a theoretical debate of risk. One organization temporarily got stuck on the definition of risk. The leader saw that wasn’t where the debate (and energy) should be and so decided to adopt the definition in the Australia/ New Zealand joint standard on risk management and moved forward. Our study participants told us to steer clear of methodological and territorial disputes and just get on with the job. Focusing on content over theory will better serve the organization, particularly in the early stages of implementation. A word of caution however. Adequate deliberation and strategy development are required. Make risk management comprehensive – that is, include policy, processes and practices, tools, templates, governance – but do not
overcomplicate the risk management framework. It will be perceived as academic or simply too difficult to adopt. Another common message is that implementing risk management takes time.

Implementation may be phased and somewhat temperate, but it cannot be haphazard, and it must be approved and supported by the leaders of the organization. Where implementation followed a loose approach at the outset, at some point, it was brought together. The loose phase enabled a lot of organizational learning, modification of processes to meet the unique needs of the organization, some experimentation and some early wins. But it cannot last forever. At some point, cross-organizational implementation has to take place through a standardized approach that, by this time, has been tailored to the organization. In other words, getting buy-in is important, but the practice cannot remain optional forever.

We saw that the so-called ‘fear of risk’ phenomenon – that is, when public sector organizations are reluctant to move forward on risk management for fear of public or political exposure or embarrassment – was most readily overcome by actually moving forward. Common training tended to create a greater comfort with the overall concepts. Moving rapidly from the training phase to using teams to identify risks and develop mitigating strategies tended to focus them on real problems and their likelihood of risk. This focusing effort effectively reduced the “Chicken Little” syndrome that rated all risks as imminent and high impact. Common tools, such as a risk matrix, also created ways to compare risks as never before. (See Appendix E for samples).

The Bottom Line:
Expect a multi-year implementation, starting with a pilot approach and adjust based upon experience and feedback, to build understanding and support and to effectively integrate into the normal business cycle.

2. Provide Leadership Support: Demonstrate visible and continuous senior leadership

Leadership: it’s continuously touted as a critical success factor in implementing and sustaining any significant organizational change. Executive leadership support is essential, without doubt. Once that fact was confirmed, we wanted to see how the senior leadership in these organizations demonstrated that leadership support and set the tone at the top. As one manager joked: “A memo from the deputy minister is not leadership commitment.” Somebody has to step up: chief executive, chief auditor, or chief risk officer. The power of the individual leader is apparent in how an organization approaches, implements and fosters risk management. Many of the leaders in our study were drawing on a background and experience in risk management, and led the charge for moving risk management forward in their organizations. However, other leaders were sold on the concept by champions in the department, and then demonstrated their commitment to support the initiative. The significance of executive support was made clear at some of our study organizations when the sponsoring executive leader left the organization. Without that constant, consistent force, risk management activities faltered. In other cases, however, the initiative survived and was sustained even with chief executive turnover, largely due to continued, strong leadership.

As one study participant stated: “The only way you can legitimately talk about risk is to actively manage risk.” Visible and constant support is required throughout the risk management implementation. Practical examples of leadership support include:
• Making strategic changes in organization structure to facilitate collective discussions.
• Appointing risk management champions to key leadership positions.
• Introducing Risk Management Committees mandated with risk management responsibilities or expanding the role of the Audit Committee.
• Establishing performance agreements which hold executives accountable to manage both the risk management process and the risks that flow from it.
• Adequately resourcing the implementation and practice of risk management.
• Having the top leader serve as the Chair of the Audit Committee that is mandated and held accountable to manage risks.
• Meeting with senior managers individually to thoroughly discuss their risk management assessments and action plans. Leaders were clear not to be perceived as “shooting the messenger”.
• Validating the quality and acceptability of their manager’s risk analysis and action plans, and then demanding regular risk information and using it in a systematic and long-term fashion.

While executive leadership of the organization must demonstrate commitment, leaders from the program and business lines must also walk the talk. Personal involvement in sponsorship was deemed essential. That is, active participation by leaders in training, risk assessments and risk discussions, assigning risk accountability, and ultimately allocating resources to implementing and managing risk. Leadership must really want to know the risks and what they mean. This dialogue ensured positive synergy in understanding where the leadership wants to go and the risks to getting there. A sure way to kill a risk program is not to use – and not be seen to use – the risk information in decision-making. A common message was the staff is adept at identifying true commitment versus pretence.

The goal is to create an environment where people are encouraged to identify risks and possible solutions. Saying “thank you” for raising an issue and a viable solution, even if it costs money, is a powerful message. In one situation, a risk management pilot group received an additional $1 million budget allocation as a result of their participation. Several organizations identified that the risk management processes they put in place served to re-balance their view of their risk profile to better account for underlying, on-going risks that do not receive a lot of publicity.

The Bottom Line:

Effective leadership means hands on leadership throughout the organization dealing with both implementing risk management practices and managing risks as an integral part of doing business.

3. Adequately resource and manage: Ensure the right mix of skills at the right levels

In our study group, no single organization structure to support risk management emerged as best. The specific organization structure adopted mattered less than the fact there was a central coordinating body for training, quality control and framework development to provide consistency. An integrating mechanism or central function that can monitor the quality and consistency of risk assessments and mitigation plans, offer senior management advice, provide senior management with regular reporting at the corporate level and identify emerging themes was often considered the
“Ways have to be found to take a ‘whole of organization’ view of risk through integrated reporting, corporate monitoring and rolled-up summaries. Someone has to bring it all together.”

Our study showed that risk management champions or advocates are required throughout the organization. In addition to visible executive leadership and designated sponsors (often in the Internal Audit or Risk Management function), other formal and informal champions of risk management are important. Important not just for the initial implementation but also to sustain the risk management process. Until risk management is embedded in an organization, the burden to sustain the momentum lies with the “champions.” We saw several types of champions needed throughout the process, each supporting and substantiating the risk management implementation in specific ways.

- Policy champion: to initiate the policy need, get the decision to go forward and ensure that it happens.
- Technical champion: the source of training and design, the source of continuing advice to business units.
- Operational champion: the first business unit leader to step up to the plate to pilot or show how it can be done.
- Unit Champions: in large organizations, the executive needs someone to co-ordinate efforts internally and to liaise with the corporate resource, usually the Technical Champion, on implementation, to work with various elements of the business unit on implementation and operation and to work with the corporate champion on the roll-up issues as well as quality.
- Corporate Champion: the central agency function of the organization (location: generally head office, chief executive office, central planning unit): operates overall business management processes of which risk management is a part.

In the majority of organizations studied, internal audit initiated and led the risk management implementation effort. Organizations seem to draw upon internal audit’s existing skill set and their recognition of the enterprise-wide view. In a number of cases studied, the internal audit group evolved to formally include risk management responsibilities, often confirmed through a change in the mandate and name of the group. Internal Audit and Risk Management functions currently exist at some of the organizations studied. In some instances, we saw resistance to having internal audit play a lead role once the process had begun. However, the course taken tended to reflect the energy and personality of the individuals involved more than the function they served.

