

Risk Management for Regulators – Part 2: Risk Identification

by Richard Steinecke
October 2014 - No. 190

As discussed in the last issue of *Grey Areas*, risk management follows a systematic cycle beginning with risk identification and then moving on to risk assessment, risk treatment and monitoring and assurance. In this issue we look at risk identification for the three areas in which a regulator is most likely to employ risk management, namely:

- for the entire organization,
- for specific initiatives and policies, and
- for an external review from the perspective of those most protected by the regulator.

The goal of risk identification is to comprehensively review all aspects of the external and internal environment so as to recognize and list every event that could prevent or help a regulator achieve its objective. An unidentified risk has the potential to do the greatest harm to the regulator as no steps will be taken to prevent or reduce the consequences of that risk.

Risk Identification for the Entire Organization

When beginning systematic risk management for the first time, it is useful for the organization to do an environmental scan. Typically this involves reviewing the key documents for the regulator (e.g., enabling legislation, governance policies, website), searching for external comments about the regulator (e.g., audits

and reviews, media reports, literature review, government statements, court and tribunal decisions), interviewing knowledgeable observers and stakeholders and even a sample of those dealing with the regulator, interviewing senior management and a representative sample of front line staff, and conducting an on-site visit to observe the operations of the regulator. The purpose of the environmental scan is to help identify the questions to be posed when conducting the formal risk identification process.

The regulator then assigns an individual or small group (risk manager) to facilitate the risk identification process. The risk manager can be internal or external, but must have the support of the leadership of the organization to ensure that everyone participates fully in the process.

There is no single correct risk identification process. Typically, the risk manager begins by systematically reviewing all available documents and speaking with all available individuals for each of the four risk quadrants (i.e., hazard risk, operational risk, financial risk, and strategic risk) discussed previously. A physical inspection of the actual operations of the regulator can often be helpful even for those with some familiarity with the regulator. The risk manager will be asking “what could possibly go wrong?” and “how could this be done better?”

Checklists are often available for the more generic risk categories. For example, insurers often have listings for insurance risks. Risk management associations may have generic checklists available. A wealth of risk management literature can help in developing a more tailored checklist. Risk managers

FOR MORE INFORMATION

This newsletter is published by Steinecke Maciura LeBlanc, a law firm practising in the field of professional regulation. If you are not receiving a copy and would like one, please contact: Richard Steinecke, Steinecke Maciura LeBlanc, 401 Bay Street, Suite 2308, P.O. Box 23, Toronto, ON M5H 2Y4, Telephone: 416-626-6897
Facsimile: 416-593-7867, E-Mail: rsteinecke@sml-law.com

WANT TO REPRINT AN ARTICLE

A number of readers have asked to reprint articles in their own newsletters. Our policy is that readers may reprint an article as long as credit is given to both the newsletter and the firm. Please send us a copy of the issue of the newsletter which contains a reprint from Grey Areas.

Grey Areas

A COMMENTARY ON LEGAL ISSUES AFFECTING PROFESSIONAL REGULATION

for other similar organizations may have checklists that can be used.

From the above materials, surveys on specific risk areas (e.g., the registration process, the complaints and discipline process, continuous professional development, users of the regulator's website) can be developed for administration to the staff of the regulator, registrants, the primary beneficiaries of the regulator's activities, and stakeholders.

Brainstorming activities are also typically employed. This can be done in writing, in focus groups, with experts or consultants or in workshops with staff of the regulator. For example, meeting compliance obligations is a fundamental risk management activity. However, identifying all of the compliance obligations for the regulator itself (rather than the regulated) is not straightforward. Many organizations are not aware of all of their compliance obligations. Even asking the regulator's lawyer (whose role is generally to respond to requests for specific advice on particular issues) will probably not provide an exhaustive list.

The risk manager would probably also need to do the following:

- speak with the regulator's chief executive officer (and assistant) about what reports the regulator must file each year;
- survey the heads of each department (e.g., human resources, corporate, finance, IT) about the compliance obligations of which they are aware;
- touch base with the regulator's auditor;

- compare notes with other similar regulators to see if they are aware of other compliance duties; and
- conduct independent research of additional compliance obligations that the above steps may have missed. Again, checklists from other sources might be valuable here.

Strategic risks are the most difficult to identify. While some, such as the demographic changes (e.g., aging society, immigration) are fairly well known, others are not so obvious. Many professions have been taken by surprise by rapid technological change (e.g., the ability to provide services or products over the internet), social and economic developments (e.g., transferring services off-shore) and sudden media interest (e.g., in the complaints process or in quality assurance activities). Risk managers will not only want to involve as many people as possible in identifying such risks (e.g., a workshop with Board or Council members; focus groups with stakeholders) but will also review the experience of other regulators for analogous risks.

At this point, the risk manager's goal is to obtain a complete list. The analysis of the significance of the items on the list does not take place until the risk assessment stage. If a regulator has not already done much risk management activity, the initial risk identification process can be a lot of work. On the other hand, if a regulator has done some risk management activity, there is a danger that it will simply compile the currently identified risks into a single list without looking for other unidentified risks.

Grey Areas

A COMMENTARY ON LEGAL ISSUES AFFECTING PROFESSIONAL REGULATION

Risk Identification for a Specific Initiative or Policy

The risk identification process for a specific initiative (e.g., whether to purchase property or continue to rent) or policy (e.g., making complaint decisions public) is much more focused than an organization-wide one. The purpose of the process is to identify all of the events that could hurt or help in achieving the initiative's goals. Risk management principles can be used to enhance the existing project management or policy development processes. For example, if the current policy development process involves committee discussion, staff input, Board or Council discussion and consultation with the profession, risk management principles could enhance the process.

Many of the techniques identified above can be employed (e.g., research, surveys, interviews, workshops, consulting experts). Again the policy person (or, if there is none, the risk manager) will be asking "what could possibly go wrong?" and "how could this be done better?" The techniques will be implemented in a systematic manner until the policy person / risk manager is satisfied that all risks (good and bad) have been identified.

For significant initiatives or policies there are specialized tools that experienced risk managers can employ, such as cause and effect analysis, failure analysis, future state analysis and strategy analysis.

External Risk Officers

An external Risk Officer focuses on risks to the primary beneficiaries of the regulator, often the clients of those being regulated and the general

public. This focus on the client may result in a different prioritization of risks. For example, while an insurance claim for injury to a visitor to the regulator's office has some impact on the regulator's effectiveness, it is unlikely to be the most significant risk to the clients of those being regulated.

Thus, the Risk Officer begins by trying to identify the risk events that are likely to produce the greatest harm or the greatest benefits to the primary beneficiaries. In other words, what change in the regulator's activities (e.g., modifying how inspections are done) would result in the least amount of harm to the most beneficiaries?

This focus helps direct the Risk Officer's approach in conducting risk identification. A Risk Officer may search for sources of data on the most frequent and most serious harm done by regulated members to their clients. For example, analysis of inquiries and complaints made to the regulator, court and tribunal decisions (e.g., civil suits and human rights complaints) and surveys of a sample group of primary beneficiaries may provide useful information.

Once the risk identification process is complete, the next step is risk assessment, which will be discussed in the next issue of *Grey Areas*.