

Some Notes on Integrated Risk Management

Purpose

Integrated Risk Management – or IRM – is at an interesting stage of development within the Government of Canada. Like Strategic Outcome Planning before it, IRM is moving from being a *compliance obligation* – i.e. something required to ensure acceptable Management Accountability Framework evaluations – to something closer to being a “*strategic must-have*” that improves the performance of Departments and adds value to their reputation and “investment worthiness”. Thus, while IRM is in the process of “turning the corner” from “corner of the desk” status to mainstream business practice, that tipping point has not yet been reached, which makes this an opportune moment to offer some comments about how to make IRM more effective and valuable to Departments.

IRM – The “Short Game” and the “Long Game”: Challenges & Responses

At any point in the annual planning and implementation cycle, those in charge of IRM operations in Departments are running both a “short game” and a “long game”. The “short game” involves rolling up program-specific and Department-wide risks into periodic or annual reports that identify “bet the business” risks that merit priority attention by senior management. The “long game” involves embedding a culture of risk awareness and management at all levels in the organization, so that risk management becomes integral to day-to-day operations. Both the “short game” and the “long game” have issues that need to be “wrestled to the ground”.

The IRM “short game” faces two challenges – first, getting the risks right, i.e. identifying and validating risks, and second, creating a decision-making platform centering on these risks. In terms of the challenge of “getting risks right” in the first place, the following comments are in order:

- **Limitations of program self-evaluation:** IRM still depends too much on program self-evaluation, and the biases inherent in that process;
- **Pooling of risk-relevant information:** There are ways to counter-balance the limitations of program self-evaluation, and they involve integrating sources of risk-relevant information inside Departments;
- **Getting external risks “right”:** Counter-acting the limitations of program self-evaluation also involves ensuring that external risks get the same attention as “internal to the organization” risks, which may not be the case, and which may be creating blind spots in IRM;

In terms of the second challenge – creating a risk-based decision-making platform – two points can be made:

- **Getting the corporate risk list “right”:** With respect to making IRM relevant to senior Department management, the structure, number and content of corporate risks may be in some cases be an obstacle to more informed and focused risk-based decision-making; and,

- **Adopting a storytelling approach to IRM:** Like other policy and decision-making functions, effective IRM must involve a strong measure of effective story telling. Risk management needs to tell a short, compelling and convincing story to senior management if it is to make risk management an effective decision-making platform.

With respect to the IRM “long game”, the challenge is one of broadening the IRM footprint in the Department, and several points are relevant here:

- **Encouraging “ownership” of risk:** Anyone who has worked on legal risk management inside a federal department has almost certainly encountered the phenomenon of the Department’s lawyers somehow “owning” legal risk, i.e. as if legal issues did not arise from the operations (or malfunctions) of the programs themselves. To some extent, “failure to own risk” is also an underlying challenge facing IRM operations. But, there may be accountability-related measures that can “encourage” the “ownership of risk”.
- **Developing a community of interest and practice:** Embedding a culture that is supportive of risk management is all about developing and nurturing a community of interest and practice in risk management; and,
- **Building the IRM brand:** Moving integrated risk management from “corner of the desk” status to something approaching a mainstream planning and management activity is all about “building the IRM brand” inside the organization.

1. The Limitations of Program Self-Evaluation

Unlike Audits or Evaluations, which involve officers external to the program coming in and conducting their examinations of program operations, which is of necessity resource- and labour-intensive exercises, IRM operations typically are much less well-resourced undertakings. As a result, IRM depends heavily on self-evaluation by program managers.

Over the long haul, this lack of IRM “boots on the ground” is almost certainly the right way to proceed, because it keeps the onus on programs to internalize good risk management practices, and self-evaluation of risk is an excellent starting point in terms of creating a risk management culture at all levels in a federal department.

The problem, of course, is that self-evaluation is not without its limitations. Essentially, there are two major “risks” associated with program self-evaluation:

- First, the tendency is for programs to *under-state* the extent and intensity of business risks; and,
- Second, there is an equal and opposite tendency for programs to *over-estimate* their risk mitigation capacities.