Most organizations are working through the direction advanced by the Institute of Internal Auditors regarding the relationship between audit and risk management responsibilities. No matter the stage of implementation, every organization needs a driver of risk management to provide consistency, diligence, process improvement and sustainability.

All successful implementers resourced risk management expertise to guide the processes and people. Whether internal or external providers, it was critical that these resources be accessible and credible to managers and staff in the organization. And it’s not just knowledge of risk management that’s required. A diverse skill set seems to make sense. Competencies required included not only knowledge of risk management and of the organization, but excellent facilitation skills, analytical skills, sound judgment and effective communication skills. Sometimes these competencies were found in a single person, but more often a team comprised the required know-how. One organization warned that you could do more harm than good if you don’t have the right combination of skills. Their team consists of a mix of accountants, evaluators, and communication and facilitation experts. Another common approach was to put highly trusted individuals in place, known to the organization who would be around to not only do the opening session training but also to work with teams as they began using risk management tools. This is a longitudinal commitment, not just a start-up one.
To be effective, key messages delivered in training related to risk management must be consistent, and can provide an essential communication forum. Training alone is not enough though. In our experience with risk management, we identified some world-class training programs and materials at organizations where risk management is paid only lip-service. At all the organizations researched, a key role of training and risk management workshops is to establish a common language and tools for the organization. This may include access to information implications and tips on how the organization approaches these requests for information. Several organizations reported that they modified their risk management tools as a result of the training and workshop sessions. This was seen as a win for those involved and as a greater integration with “how we do business around here”.

In addition to a central point of contact, some organizations determined they needed business unit champions to provide expertise to the business unit, liaise with central co-ordination and serve as a point of translation of business and corporate needs. These business unit champions must have sufficient authority and influence to effectively play this role. Interest and enthusiasm for risk management is not enough to ensure adherence to risk processes and garner staff credibility in those processes.

**The Bottom Line:**

The right competencies (business acumen, facilitation skills, sound judgment) at the right levels (adequate authority and influence) must be accessible and available to guide risk management efforts.

4. **Make It Real: Keep risk management pragmatic and relevant to day-to-day operations**

For any change to take hold effectively, it must make sense to those who are to adopt it. And this includes risk management implementation. Fundamentally, those charged with leading the implementation knew their business and integrated risk management practices into existing decision-making processes. Risk management that was considered to be a management tool and communicated as such seemed less threatening and therefore more readily adopted.

One organization wanted risk to be a conscious part of decision-making but only one part. During its implementation, risk management at one large organization was positioned as “fundamentally helping managers understand the barriers to their objectives.” Risk management was positioned as a process to identify the risks and viable solutions.

It is also important to understand the culture of the organization and build the training and management into it. The most appropriate implementation strategy depends on the existing organizational culture. Some businesses confirmed this through a formal risk readiness assessment to understand the current risk culture and state of risk management implementation.

Through the experiences of our study participants, we observed a number of practical suggestions in making the risk management effort “real”:

**Training**

- The role of pervasive and thorough training is important. All staff must have the same tools accessible to them and managers must participate in training. An organizational focus for training is essential. It is not a one-shot deal.
- Move rapidly from training to doing, using cross-sections of internal unit staff and internal stakeholders from other units.
- Learn by doing – move quickly to workshop-type exercises that use common and simple tools for risk identification, prioritization, costing and communication.
- Go see the managers where they are – don’t make risk training a headquarters only event.

Communicate the Value
- Make sure managers see the value. One idea is to use real life examples in training forums and work together through the assessment and action plans with those managers. It was frequently emphasized that using risk management processes is a successful way for managers to communicate their concerns and priorities.
- Start with identifying meaningful, realistic steps that the managers can take to mitigate their risks.
- Ensure it is relevant to daily operations. Pay attention to content and not just process. Risk management cannot be simply a compliance exercise.
- Make risk management guidance and support accessible throughout the organization - on the intranet, in a designated function or resource, etc.

Simplify
- Keep it simple. If risk management is too complex, no one will understand or use it. Managers are wary of too much “framework”. If too complicated, employees will think it is an academic, theoretical or conceptual exercise.
- Get line managers involved in building tools and templates – risk registers, standard risk assessment tools, risk worksheets and workbooks, risk profiles – to improve the chances of having them adopted. These should be shared up and down the management line.
- Put it all on one page. Use a common language and template and make it standard. Keep a consistent format for ease of use.

Lead by Example
- Ensure action plans are viable and reasonable. This is a critical step. At the outset, this will require a fair amount of control: to ensure that risk identification does not get out of the scope of reality and potentially embarrass the organization. As this evolves, most organizations found that suitable language and retraining were the rule of the day. This even applied to those organizations that used stakeholder engagement in risk identification.
- Create and sustain in-house expertise to support business unit risk management. This does not preclude using contracted or purchased resources as support, but having the same person on a continuing basis providing support creates a momentum for, as well as a continuum of, development.
- Practice what you preach. To gain credibility, national and corporate services groups (often the champions of risk management), must demonstrate adherence to risk management practices.

**The Bottom Line:**

It is critical to keep communicating and reinforcing the key benefits and goals of risk management as one of the management tools to help meet organizational objectives.
5. **Integrate: Incorporate risk management in existing planning and decision-making processes**

Successful implementers agreed that risk management must be integrated into existing management processes. They also made it clear that risk management does not replace overall business and management planning. Rather, it embellishes it. Therefore, it makes sense to incorporate the risk discussion into current planning and decision-making mechanisms. As one manager remarked: “If you identify a major risk to the organization, how can it not become a corporate priority?” How to embed risk management with other decision-making processes is the issue. Creating a separate risk management process, distinct from the existing decision-making processes, is not the way. Managers were not interested in adopting a process that appeared to be an additional layer to already complex protocols.

Fundamentally, risk management cannot stand alone – it must be part of the way the organization manages itself in both strategic and operational terms. With the current trend to modernize government, risk management is increasingly seen as integral to good business and a key management responsibility. A key point to selling this politically was to stress that effective cross-organizational risk management practice would provide a greater surety that the organization had done a more effective job – or at least had the capacity – to reduce surprise and get ahead of the bad news curve. No one suggested that unanticipated events could be avoided. However, many recognized that some previously highly damaging situations could have been avoided with a systematic risk management process.

