Getting Serious About Risk-Control

BY MALCOLM K. SPARROW

For many agencies of government, risk-control is at the core of their mission. They exist primarily to identify and control harms of one kind or another—actual or potential. They are responsible for such functions as crime control, environmental protection, occupational safety and health, disease control, transportation safety, consumer and investor protection, and national security and counter-terrorism. Risk control is central to what they do.

For many other agencies, risk-control is incidental to their mission. For example, they may exist to provide education or welfare, conduct medical research, promote trade and economic development, or develop infrastructure. In the course of their business, however, they discover the need to protect against a range of risks that could seriously undermine their programs and their ability to carry out their primary missions.

Agencies and departments need to recognize and control their vulnerabilities to fraud, waste and abuse. In the work environment, they carry significant responsibility for controlling workplace violence, occupational safety, sexual harassment, and discrimination. They must guard against corruption, reputational risks, and potential distortions of their agenda from improper political interference. They must protect critical information infrastructures and confidential data. And they all bear some responsibility for the securityand safety of their buildings and personnel.

For more than a decade, I have worked with agencies in the first category—mostly agencies of social regulation and law enforcement—and watched many of them develop a renewed appreciation for the central role that risk-control should play in their operations.

Organizing Around Risks

Organizing around risks and risk-concentrations is quite different from organizing around functions or processes. Agencies learn that risk-control provides a framework within which they can sensibly exercise their regulatory flexibility, and provides a more appropriate basis for constructive and purposeful engagement with industry and the public than the oft misapplied notion of *customer service*.

Executives discover that the existing management literature provides comparatively little guidance (outside the narrow realm of financial risk management) on how to develop and sustain a risk-management operation in practice. Many of them, leading their agencies on this particular voyage of discovery, determine that they ought to give operational priority to the business

The Importance of Structure

The US National Institute of Neurological Disorder and Stroke (Bethesda, Maryland) recently constructed a new, formal risk-management operation. The Institute's primary mission is to guide, fund, and conduct medical research on neurological disorders.

In establishing their risk-management approach, the executive team wanted to avoid duplicating existing work or dressing it up in a new form, and to focus attention on those risk areas which might otherwise be left to fester. Kevin Kirby, Acting Director of the Institute at the time the program was launched, said "I just want to be able to sleep at night, knowing that all the things that ought to be taken care of have been taken care of."

The risk-management approach the institute developed sought to minimize, as far as reasonably possible, the degree to which adverse events—especially those that are unpredictable, uncertain, improbable, or unanticipated—could damage the Institute's ability to pursue its central mission and vision.

The executive team set up committee structure around eight major categories of risk: (1) clinical research risks; (2) risks to the Institute's political and public support; (3) ethics, conflicts of interest, and research integrity; (4) workplace issues (HR, Employment Equity, Sexual Harassment, Workplace Violence, and Occupational Safety and Health); (5) Information Systems and Critical/Confidential Data Issues; (6) Financial Risks; (7) Terrorism; and (8) "Other" (to keep space open for new or emerging risks that did not fit other categories). ■

of identifying and controlling harms, only to discover that they lack any formal machinery to manage or support this type of work.

According to Shane Tregillis, of the Australian Securities and Investments Commission, the challenge "is how to ensure that problem-solving—or our preferred terminology of an 'integrated risk-based approach to compliance and enforcement'—becomes the organizational framework and not just an add-on activity." It is much more difficult "to adopt this as an overall whole-of-organization approach."

Increasingly, agencies are realizing the distance that lies between talk and action. Richard Felder, of the U.S. Office of Pipeline Safety, points out that: "Risk management is much more than the technical models used to calculate probabilities and consequences. To be useful as an alternative regulatory approach, risk management must be an integrated program of activities institutionalized into the way that the company conducts its business on a day-to-day basis."

The pioneers in the area are now recognizing risk-control as a substantial and rather unfamiliar professional skill; they are developing the organizational infrastructure and managerial practices required to place effective risk-control at the heart of routine operations; and the most advanced of them are finally linking the new forms of organizational behaviour with the "results-oriented" performance story that they really want to tell—a story of risks abated, problems solved, and significant patterns of non-compliance eliminated.

Formal Structures

Those who have worked hardest and longest at risk-mitigation say that they experience this work as analytically and intellectually demanding, in ways they could not have predicted going in.

Meanwhile, others see no need for anything new, claiming that risk-control work, where it really is necessary, should simply be delegated through existing line-management structures, with each functional manager or process owner being required to identify and handle the risks within his or her own areas.

Sadly, this approach breaks down at the earliest possible stage—when executives ask for risks or problem areas to be nominated for attention. When the risk-control function is simply delegated down the line, managers will generally identify only those risks of which they are aware, which align neatly with their functional or program areas, and which they are happy to disclose.

But these constitute only a small subset of all the risks that an agency ought to address. These are the risks which are already the most visible and obvious ones—those which are "in your face." These are usually the risks which are already best controlled.