My own experience tends to support these observations. At various times in my career, both as a public servant and a policy consultant, I have had the opportunity to view the self-assessments of programs with respect to both legal and program risks with the advantage of having detailed Department-wide information on both kinds of risks:

- The number of times that programs have reported no or minimal legal risks when in fact they were running very serious legal risks generated significant levels of cognitive dissonance; and,
- Similarly, the number of times that programs reported no significant business risks when other, rock-hard information suggested the exact opposite was equally troubling.

This may not be a case of a program “keeping two sets of books”, one for the lawyers and one for the IRM types. It may simply be a case of program officers and legal advisors and IRM analysts all not yet speaking exactly the same language. In any event, this is a phenomenon that needs to be addressed, and a bias in risk reporting that is capable of being counter-balanced.

2. Pooling of risk-relevant information

I would venture the guess that most IRM units are still very much in the business of “blazing a trail” and “selling IRM to the rest of the organization”. The match-up is a bit daunting – i.e. a usually fairly small IRM unit attempting to cover the 80 percent of the organization involved in program delivery.

One way of redressing this imbalance in relative resources and counter-balancing the “downsides” of program self-evaluation – i.e. under-estimation of risk and over-estimation of risk mitigation capacity – is to bring to bear more information about programs generated by sources *outside* the programs themselves. In essence, the IRM unit needs to make common cause with other units that generate risk-relevant information.

The first and most obvious candidate would be the Audit Reports and Evaluation Reports generated in every Department of the federal government.

To be sure, the formal language of Audit Reports focuses on compliance with government-wide and Department-specific directives and program mandates, while the formal language of Evaluation Reports focuses on questions of effectiveness, efficiency and economy and the continued relevance of programs to the objectives of the Department and the Government of Canada as a whole.

That said, any analysis of the “conclusion and recommendation” sections of Audit Reports or Evaluation Reports will almost certainly reveal that these Reports are replete with statements that are directly relevant to the identification and management of risks.

A second and perhaps less obvious candidate for hard-nosed, objective information about risks that are either program-specific or Department-wide is the risk assessment process usually managed by the Legal Services Unit in a federal department. What is particularly valuable about legal risk information is that every case identified as a risk can be assessed and compared against other comparable cases and directly related precedents. Thus, notwithstanding the inherent unpredictability of legal cases – i.e. anything can happen in a court room – legal risk information has multiple foundations of objective analysis that is independent of program evaluations.

Both Audit and Evaluation Reports and Legal Risk Assessments are very powerful and credible sources of information that can supplement, counter-balance, and in some cases, challenge the risk assessments made by programs themselves. In both cases, this information is produced by highly trained professionals *not* working in the programs, but working within well-defined analytic frameworks or protocols.

And this pooling of risk relevant information will have the advantage of going well beyond the level of programs. Both the Audit and Evaluation and Legal Services groups have “whole of the organization” mandates and vantage points, and their information can support the IRM team in terms of aggregating risks across the entire set of programs, and thus in making the “tough calls” about which risks require priority attention by senior Department management.

But to do this counter-balancing of program self-evaluation of risk on an ongoing basis, what is required is that the operational silos in which Audit and Evaluations and Legal Services operate be broken down such that there is sharing of risk-relevant information in all directions between Audit and Evaluation, Legal Services and IRM operations and units. Or, put in language less loaded than “silo busting”, the IRM process and the credibility of its assessments will be strengthened to the extent that there is a conscious and determined integration of the work of units inside a department that produce risk-relevant information.

3. Getting external risks “right”

Like most large, complex organizations, Departments tend, for obvious and perfectly understandable reasons, to be “self-absorbed”. Notwithstanding comments already made about the potential downsides of program self-evaluation of risk, it is probably easier for risks *internal* to the operation of programs to be identified, i.e. rather than more externally derived risks. For example, how many organizations, financial or otherwise, saw the most recent economic downturn coming in time?