There appears to be no single formula to successfully integrate risk management into current management processes. Determining how to roll up business level risk profiles to the corporate level and factor them into the planning process is key. Integrating risk management into priority setting and resource allocation at the level business plans are developed seemed to be an effective approach. Planning sessions included focused discussions on key risks. This was done in a variety of ways. In some instances, high-level risks developed through the internal planning process were formally reported. In another, risk identification was one of several exercises leading to the creation of plans. And still in others, regular risk reports were provided by business or unit heads. The essence is that the use of risk management was linked to how the organization operated its priority setting processes. In a few instances, the risk identification process formally engaged stakeholders such as advisory groups in advance of the formal planning process.

Due to the danger of stove-piping within organizational units, organizations must balance business unit processes with integrating corporate processes that bring strategically significant risks to the corporate level. All levels of the organization must be involved to ensure that all relevant risks are addressed and mitigation expectations are communicated to the appropriate managers. Successful organizations bundled risks to identify high impact and high likelihood issues – that is, those that are most politically and programmatically relevant – and then prioritized and allocated resources accordingly. The distribution of resources was deemed to be more conscious and relative to risk exposure than in previous planning exercises.

It is important to note that all organizations that had successfully integrated risk management into planning relied on a coordinating function to pull risk assessments or profiles together. This formal co-coordinating function had several elements.

- It served the business planning and control process of the organization; and so might be a corporate planning unit or the chief executive’s office. In a few cases it was internal audit.
- It provided a challenge function to the risk identification process, questioning in some instances whether the risk identified was fully considered.
We feel that we must refresh our 'lists' quarterly – do not let it get stale. The government business cycle offers good milestones for updates.

We saw examples where continuous integration occurs around the management tables. In these cases, the chief executive was key to ensuring these discussions happen and making them happen at the right levels of the organization. Some organizations have established a separate Risk Management Committee or have changed the role of the Audit Committee to be an Audit and Risk Management Committee. Others specifically added "risk" to existing management committee agendas on a regular reporting basis as they would for financial reports. What they all had in common was a process in which risk identification and assessment conducted within silos came to a collective table to either get assistance, validation or acceptance. Raising awareness of these issues allowed the managers to address them at the most efficient level, whether it is corporate or business unit. Our study participants stressed that complete risk management includes assessment, response, mitigation and communication and that the entire risk process must be integrated. Consistency in messaging, risk definitions and process was critical.

In several instances, and especially as risk management was being moved into the organization, leaders played key roles on an individual basis. They would set up one-on-one sessions with individual senior managers to identify and verify the approach to risk management. This was a powerful practice as most managers struggle between including all risks and a reluctance about being seen as alarmist. Such individual sessions permitted both the leader and the manager to sort out the boundaries of risk tolerance, as dynamic and varied as they might be.

Another example of integration included setting up cross-unit working teams to discuss risks and action plans. As internal client service providers, corporate services units participated in risk assessments of each program area. With insights to the challenges and obstacles the programs were facing, the corporate services groups could themselves conduct a more relevant risk assessment of their own program, and develop action plans that were better geared to serving their clients. There was anecdotal evidence that these cross-functional working arrangements also fostered teamwork and communication across silos.

"Closing the loop" was cited as critical to effectively embedding risk management into the organization’s decision-making processes. One organization established a Risk Management Committee to whom risk assessments and mitigation plans were regularly presented. Risk assessments and action plans are refreshed on a formal basis quarterly in some organizations. Here again, leadership is the key and the leadership need is specific: leaders have to be prepared to use the risk management data in how they make decisions and to hold their executives to account for it. In one instance, we noted that formal high-level corporate risks were assigned to specific members of the management team to manage on its behalf.

No one started with risk management as part of the management cycle – they each had to learn what risk means in their organization, establish a foundation, and then integrate risk management into existing management processes as promptly as possible. What became clear in retrospect is that their management cycle was enriched and improved by the use of risk management.
6. **Engage stakeholders: Include and communicate with stakeholders early in the process**

Of all the successful practices in implementing risk management, we identified that determining the best approach to engaging stakeholders varied the most. This is not surprising due to the very assortment and interests of stakeholder groups. But one common theme emerged clearly – it’s not whether you engage your stakeholders, but who and how. Further, the more significant your engagement with stakeholders is, the more important that they provide substantive input to risk identification, prioritization and mitigation. It is very risky not to involve them, especially when the outcomes are integrated into increasingly public business and budgetary plans.

The public sector move towards improved transparency and openness has encouraged organizations to more formally and regularly consult with their stakeholders. Stakeholders may include employees, managers, politicians, the public, special interest groups, unions, communities, and other government organizations. Different approaches were taken with different stakeholders. As with the theory of risk management itself, the practice of holding a broad range of stakeholder consultations is to reduce surprises and uncertainties in order to improve the likelihood of success. To this end, a number of organizations in our study had extensive stakeholder involvement.

In some cases, stakeholders were engaged early in the process to help plan the risk management implementation and agree on governance strategies. Often existing consultative mechanisms were used as those stakeholders had the greatest familiarity with the program objectives and the organization itself.

Others maintain contacts and establish relationships on an ongoing basis so that they can effectively work together to treat risks if they occur. One organization is holding more significant public education sessions through open houses and public consultations. These are considered important so the public can understand the types of challenges and decision-making processes the organization has to make within its budgetary constraints. The goal is to have stakeholders see how the business plans are linked to their risks, the choices that were made and why. Although not always widely attended, these open sessions are an important aspect of the organization’s consistent imaging and messaging. Involving stakeholders in determining trade-offs has shown to be time consuming yet critical in managing their expectations.

In one organization, the decision was made to develop – on a pilot basis – a formal risk identification process within a specific community. What was intriguing about this on a more general plane was that this involved many stakeholders focusing on the issues of air quality. This organization realized, quite rightly, that such a scope of stakeholder engagement in discussing risks and indeed risk tolerances needed a formal governance process that ensured that input was respected. But it also ensured that, in the end, the appropriate regulatory powers of the government were also respected. How stakeholders are engaged is important.

“Educate, educate, educate” is what one senior government leader told us. Clearly communicate the context and benefits of risk management throughout the organization – to managers, employees, stakeholders, and politicians. This seemed particularly apropos in those cases where

---

**The Bottom Line:**

Risk management is inextricably aligned to the organization as a going concern. Link risk management into how the organization makes decisions and sets priorities, providing a mechanism in which risks come to a collective table for assistance, validation or acceptance.
the Internal Audit function is leading the risk management charge. Depending on the mandate of internal audit in the past, managers and executives could perceive that risk management was “something that is going to be done to them.” We heard that organizations should expect that the stakeholder perspective on risk would need broadening and a clarification of what risk management encompasses. Risk management is not just technical, scientific or engineering risk, and that was a new message for many of our study participants. One organization talked to its ministers and cabinet before engaging other stakeholders in order to reduce the potential for surprise or criticism.

Determining how to best manage third-party risk is an issue for more and more public sector organizations. The growth of outsourcing of operations and contracting to other sectors has led some organizations to consider how to manage shared risks. One organization established a joint Risk Management Committee with its key third-party service provider, mandated to identify and address joint risks. Developing formal risk sharing arrangements with third-parties is still a relatively new practice, especially between organizations within the same jurisdiction.