By adopting more formal risk-management structures, agencies are better able to deal with the risks that are invisible or uncertain, unrepresented or under-represented in their normal process flows, awkward in shape and size (thus not falling clearly within the responsibility of any one official or department), or shared (where cooperation with other agencies is a pre-requisite for effective intervention).

Special Risk Challenges

International and global risks are larger-scale or higher-level risks than the available control mechanisms. Global Warming, emerging infectious diseases, genocide, and international terrorism are good examples.

Effective action is limited by the absence of any central control mechanism or any legal mandate or authority to act on a sufficiently broad front. Inevitably, there is reliance on international treaties and voluntary cooperation between agencies, organizations, and nations. It is difficult to divide the work, the costs, and the credit between the contributing parties.

Control operations exist in an environment of multiple and competing perspectives on the problem, often without any effective political process to resolve them.

Where conscious opponents are involved, the "control" business turns into a continuous, dynamic game, played against opponents intent on outwitting the control operation. Examples of such opponents include terrorists, drug smugglers, fraud artists, hackers, and thieves.

There may also be "quasi-conscious" opponents such as viruses that mutate and evolve through a process of natural selection to become drug-resistant.

Control strategies must always take the opponent's adaptations into account. Winning the control game requires close monitoring and study of the opponents' moves, along with understanding and undermining their strategies. Risk control becomes a game of intelligence and counter-intelligence.

Invisible risks are those which by conscious design or by some quirk of their nature, do not reveal themselves. Their magnitude is usually uncertain, resulting in serious under-investment in control.

Examples of harms which often go unreported or under-reported include: corruption; extortion; drug-dealing; date rape; fraud; gambling; prostitution; many forms of white-collar crime; and crimes within the family such as sexual or physical abuse.

To tackle such risks, an agency must first uncover them. Systematic measurement is a critical first step in developing an effective control operation. Proactive and intelligence work are vital for scoping and detection—for helping to reveal the true nature and extent of the risk and to ensure that interventions are designed around the whole of the risk rather than the tip of the iceberg.

Risks where prevention is paramount involve unthinkable disasters—for instance, nuclear or biological terrorism.

It is extremely difficult to estimate the probabilities and magnitude of the risk. This makes it hard to set the budget for control. The norm is serious under-budgeting. It is inherently problematic to justify the cost of such work, given the absence of visible disasters. It is also difficult to measure "preventive performance" in meaningful and persuasive ways.

Interventions must be designed, and their effectiveness measured (to the extent possible) a long way back in a chain of possible events. All control work has to be conceived, organized, and conducted far back in the development of the threat.

Analysis is fundamentally important in breaking the risk and its precursors into elements that can be controlled or reduced.

Where performance is enhanced by risk-taking, the culture may reward and even celebrate excessive risk-taking by those who can get results and "get away with it." Pressure for performance may impel employees to "drive close to the edge"—to the brink of disaster.

Examples include: respect for human rights in the context of interrogation techniques; respect for legal constraints in detective work; respect for safe practices in the construction industry; and risk-taking by investment traders.

Managers may be ambivalent about the degrees of risk-taking they are condoning. They may abdicate their responsibility for supervision, turning a blind eye and preferring not to know how their subordinates are operating.

Organizations may prefer to sacrifice individuals who fall over the edge rather than give up the performance gains associated with risky practice.

Investigation and punishment, after a fall, may turn out to be window-dressing, as the organization may well be reluctant to give up the performance gains.

Risk control within organizations set up to do something else—for instance, fraud control in health care or welfare services, and security operations in an academic or medical setting.

The priorities, the working assumptions, and the cultures of such organizations can make risk control difficult. Risk control operations may run up against built-in assumptions of trust and cooperation and the idea that all the customers or clients are fundamentally honest. The organization may be unwilling or reluctant to devote resources to audit, surveillance, and enforcement. Officials responsible for customer service and process management may end up opposing, sabotaging, or sidelining the risk control operation.

Components Needed

At a minimum, a risk-management system must have the following components:

- *A Nomination System* which generates and funnels nominations for risks to be addressed.
- *An Assessment and Selection System* which allows and requires managers to "pick the important problems."
- *An Assignment System* for committing personnel/resources to risk-mitigation projects.
- *Project Records*: project files, paper or electronic, organized around risks or risk-concentrations (rather than around cases, programs, systems, or functional divisions).
- *Managerial Oversight and Periodic Review* for monitoring and adjustment during the course of any risk-mitigation project.
- *A Reporting System* to highlight success in risk-mitigation.
- *Support Systems*: for Teams/Managers, access to specialists in the risk-management or problem-solving art, as they grapple with unfamiliar work.

Two other features are highly desirable:

- *A Reward System* to provide recognition for project teams that achieve important results.
- *A System for Learning*, to identify: what works and what doesn't; what resources are available within and outside the agency; contact information; and keyword-searchable databases of projects.

Successful Risk-Mitigation Projects

More and more agencies are learning how to organize resources around important risk areas and to respect the natural shape and size of problems they seek to address, rather than forcing them into the existing organizational apparatus.