Accordingly, one way to counter-balance this natural tendency to be more familiar with the inner workings of programs rather than with risks originating from “outside” the organization is to make an explicit linkage between the IRM operation in a Department and that unit responsible for conducting periodic scans of the Department’s environment.

This linkage between IRM and environment scanning is particularly important to improved risk management for several reasons:

- First, the focus of environment scanning is “outside” the organization and the flow of information – the dynamic, if you will – is “outside in”, which constitutes a useful balance to the “inside out” dynamic of Audit Reports or Evaluation Reports, which tell a very useful story about a program to the rest of the Department;
- Second, environment scanning will typically identify factors that have the power to negatively affect the achievement of a Department’s mandate, but on which Departments have influence as opposed to direct control. Thus, if the external risk is big enough, and the Department’s capacity to influence is limited, then the Department is facing a potentially serious challenge to its mandate and this is the kind of risk that can only be identified through a consciously outward oriented environment scanning function; and,
- Third, environment scanning may identify emerging or fast-moving risks that are essentially “out-running” Audit Reports or Evaluation Reports or legal risk analyses, all of which experience time lags between initial identification of issues and drafting of the final reports or analyses.

Finally, making a linkage between Integrated Risk Management and environment scanning can be a promising first step with respect to the integration of IRM into the broader suite of core

Departmental planning processes, which is another way of helping IRM make the transition from “corner of the desk” status to mainstream business practice.

4. Getting the corporate risk list “right”

Getting the Department’s corporate risk list “right” is an important part of ensuring that everyone in the organization is “talking the same language” with respect to integrated risk management. The corporate risk list needs to be a framework that supports common meaning across various risk-relevant operations. For example, this is the frame of reference for understanding where IRM risk-related findings overlap with findings of Audit Reports, Evaluation Reports, legal risk assessments, the results of environment scans, etc.

More importantly, the Corporate Risk List or functional equivalent constitutes the framework for risk-related decision-making by senior Department management. Thus, getting the Corporate Risk List “right” is an essential step in creating a decision-making platform for senior management.

In short order, much of the focus on a corporate risk list revolves around the number and content of the issues that make it onto the corporate risk list. There are several considerations to keep in mind:

- First, while a long list of risks – say, ten or more – will certainly address issues of completeness, this kind of over-running of the target also brings with it the possibility that “if everything is a risk, then nothing is a risk”;
- Second, while it is important to identify a range of externally-derived risks that *could* hurt the Department, it is equally important to avoid making the mistake of “strategic over-reach” and spending time considering risks over which the Department has virtually no control;
- Third, too few corporate risks raises the other possibility, i.e. that important information about significant specific risks will be lost in what becomes too high a level of aggregation of risk-related information;
- Fourth, it is important to watch for items that really have no business being on a corporate risk list. For example, communications capacity is sometimes found on corporate risk lists, when what is really needed is simply a firm message to the Communications Branch to do its job. The same can be said for “HR”-related risks: is there a significant, Department-wide risk “in play”, an issue that, if left unattended, will negatively impact or even cripple the capacity of the Department’s workforce to pursue its mandate, or is this a case of simply ensuring that the Human Relations (HR) unit does a better job of workforce planning? Every item on a corporate risk list has to have a “mission critical” linkage to the ability of the Department to act on its mandate and pursue and deliver on the program objectives set out in the annual Report on Plans and Priorities (RPP); and,
- Fifth, every risk found on a Department’s Corporate Risk List or functional equivalent has to be framed in a specific enough manner that the “story” of this risk can be updated annually in the Department’s RPP or DPR. Otherwise, what is supposedly a Department-wide corporate risk is really nothing more than a “good business practice” masquerading as something meriting more attention than it is worth.

5. Adopting a storytelling approach to IRM

Most Corporate Risk Profiles – or CRPs – tend to be relatively long and overly technical “reads”. That level of detail may be required by central agencies to ensure and demonstrate that a Department has done its due diligence. All too often, however, formal CRP documents come across more as “back of the house” technical supporting documents rather than “front of the house” decision-making platforms.