For internal stakeholders, communication strategies ranged from extensively planned to relatively informal. In either case, consistent and repeated communications helped embed risk management. Any and all opportunities to talk about and reinforce risk management practices were exploited: risk assessments, training, presentations, newsletters, and intranet. Several organizations even had a specific colour associated with their risk management communications.

**The Bottom Line:**

Educate and involve stakeholders in the organization’s risk management practices so that they understand the business’s trade-offs.

7. **Make it transparent: Build transparency into the risk management design**

“Making decisions with eyes wide open”. “What I don’t know can hurt me.” “We can’t afford NOT to do risk management.” These are all quotes from our study participants as they discussed the political element of risk management. They all reflect an underlying reality: implementing risk management can meet political resistance but can also better serve the goals and concerns of political leaders when it is done well.

Not surprisingly, organizations operating in the public sector context are concerned about transparency and openness. Public sector risk management is different than in other industries and should, one could argue, be implemented differently. We found that transparency should be built in the design and reporting process from the start. Transparency can be defined as carefully documented, consistently used and adequately shared information. The bottom-line in dealing with risk in the public eye is to use the same judgment as you otherwise would in conducting the business of government. That is, assume that the information will be public and plan accordingly. Managers we spoke with cautioned against airing risks for which no mitigating strategy or action plans have been developed.

Responding to questions related to access to information, several organizations indicated that a formal risk management process can actually give the public and politicians confidence in the capacity to deal with known risks. We saw examples and heard testimonials that integrated risk management practices, documented carefully in a one-page report, actually reduce their freedom of information requests, rather than increase them. Some organizations suggest using legal staff for assistance in shaping risk management messages. All
said to be sure to avoid processes that produce excessive paper or that fail to tell the complete story on a risk issue.

We heard divergent opinions on when to involve political leadership. Some organizations had success engaging their Ministers in discussing the need for and benefits of risk management at the onset of the program. This communication fostered support and commitment. On the other hand, we heard that it was better to wait and have a story to tell about the practical, tangible aspects of risk management at that particular organization. Each organization needs to determine how to involve their political leadership at the appropriate level of both implementation and ongoing information flow. Regardless of when it was delivered, a key and consistent message to politicians is that effective risk management is an early warning system that reduces the potential for surprise.

Ministers and leaders move from issue to issue. Policies and expectations change. But the risk management framework and implementation must be robust enough to survive the machinery of government changes. In one organization, the senior leaders meet weekly with the chief executive. An important element of these meetings is a discussion around the key risks faced in the senior leader’s business lines. Risk management brings credibility to issues and positions. It is not just anecdotal but a more definitive and sound justification for a particular solution or additional resources. The chief executive is thus armed with tactics when talking to others within the organization or within political circles.

**The Bottom Line:**

Use the same sound judgment in establishing and communicating risk issues as you otherwise would in conducting the business of government.

8. **Establish Risk Tolerances:** Provide a forum for people to discuss risks and to come to common understanding of thresholds.

Should a public sector organization establish quantifiable risk tolerances as part of its risk management practices? While two organizations in our study did just that, most organizations determined that setting specific, quantifiable risk tolerances is not widely practical. Setting tolerances is a dynamic process that often involves top leaders giving ongoing guidance, not setting clearly delineated thresholds. One common exception to that philosophy is the establishment of filters and spending tolerances as a legitimate form of risk tolerance setting needed in many operational functions.

Risk tolerances are often made clear in where and how resources are allocated; yet another key reason to formally integrate with the organization’s planning process. In helping business units rate risks, simple scales involving peer judgments can be very useful. These often establish likelihood and impact of risk and not necessarily corporate priority.

Setting risk tolerances is a complex business poorly served by excessive rigidity. We saw that most often risk management practices provide a forum for where people talk about risk and come to a common “threshold” for a specific situation in light of the current political landscape. The direct involvement of top leaders in setting the context boundaries for decision-making effectively occurs through the integrating mechanisms discussed previously.

Quantification must not be phony, that is, too complex or not based on the science/metrics of the operation. Quantification for its own sake can often mislead the public and those involved within the organization.

*Risk Management: Moving the Framework to Implementation*
*A Study by Deloitte & Touche and The Conference Board of Canada*
Sustaining Risk Management

As difficult as implementing risk management is, our study participants told us sustaining it is even harder. Our study showed that the real challenge comes after the fan-fare of introducing risk management. An organization's risk management strategy has to be managed over time – it is not a one shot deal. Most of those we talked to are now facing this challenge. Now that we have everybody talking about risk, what do we do to keep them talking about and managing risk?

Good practices for the initial implementation appear to be good practices for sustaining risk management. Our study participants said the risk management process needs to continue to evolve as the organization learns. Continue to solicit feedback from those involved in the process. Acknowledge the skills and experience of staff by paying attention to their criticism and adapting the process and framework as required.

At a minimum, if attention to risk management falters, progress will slow. At worst, it can get derailed all together. In the public sector arena a common challenge is a change in leadership. As we saw with the leadership element, if the new leader is not as passionate or committed to risk management, chances of sustaining an effective risk management process are compromised.

Continuing to hold managers clearly accountable for risk management is critical for an organization to sustain its risk management process. Regularly discussing risk status and plans at management tables, requiring regular reporting to the Senior Management Committee and/or Audit Committee, or presenting formal updates quarterly to the Executive Committee where each member is assigned responsibility for a key risk have been effective mechanisms to clarify accountability and reinforce a sustained risk management practice. In one organization, Internal Audit conducts mini-reviews or audits against mitigation action plans. They are also trying to move to a more “self-reliant” process whereby business units conduct their own risk assessments without facilitation of the central group. Leaders and champions need to reinforce the use of formal risk management methods and processes after risk management has been “implemented.” Not insisting on continued rigour and consistency in key practices can reduce the effectiveness and benefits of risk management over time.

As already noted, training is a continuous process. Having in-house capacity with tailored training tools is important. The identification of the champions network also is important. In a fully mature system, risk management will become a routine part of operational and strategic activity.

The Bottom Line:

Like all elements of good management, sustaining and nurturing effective risk management takes continuous effort. The tools and discipline must be in place to assess and refine the practices.
First Steps – How Practical Links were Built between Theory and Practice

This applied research was designed on the premise that having only risk management policies and frameworks in place is insufficient. In fact, having only a policy (or framework) can create false expectations and frustration among managers and staff. An important learning of this research was that there is no prescriptive set of steps that will create, Lego-like, a fully integrated risk management implementation. As indicated previously, implementing risk management on its own, and not as an integral part of the management tool kit of the organization, can be counterproductive. Moving from theory to implementation can often be challenging.