In reflecting on their hard-won successes, agency executives usually discover that the following observations apply to their successful risk-control initiatives:

- Neither the specific components of the risk, nor the solution, were conceived anywhere in the agency's legislation. The solution of the problem or the mitigation of the risk required neither a change in legislation, nor any change in the agency's general policies.
- The "problem" or "risk-concentration" was identified, managed, and solved below the level of strategic planning. Although the agency's mission statement, authorizing legislation, and strategic plans might specify broad classes of risk, successful projects usually address carefully delineated sub-components.
- Responsibility for tackling the problem did not naturally lie with any one official, and had to be assigned. Attention to the problem would have remained diffuse, uncoordinated, and probably ineffective, had senior management not made a conscious decision to organize resources around it.
- The relevant performance measures (indicators of risk-reduction success) were specific to the project and were selected before developing the action plan. Designing relevant metrics took as much creativity and imagination as the action plan itself.
- The team needed the flexibility to experiment with a number of approaches, quickly abandoning those that did not work. The team could not have predicted in advance what would work, or how much it would cost

Difficulties and Success Factors

Obstacles

After Florida's Department of Environmental Protection had spent two years attempting to formalize their approach to operational risk-control (which they termed "Environmental Problem Solving"), the key staff driving this system came up with their top ten reasons why they considered this kind of work basically "impossible":

- It's viewed as *extra*: Everyone is busy with more structured and manageable tasks, all of which have deadlines and therefore take precedence.
- The required analytic support (data analysis and help with statistical work) is not available.
- No formal budgetary support or legislative mandate for Problem-Solving/ Risk-Management. Everything else the department does has both.
- Real world problems come in awkward shapes and sizes, which do not fit established groups or units. Dealing with them properly requires coordination and commitment across different units and agencies.
- Management does not understand this kind of work, and fails to support those who try to do it.
- Problem-solving and risk-mitigation work brings an unfamiliar degree of *discretion*, and uncertain degrees of *authorization*. Risk-mitigation teams are not sure whether they can commit agency resources. Persistent uncertainty can bring projects to a standstill.
- Many agency staff—and some managers—are not really clear whether this type of work is actually *new*. Many think it isn't. If it's not new, why should anyone worry about it? But if it is new, and important, then it demands attention, recognition, and dedicated resources.
- Risk-mitigation project teams are generally incapable of methodological rigour, and don't understand why the different stages are necessary.
- Risk-control involves working with external parties (representatives of regulated industries, and of interest groups) under unfamiliar terms of engagement.
- Risk-management is rejected by many as one of the fashionable new soft options being pushed by senior management as they cater to political pressures.

Overcoming these Challenges

In Florida, these difficulties were eventually overcome as a result of three factors:

- *Sustained managerial commitment* to the approach over time (despite changes in administration).
- The production of risk-mitigation *accomplishments* (e.g. as recognized by awards and favourable media attention).
- Construction of the necessary *formal apparatus* to drive risk-control operations on a continuing basis.

Why place so much emphasis on formal machinery? Experience shows that without the machinery, risk-mitigation work will happen only spasmodically—conducted here and there by a few entrepreneurial individuals.

In order to institutionalize this new form of work, any organization needs mechanisms to identify the work, require attention to it, drive it, manage it, record it, report it and reward it. Otherwise, all other types of work—with their deadlines and mandates—will take precedence, and risk-mitigation will make little progress.

(as contemplated by some performance-based budgeting requirements).

- The remedies invented were qualitatively new—not merely mixtures of existing methods and tactics.
- All personnel engaged on the problem solving team had other duties. Once the problem was solved or the risk-concentration sufficiently mitigated, the project entered a longer-term "maintenance" phase, and the original project team ceased to exist.

Long Term Effectiveness

Risk-management remains relatively immature as a pattern of organizational behaviour. Much has yet to be learned about the structures and mechanisms necessary to support effective risk-management in the long term, and the particular challenges presented by special classes of risk.

Pioneering agencies find this work to be different, unrelentingly difficult, and intellectually demanding. Many government agencies, especially regulatory and enforcement agencies, are adopting risk-management frameworks to reorient their core businesses. Many others are recognizing the need to use formal risk-management approaches to protect their personnel, their clients, their resources, and their ability to carry out their primary missions.

We are just beginning to realize the importance to society of developing the art of risk-control as a core professional skill for public officials.

Dr. Malcolm K. Sparrow is Professor of the Practice of Public Management, John F. Kennedy School of Government, Harvard University. A mathematician by training, and formerly a Detective Chief Inspector with the British police service, he now specializes in issues of enforcement strategy, regulatory compliance, risk control, and intelligence analysis.

Dr. Sparrow is the author of ***The Regulatory Craft: Controlling Risks, Solving Problems and Managing Compliance*** *(Brookings Press, 2000), upon which this article draws.*

He will be the Keynote Speaker at the Ontario Red Tape Commission's International Conference, to be held in Toronto from September 25-27, 2002.