This raises a directly related concern about the extent to which current IRM practices and products – e.g. program-specific risk profiles or Department-wide CRPs – sometimes tend to be “process heavy” and “insight lite”. Much of this can be reasonably attributed to the fact that the IRM process in most Departments is still very much a “work in progress”, with approaches and formats still in flux and development. And a major challenge in IRM is the aggregation of program-specific risk profiles and insights into a broader statement about current and emerging risks at the level of the Department as a whole.

For all of these reasons, it is proposed here that a storytelling approach be adopted with respect to IRM. After all, the “end game” of the annual risk management cycle is to capture the attention of senior Department management. Thus, at its core, the annual integrated risk management report – usually termed the Corporate Risk Profile – should tell *a short, compelling and convincing story* to senior management about which risks are potentially “mission critical” and requiring priority attention and which risks can be accorded “watching brief” or “watch list” status.

Employing a narrative approach to the Corporate Risk Profile makes any given iteration of this story an opportunity to “pull forward” the Department’s risk management story from the year before and to set the stage for next year’s risk management story:

- Here is where the Department was last year at this time. Those are the risks that we targeted for action, and we can report now on the results of those risk mitigation initiatives;
- Here are the risks we *now* face in the Department, and these particular mission critical risks require immediate and focused attention; and,
- Here is where we want the Department to find itself this time next year in terms of risks that have been successfully contained and with respect to the positioning of the Department to anticipate and respond to risks that might be emerging “just over the horizon”.

Adopting a storytelling approach to integrated risk management at the highest levels of a Department positions the risk management leaders in the Department to develop and update a multi-year narrative structure with respect to investments in the IRM process itself:

- Those are the investments we made last year at this time in terms of improving key aspects of the IRM process;
- We now see that several new improvements are required so that the Department’s capacity to identify and mitigate risks is improved; and,
- This is where we want our integrated risk management system to be positioned a year from now.

Adopting a storytelling approach can also serve as a way of addressing the issues of process and clarity of message identified at the outset of this segment. Focusing on storytelling can function as a form of *triage* which will identify those activities, processes and formats which directly support the telling of this *short, compelling and convincing story* to senior management about “mission critical” (read: “bet the business”) risks that require priority attention, and which processes and activities are less relevant to “getting this story right”.

Another way of looking at this is to think of the storytelling approach to IRM as an opportunity to “reverse engineer” the entire integrated risk management process from a successful presentation of the annual CRP to senior management and work backwards and downwards to identify those activities that “build the story” and those are less directly relevant to “getting the IRM story right”. Using a storytelling approach in this manner will identify the critical pathways from program-specific self-evaluation of risks through the pooling of other sources of risk-relevant information to the development of a CRP that makes its own strong case for consideration by senior management. In this way, the IRM process can become more “content heavy” and “process lite”.

6. Encouraging “ownership” of risk

As noted at the outset, the IRM “long game” aims at embedding a culture of risk management across all programs, organizations and levels in a Department. Part of that “long game” involves the issue of “ownership of risk”.

The complex nature of modern public sector organizations means that, of necessity, it is difficult in many cases to allocate mission-critical risks to a specific senior executive or program. For example, while the rising tide of “boomer” retirements poses a serious challenge for many Departments, the replacement of key scientific, technical or other cadres cannot be the sole responsibility of the Director-General of Human Resources, because making a given Department an employer of choice is a function of senior leadership as a whole. Still, to the extent that serious risk is not “owned” by a single executive, the accountability for risk management may remain cloudy, a situation that does not bode well in terms of effective and accountable risk mitigation.

As noted in the introduction, there is also the ongoing challenge of “ownership” of risk at the level of programs. The ongoing transition of IRM from “corner of the desk” status to mainstream business practice will depend, to some considerable extent, on programs following through on risk mitigation strategies.