Although a prescriptive solution is not feasible, we highlight some of the practices that were reported to us – and contained in the main body of the report – that were seen as ‘first steps’ in moving towards risk management. Similarly, we also provide a range of questions to consider about risk management implementation in Appendix F.

Highlights from several interviews reflected that “We would not have moved forward without…”.

- Approving a risk management policy, along with an implementation plan that:
  - obtains senior management endorsement
  - establishes governance, e.g., converting the Audit Committee to an Audit and Risk Management Committee that would steer implementation
  - assigns implementation leadership and responsibilities
  - approves a training plan
  - creates accountabilities for both leading implementation and supporting it
  - establishes report-back protocols for the senior management committee
- Establishing an operational or line manager as a champion. Alternatively, finding an operational or line manager as a pilot project
- Ensuring the Chief Executive’s overall support and having him or her fix it as a performance objective for his or her direct reports
- Actively engaging the Chief Executive in discussions about risk and in guiding initial efforts at risk identification and mitigation strategies (this shows commitment, gives real time guidance to managers and familiarizes the Chief Executive with the process too)
- Developing and delivering training that involves all levels of staff, working together
- Assigning staff members as trainers and assistants to line units in their implementation
- Using the training format to move quickly into operational units’ workshops that actually create risk profiles and mitigation strategies: using the trainers as consultants to this process
- Involving operational staff and managers in molding off-the-shelf training packages to the organization’s needs: creating an operational level implementation group or network
- Permitting a high degree of implementation flexibility for operational units at the outset, with the understanding that the organization as a whole will eventually (often within three business cycles) have to solidify its risk methodologies
- Making sure, either directly from the implementation leader or through the Deputy Minister or Chief Executive’s office, that political staff and politicians, if necessary, understand the scope of risk management in planning and operations, are familiar with reporting tools and have their needs met
- Assigning implementation leadership, perhaps in the audit group, but engaging quickly the business or corporate planning group so that this is not seen as simply an extension of audit
- Above all, showing considerable flexibility with respect to how implementation should proceed and to maximize the opportunities for operational units to mould the look and feel to the organization’s way of doing things.
Conclusion

Risk management is an important element of overall good management and will continue to be an integral part of management processes in many governments in Canada and abroad. The goal is better decisions, supported by a risk management process and rigour. Visible leadership, appropriate stakeholder consultation, adequate resources and a practical approach tailored to the organization’s existing culture and operational processes all contribute significantly to the successful migration from risk policy to implementation.

As we focused on how these organizations successfully implemented risk management, several commonalities became evident. Although no two organizations followed identical processes to bring formal risk management to their organizations, they all experienced a number of similar successes and challenges along the way. Specifically,

- All have risk management policies and directives requiring the implementation and practice of risk management – both central government and organization based.
- All have taken, or are taking, a number of years to fully implement risk management. Organizations modified their risk management approaches over time as they developed and learned.
- There is a general consensus that risk is an art, and not a science. That is, there was a greater reliance on engaging people in learning and doing than on adopting a ready-made solution. Adopting a structured methodology – and then interpreting it to the organization’s context – was effective.
- Most organizations had substantial experience with risk assessment – especially in areas of large-scale IT projects, science or engineering activities upon which they built broader risk management.
- All organizations have found ways to customize their implementation, to make it more sensitive to existing culture and practice and to engage various levels of staff and stakeholders in the process.
- A significant element of both top-down direction and leadership and bottom-up engagement and input are involved in the process.
- In most cases, the Internal Audit group was the initial champion, and in many cases, still is. Its role has evolved in some cases to providing technical support, continuing training, evaluation and monitoring.
- There are four key champion roles for risk management, each supporting and reinforcing the risk management implementation in specific ways: leadership, operational, technical, and corporate.
- The role of training and education – both at the outset and on an on-going basis – is key. Using a common language, messages and tools within the organization - be it home grown or purchased – and maintaining it over time is important.
- Engaging politicians and the public in introducing risk management practices and the use of the results of the process is key and useful in establishing more confidence in public sector organizations.
- Risk management works best when all elements are introduced and used together: that is, risk identification, risk assessment, risk mitigation, risk communications and integration into how the organization plans and manages.
- Some organizations have integrated risk management into their existing management processes at the corporate level and other organizations are in the planning stages of integration.
- Anecdotally, deliberate, formal “integrated” risk management has made a difference – in the quality of decisions, service delivery, morale, and in the reduction in number and severity of crises.
In addition to improving the identification and mitigation of risks at his organization, one senior official indicated that risk management has resulted in other benefits. Involving different levels of the organization in the process, who see things senior managers don’t see, learning from each other in discussions related to risks and action planning, and opening the door to improved dialogue have all produced spin-off benefits. There is a better understanding of corporate objectives and priorities, increased pride in the workplace, and improved morale with a feeling a greater connectedness to the organization. Overall, he credits the effective implementation of risk management as directly contributing to an overall stronger, happier workforce.

Establishing formal mechanisms to measure the effectiveness of risk management on achieving the organization’s objectives is on the horizon. Organizations are beginning to consider how to demonstrate that integrated risk management does in fact make a difference. Organizations involved in third-party relationships are also trying to determine effective ways to manage those shared risks.

We have highlighted a number of practices we hope will be useful to senior government leaders as they begin or continue their risk management implementation. Significant and relevant experiences are available from which public sector senior leaders can learn and tailor as they successfully move their risk management framework to implementation.
The Project Team

The project managers for this study were Carolyn Farquhar, Director, Organizational Excellence at The Conference Board of Canada and Mary E. McBride, Practice Leader, Risk Consulting and Regulatory Services, National Capital Region, Deloitte & Touche.

The Primary Researchers and Authors were Andrew Graham, a former federal government Assistant Deputy Minister and current educator of Public Management in the School of Policy Studies at Queens University, and Lori Bender, a Senior Manager in Risk Consulting and Regulatory Services with Deloitte & Touche.

The team was supported by Inga Michalek of the Conference Board, Jane Kinney, Partner, Canadian National Leader, Risk Consulting and Regulatory Services, Deloitte & Touche and Colin Potts, former Deputy Controller General of Canada as well as retired partner at Deloitte & Touche. In addition, support was provided by senior leaders within Deloitte & Touche in Canada, Australia, New Zealand and the United Kingdom.

Contacts for Further Discussion

Carolyn R. Farquhar,
Director, Organizational Excellence, The Conference Board of Canada
farquhar@conferenceboard.ca
(613) 526-3090, ext. 410

Mary E. McBride, Practice Leader, Risk Consulting and Regulatory Services,
National Capital Region,
Deloitte & Touche
mmcbride@deloitte.ca
(613) 751-5369
Appendix A
Project Methodology

Governance of the Project

The study was collaboratively conducted by Deloitte & Touche and The Conference Board of Canada. A governance structure was established for this study. An Advisory Committee of partners was created to be actively involved in the work of the study. (See Appendix B) The Advisory Committee assisted in determining the target government organizations and scope of the study, discussing the implications of the study material to guide the preparation of the analytical report, and reviewing and commenting on the deliverables prior to their finalization.

Methodology

Through a series of consultations, research and engagement of the project’s Advisory Committee, a number of public sector organizations were identified and approached for study. Public information (via web searches, reports, etc) and that documentation the organization was prepared to share with the researchers was gathered. We then conducted an interview process with each organization based on this information. Any third-party information, e.g. auditor’s reports, evaluations, articles, was used as support documentation, when available.

The focus of this study was to learn from public sector organizations that have developed and implemented risk management practices into their core operations. The research therefore pursued the following overall structure:

- Describing the use of risk management in the operation of the organization;
- Describing the implementation process;
- Accomplishments and difficulties encountered;
- Lessons learned; and,
- Impacts of implementation.

The interviews were conducted in person by a representative from Deloitte & Touche and The Conference Board. Interview formats varied, and included group discussions with a small number of key players as well as individual interviews. Areas responsible for corporate risk management as well as program areas were actively involved in the interview process. An Interview Guide was developed, with review and comment from the Advisory Committee, to provide structure to the process. (See Appendix C) The Guide was distributed in advance of the interviews so that the participants could prepare for the discussion.

In addition to holding in-depth interviews with the participants, the project team conducted extensive research and documentation review on the state of risk management implementation in governments in Canada, New Zealand, Australia, the United Kingdom and the United States. (See Appendix D for a bibliography.)

It is important to note that this study was not conducted as an assessment of performance against a risk management model or framework. The study was intended to solicit and identify useful practices and advice from a small number of public sector organizations with the intent to build this compendium of learnings for other government leaders.

Study Participants

The final list of jurisdictions to be studied was subject to consultation and approval by the project’s Advisory Committee. Our study participants included:
- Canadian Food Inspection Agency;
- City of Winnipeg, Manitoba, Canada;
- Human Resources Development Canada;
- New Zealand Inland Revenue Department;
- Ontario Ministry of Transportation;
- Ontario Ministry of Environment;
- United Kingdom National Savings and Investment;
- United States Department of the Interior – Office of Air Services; and,
- Victoria Department of Sustainability and Environment (Australia).

**Deliverables**

The Conference Board of Canada, in partnership with Deloitte & Touche, as well as the study sponsors, produced an Analytical Report which describes the results of the study and provides an analysis of key themes and useful practices for senior government leaders to consider when implementing risk management. A Highlights Report will be developed for broader distribution, and a presentation by representatives of the project team, communicating key findings of the study, is offered to Advisory Committee member organizations.
Appendix B
Advisory Committee Members

Canadian Food Inspection Agency
Tom Beaver, Executive Director
Liette Dumas-Sluyter, Director, Integrated Risk Management Directorate

Human Resources Development Canada
Basil Orsini, Director, Corporate Risks

Public Works and Government Services Canada
Christopher Wilson, Assistant Director, Strategic Planning and Relations, Real Property Program Branch
Susan Vered, Manager, Strategic Planning and Relations, Real Property Program Branch

Royal Canadian Mounted Police
Brian Aiken, Director General, Internal Audit
Paul Gauvin, Deputy Commissioner, Corporate Management and Comptrollership

Treasury Board of Canada
Marie-France D’Auray-Boult, Executive Director, Risk Management Directorate
Alan Starcher, Senior Advisor, Risk Management Directorate

Alberta Finance
Rod Matheson, Executive Director, Treasury Management
Lowell Epp, Senior Manager, Capital Markets

Alberta Revenue
Richard Whitehouse, Director, Risk Management and Insurance

BC Ministry of Finance
Philip Grewar, Director, Risk Management Branch and Government Security Office
Arn van Iersel, Comptroller General
David Fairbotham, Executive Director, Internal Audit and Advisory Services

Nova Scotia Department of Finance
Shirley Carras, Chief Risk Officer
Kevin Malloy, Controller

Ontario Ministry of Finance
Gabriel Sekaly, Assistant Deputy Minister, Fiscal and Financial Policy Division
Marsha Chase, Manager, Modern Controllership Training Office of the Provincial Controller
Robert Siddall, Provincial Controller, Office of the Controller
Context: The focus of this study is to learn from public sector organizations that have developed and implemented risk management practices into their core operations. The questions therefore will pursue the following overall structure:

- Describing the use of risk management in the operation of the organization
- Describing the implementation process
- Accomplishments and difficulties encountered
- Lessons learned
- Impacts of implementation.

Objective: The anticipated result of this survey will be a compendium of useful practices to assist other public sector organizations in implementing risk management policies. These practices may be in place or may be part of overall government policy frameworks but not yet implemented.

Methodology: Through a series of consultations, research and engagement of the project’s Advisory Committee, a number of public sector organizations will be identified and approached for study. Public information (via web searches, reports, etc) and that
documentation that the organization is prepared to share with the researchers will be gathered. There will then be an interview process with each organization based on this information. Any third-party information, e.g. auditors reports, evaluations, articles, will be used as support documentation.

In most cases, the interviews will be conducted in person by at least one of the two prime researchers. As circumstances warrant, a third-party may administer the survey in person with one of the prime researchers participating by conference call. Interview formats can vary, but it is anticipated that group discussions with a small number of key players will be held. Alternatively, individual interviews can be conducted as appropriate for the organization. The Interview Guide will be distributed in advance of the interview so that the participants can prepare for the discussion. We also encourage written replies and comments prior to interviews to permit more informed discussions.

**Interview Guide:**

**A. Getting Started – (The impetus for implementing risk management and the steps to prepare for, cost and communicate implementation plans and objectives.)**

1. Are there risk management policies in place? Are they central government or organization based?
2. How does your organization define risk and risk management?
3. Was your organization building on a foundation of risk management or was a common risk language new to the organization?
4. Was senior management engaged in the strategy and planning activities? If so, how and what was most effective?
5. Was a decision-making process defined and presented for the implementation? To whom? Were costs and processes outlined? Was a governance process and structure determined?
6. Did you develop a communications strategy or plan for specific stakeholder groups, including politicians, the public and sectoral groups?

**B. Implementation Process – (The How and Who of implementation, and the implications to systems, governance, process, communication and cost.)**

1. When did you begin your risk management implementation? Did you take a phased approach? Was there a pilot testing stage?
2. Was there a formalized implementation plan?
3. Are there internal or departmental risk management champions?
4. How do you capture information about risks? How is it reported? How are decisions about risks communicated? What information support systems and reports were identified as necessary?
5. How do you communicate your risk management process and the importance of managing risks to staff?
6. What processes did you put in place to get people ready and equipped?
7. Does your risk management policy provide implementation procedures? If so, how are they documented and communicated? What tools and
techniques were developed or refined to support risk management practices?