In this respect, there is a potential imbalance between the way Audit and Evaluation Management Action Plans – or MAPs – are implemented and the way that program-specific risk mitigation plans are implemented. By and large, the implementation of MAPs is monitored by the Audit and Evaluation units and often reported to Departmental external audit committees. For the most part, it is common knowledge in Departments that non-implementation or outright disregard of MAPs arising from either Audits or Evaluations can have serious negative repercussions. Is integrated risk management in most Departments at the point where the same can be said with respect to the implementation (or lack thereof) of program-specific risk mitigation strategies, and the monitoring of these implementation efforts?

To the extent that non-implementation or under-implementation of program-specific risk mitigation strategies is less accountable than comparable undertakings like Audit- or Evaluation-related Management Action Plans, the incentives for programs to “own” risk will be less pronounced.

7. Developing a community of interest and practice in risk management

If increasing accountabilities relating to risk management is the “stick”, investing in a risk management network is the “carrot” in the “long game” of embedding a risk management culture at all levels of the Department. Risk management workshops are a key element in risk management in both private and public sectors. But networks and workshops should really be viewed as elements in the broader undertaking of building a *community of interest and practice* in risk management.

The concept of a “community” communicates a sense of shared identity and “value”. Taking the time to hold regular video conferences, to share information about developments in risk management inside the Department or inside the Government of Canada as a whole, having guest speakers, holding risk management workshops, sharing success stories – all of these are visible indicators to program officers at all levels and all locations in the Department that what they are doing on risk management is important and valuable to the Department as a whole.

The “word of mouth” advertising on the part of members of a risk management community of interest and practice is very effective in terms of spreading the gospel of risk management to colleagues. And, at the point where members of a risk management community or network feel sufficiently capable and empowered, their “on the ground” leadership and innovation will become a powerful force in terms of embedding a culture of risk management in the Department as a whole.

8. Building the IRM brand

Perhaps the easiest way of making this point is to compare integrated risk management to the Audit function in any Department in terms of brand awareness and brand strength. Audits enjoy both high *brand awareness* – everyone knows about Audits and what they do (and the consequences of critical Audits) – and *brand strength* – everyone accepts the legitimacy and importance of Audits. It is fair to suggest that integrated risk management probably does not enjoy that same level of brand awareness and brand strength – there is probably less uniform awareness about IRM across all levels of a Department, and there is probably less uniform support for or acceptance of the necessity of IRM. In some ways, IRM is still a box to be ticked, something to comply with as opposed to embracing.

Turning the corner on brand awareness and brand strength for IRM will require a number of developments and innovations. For example, if Corporate Risk Profiles become more accessible and compelling documents – and are given that recognition by senior management – this will not be lost on program managers. If senior executives wind up “owning” a major risk and subsequent risk mitigation strategy, that will not be lost on other levels of the Department. If the implementation of risk mitigation strategies is monitored, and if non-implementation comes with negative consequences, that will not be lost on the rest of the Department. And, if officers in programs and Regions are talking about the usefulness of membership in the Department’s risk management network, that will not be lost on the rest of the Department.

Conclusion

The objective of this short article has not been to find fault with the basic design of the IRM process in the public sector of Canada. Instead, the suggestions found here have been put forward as ways of accelerating the transition of IRM from “corner of the desk” status to mainstream business practice:

- The suggestions for pooling risk-relevant information generated by units working outside the program structure and for linking IRM to environment scanning are designed to reduce the reliance on program self-evaluation of risk and reduce the extent to which IRM processes are isolated and “working without a net”.
- The suggestions for “getting the Corporate Risk list right” and for taking a storytelling approach to IRM are designed to sharpen the focus and impact of IRM findings, make CRPs more of a front-line decision-making platform and as a way of reverse engineering from the mission critical bottom lines back to the key activities and processes that support the generation of these bottom lines.
- Finally, the suggestions about “owning risk”, creating a community of interest and practice in risk management and building the IRM brand are all designed to broaden the base of the IRM footprint in Departments. At some point, the IRM short game, building down from the decision-making top, and the IRM long game, building up from the program and Region grass roots, will converge and the result will be an integrated risk management approach that is robust, self-sustaining and indispensable to both senior level decision-making and day-to-day program delivery.