8. Who is responsible for ensuring compliance to the process and practices? Where in the organization do they reside? How are they held responsible?

9. What are the main elements of cost in implementation?

C. State of Implementation – *(The extent of leadership support, communication and staff engagement related to risk management and the results.)*

1. Have all levels and divisions of the organization adopted the risk management policy and practices?
2. Do you have a risk-smart workforce? How do you reinforce this culture?
3. Does your leadership team visibly support risk management principles? Is risk management on the leadership’s agenda? Is there open communication?
4. To what extent and how has your political leadership been involved in implementing risk management?
5. Has risk management been integrated into your business planning processes? If so, how?
6. How and to what extent are your risk management practices linked to the other management processes and/or other organizational management frameworks?
7. Does your organization establish risk tolerances for specific risks? How are they determined, particularly given the public sector context? Are there variations across the organization? How are these tolerances used?
8. At what level of the organization is risk management implemented?
9. How do you handle “freedom of information” legislation with respect to documenting risks?
10. Do you have documentation on how you make risk decisions?
11. Has implementing risk management made a difference? How do you measure the results?

D. Lessons Learned to Date and Advice – *(What worked and what did not work throughout the entire implementation process.)*

1. What worked well and what did not work?
2. What were the expected results? How do they compare with actual results?
3. Have you encountered issues or opportunities in sustaining risk management practices: have you moved beyond a one-time exercise and how?
4. How do people in your organization learn from each other? Are there formal mechanisms in place to support risk management learning?
5. Are there any important “we should have done this differently” observations?
6. What would be the three key considerations for public sector organizations contemplating how to integrate risk management into their operations?
Appendix D

Bibliography

The following is a list of reading related to risk management, many with a public sector focus.


Recent Publications of the Partner Organizations:

**Risk Management**

**Deloitte & Touche**

- *Perspectives on Risk: Building a Risk Intelligent Organization*
- *Beyond Corporate Walls: The Extended Enterprise and Risk Management* (a special supplement for the magazine Corporate Board Member)
- *Global Perspective: A Capital Idea* (briefing for executives in financial services)
- *2002 Global Risk Management Survey* (financial services)
- *Risk Management in an Age of Change* (financial services – study done by DTT and Wharton Financial Institutions Center)
- *Managing Business Risks – Dealing with Uncertainty*

**The Conference Board of Canada**

- *1998, Integrating Risk Management: Strategically Galvanizing Resources in the Organization*
- *1998, Realizing the Rewards in Risk*
- *1999, Forewarned is Forearmed: Identification and Measurement in Integrated Risk Management*
- *2000, How e-Risky Are You?*
- *2000, Integrated Risk Management: Innovative Approaches and Solutions*
- *2000, Don’t Gamble with Goodwill: The Value of Effectively Communicating Risks*
- *2001, A Composite Sketch of a Chief Risk Officer*
SAMPLE: RISK ADVISORY NOTE

Guidelines for Risk Advisory Note

**Branch:**

**Risk:**

**Corporate Risk Area:**

Short statement on the risk events and impacts

---

**Objectives at Risk:**

- Brief point form statement of Branch objectives that may not be fully met. Such shortcoming may result from the challenges identified above and/or from challenges in implementing the mitigating strategies identified below.
- Trade-offs made in developing mitigating strategies tend to be made among these objectives.

---

**Considerations:**

- Short point form statements of factors that should be taken into account in making the right trade-offs in developing acceptable mitigating strategies.

---

**Key Mitigating Strategies:**

- Identification of all key mitigating strategies.

---

**Timeframes:**

- Given targeted completion date for each mitigating strategy.
Sample Risk Register:

**STEP 1 – CONTEXT (Objectives, values, environment): TO PROJECT SAFETY AND SECURITY OF THE INFORMATION IN A PERSONAL COMPUTER**

**Environmental Context:** A government organization handles confidential and sensitive material that must not be accessed by unauthorized personnel. Policies and procedures exist around security and appropriate usage; in addition, there are generally accepted principles of computer security. Results of the assessment will be used to improve security in our unit and may highlight systemic issues that will be elevated appropriately.

<table>
<thead>
<tr>
<th>Risk Identification</th>
<th>STEP 2</th>
<th>STEP 3</th>
<th>STEP 4</th>
<th>STEP 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk (Threat)</td>
<td>Risk Factors (Vulnerability)</td>
<td>Risk Consequences (Impact)</td>
<td>Likelihood 1,2,3,4,5</td>
<td>Impact 1,2,3,4,5</td>
</tr>
<tr>
<td>Risk (Threat)</td>
<td>Risk Factors (Vulnerability)</td>
<td>Risk Consequences (Impact)</td>
<td>Likelihood 1,2,3,4,5</td>
<td>Impact 1,2,3,4,5</td>
</tr>
</tbody>
</table>

1. Action:  
   Champion:  
   Timeframe:  

2. Action:  
   Champion:  
   Timeframe:  

3. Action:  
   Champion:  
   Timeframe:  

4. Action:  
   Champion:  
   Timeframe:
Sample Guidance: Analysing the Risks

Once you have identified and recorded the risks you face in achieving your business objectives, you then analyse them. This analysis consists of using criteria to evaluate your exposure to a risk, taking into consideration your knowledge of risk factors and possible consequences.

There are two, simple criteria used to analyze risks:
- The likelihood of the risk occurring and
- The impact or consequence if the risk occurred.

Each of these dimensions takes into account any activities that you currently perform (“existing controls” that are intended either to decrease the likelihood or to limit the impact.)

Many risk assessment approaches are fairly qualitative in nature. This means that, as a risk manager, you will use experience, judgement and sometimes intuition to assess the likelihood of a risk occurring and the impact which that risk would have on the achievement of your business objectives if it did occur.

Likelihood and impact should be measured on separate scales, always keeping in mind the activities that are currently performed to manage the risk.12

<table>
<thead>
<tr>
<th>Qualitative Measures of Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Qualitative Measures of Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level</strong></td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

---

2 Better Management: Guidelines for Managing Risk in the Western Australian Public Sector, p. 16.
## Qualitative Measures of Impact

<table>
<thead>
<tr>
<th>Level</th>
<th>Descriptor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Moderate</td>
<td>The consequences would mean that the activity could be subject to significant review or changed ways of operation.</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>The consequences would threaten the survival or continued effective operation of the activity or project or attract adverse ministerial intervention.</td>
</tr>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>The consequences would threaten the survival of not only the activity, but also the ministry, possibly causing major problems for clients and for much of the provincial public service.</td>
</tr>
</tbody>
</table>
**SAMPLE: KEY QUESTIONS TO CONSIDER IN EACH PHASE OF THE RISK MANAGEMENT PROCESS**

*Key Questions to “Establish the Context”*

- What does your business unit or program strive to achieve?
- How do you or how will you go about it?
- On what do you place a high value? On what does your organization place a high value?
- What are key success factors in meeting your objectives?
- What authority and resource do you have?
- What kind of environment do you face (internal and external – i.e. customers, suppliers, regulation, technology, etc.)?
- Are there any pre-established criteria against which risks should be evaluated? Are there corporate polices or legislation that must be followed absolutely?
- How will the results of the risk assessment be sued? Who will see it?
- What is the organization’s sensitivity, capacity and maturity in dealing with risk information?

*Key Questions to “Identify Risks”*

- What can go wrong? What types of threats are there?
- Where do they come from?
- What factors influence them?
- What stakeholders will be affected or could potentially be affected by the risks?
- What potential impact or consequence does each risk have?
- Are there opportunities that need to be considered?
**Key Questions to “Analyse Risks”**

- How much control do I have over each risk?
- What are the existing controls that may prevent, find or fix the risks or events?
- What is the potential likelihood of the risks happening?
- How significant are the potential consequences of the risks if they do occur?
- What are the costs, benefits and opportunities presented by the risks?
- Do any of these consequences affect other stakeholders?

**Key Questions to “Evaluate and Prioritize Risks”**

- What is the relative ranking of the risks?
- What level of risk is my business unit or project willing to accept? How risk tolerant is my organization?
- Are the risks commensurate with the opportunities created?
- Should I accept the risk or take action?
- Which risks are the most important to treat?
Key Questions to “Develop Action Plans”

♦ What processes and controls exist and what new ones are needed to minimize the level of risk? (What should we stop doing, start doing and continue to do?)

♦ What performance indicators are needed to monitor the levels of risk, the performance of the control measures and the risk treatments?

♦ Who has responsibility for implementing the plan for managing risks?

♦ What resources are needed (people, money, technical)?

♦ Does the assessment team have the knowledge required to suggest/assign appropriate champions?

♦ Has the team developed evaluation strategies for the proposed action plans that take into account resource requirements in relation to potential realizable benefits?

♦ Do the timelines for implementing the corrective strategies take into account other deadlines and commitments of the business unit and its staff?

Key Questions to “Monitor and Review”

♦ Are the assumptions, including those made in relation to the environment, technology and resources, still valid? How often should we update or revisit the risks?

♦ Are the risk treatments effective in minimizing the risks? Are they cost effective? How can improvements be made?

♦ Do the risk treatments continue to comply with legal requirements, government and organizational polices, including access, equity, ethics and accountability?

♦ To whom should the results of the monitoring and review be reported?

♦ Should you consider doing a follow-up review by engaging the services of outside professionals?
### SAMPLE: RISK RESPONSE MATRIX

#### Risk Response Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Insignificant 1</td>
</tr>
<tr>
<td>Almost certain 5</td>
<td>M</td>
</tr>
<tr>
<td>Likely 4</td>
<td>M</td>
</tr>
<tr>
<td>Possible 3</td>
<td>L</td>
</tr>
<tr>
<td>Unlikely 2</td>
<td>L</td>
</tr>
<tr>
<td>Rare 1</td>
<td>L</td>
</tr>
</tbody>
</table>

**Legend**
- **C**: Critical risk: CAO involvement essential, inform committee
- **H**: High risk: Senior management involvement essential, inform CAO
- **M**: Moderate risk: Management mitigation & monitoring required, inform senior management
- **L**: Low risk: Manage by routine procedures
Appendix F
Questions to Consider about Risk Management Implementation

For the Risk Management Champion

☑ Do we have buy-in at the top levels to move ahead? Is there a formal approval in place?
☑ Is there governance of implementation that identifies how we will proceed, builds in accountabilities and ensures we monitor progress?
☑ Have I identified and brought on board operational managers who will champion and pilot the implementation?
☑ Can I advise on and test out the question of when risk management is integrated?
  - is it a formal element of the business planning process?
  - is there a common set of tools in place, used and understood by staff, senior managers and stakeholders alike?
  - is it a recognizable factor in resource allocation, i.e. does the resource distribution make any sense in comparison to the risk mapping of an organization?
  - are there common reporting tools?
  - is risk management a regular item in how the organization manages itself, e.g. a discussion item at executive committees, a roll-up report on risk to the Chief Executive (and possibly Minister) on a regular basis?
☑ Is risk just a part of doing business or seen as an add-on, an external imposition?
☑ Do we have the resources in place for the long-term? Training resources? Internal help to operational units? External support when needed?

For the Chief Executive/Deputy Minister/Agency Head

☑ How do we show we are serious about risk management without creating the impression that this is the flavour of the month? Take a long-term perspective with short and medium term measurement of progress? Avoid singling this out, but present risk management as a key part of our overall good management agenda?
☑ Have we sufficiently understood that this is not necessarily about changing our appetite for risk, but managing better the risks we face and have to take to achieve our goals?
☑ How do we avoid scaring people with the terminology? Establish a common risk language? Insist on risk mitigation strategies and communications plans from managers?
Have we covered the bases with our political leaders so that they understand what we mean by risk management and are comfortable with how we are proceeding?

☐ Does the minister need to be involved up-front or simply informed on implementation as part of our general up-dates?

☐ Are we equipped for risk management? Do we have the training, understanding, procedures and reporting that ensure that we use risk management well and not simply create a separate set of concerns?

☐ Have I fixed accountabilities effectively? Not just to my so-called experts, but to the operational managers who run the organization?

☐ Am I giving it enough attention? At the right times?

☐ Are we finding ways to set risk tolerances in the fuzzy areas where numbers are of little help? Through informal discussions? One-on-ones with my key operational managers to test out their views and mine? What about the Minister or his/her staff? Do I need to test out some ideas there too?

☐ Has the implementation plan allowed us enough space and time to work through the best way to do this for our organization?

☐ Is risk management seen as one of our tools of good management and not a new and dangerous idea or something imposed externally?

☐ Are we testing our views out with others, e.g. our advisory groups, central agencies, special interests?

For the Operational Manager

☐ Does my staff have the necessary level and comfort with the concepts? Is the training what they need?

☐ Do I have enough flexibility to build this management tool into how my operation is managed generally?

☐ Is there on-going support for my team? From our own corporate people? From external expertise when we need it?

☐ Do I have the guidance, when I need it, to determine if we are on the right track in terms of such things as:

- our understanding about risk and what it means higher up in the organization
- the timing of our work
- how effectively it integrates and is reflected in my business plans
- are we using the right forms, words and reporting?

☐ Are the discussions we have about risk tolerances within my operation consistent with the direction I get from above? Have I run some issues up the line informally to test them out to set the tolerance level for my people?

☐ What are my timeframes and do I have enough time to get this done effectively?

☐ Is this a flavour of the month or are we serious?