Grey Areas
A COMMENTARY ON LEGAL ISSUES AFFECTING PROFESSIONAL REGULATION
SML
Steinecke Maciura LeBlanc
Barristers & Solicitors

Risk Management for Regulators – Part 5: Risk Monitoring and Assurance

by Richard Steinecke
February 2015 - No. 193

As discussed previously, 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 the risk monitoring and assurance stage.

Once the risks of a regulator have been identified and analyzed, and the plan to treat those risks has been developed, the regulator needs to implement the risk treatment plan and monitor its success.

The first step to implementing any plan is documenting the plan. While various approaches have been adopted, perhaps the most useful and essential document is a Risk Register. The Risk Register often takes the form of a chart listing the major risks (either for the organization as a whole or for a specific project). The content of the Risk Register varies, but it typically includes the following information:

- The name and description of each risk. For example, for a paperless Board meeting initiative, two of the risks might be that Board members might not read the materials thoroughly and that the electronic form of the information might, more positively, allow search and link features to facilitate using the information.
- A score as to the likelihood of the risk occurring, its severity if it does occur and an ultimate risk level (which could simply be the product of the frequency and severity scores). For example, on a scale of 1 to 10, absent risk treatment measures, there may be a 6 / 10 frequency score and a 4 / 10 severity score for each of the two risks identified above (thus both having a score of 24).
- A list of the proposed treatment for each risk. For example, the reluctance to read electronic documents could be addressed by educating the readers as to the advantages of using electronic documents, by providing a person to contact if there are any problems, and by supplying resources (e.g., tablets) to make reading the documents easier and more fun.
- The date by which the risk treatment step is expected to be implemented.
- The person responsible for treating and monitoring the risk (called the "risk owner").
- The anticipated risk level (score) once the modifications have been fully implemented.
- The date by which the risk and its treatment is slated for formal review and reconsideration.

Another key implementation step is communication. There certainly needs to be internal communication about the risk, its significance to the organization, the nature and rationale for the risk treatment plan, the actions each person is asked to take and the record-keeping expectations. It is especially important that front line people (in this case, Board members and their support staff) understand why the change is being initiated and the benefits to both them and the organization if the change is successfully achieved.

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

External communication may also be important. In this example, observers at Board meetings should know where the piles of paper went and how they can obtain access to any public documents. In addition, practitioners and other stakeholders might benefit from knowing that their regulator is reducing costs and waste and gaining better access to information when making decisions.

Monitoring the implementation steps is necessary to ensure that they are being done and to address any unexpected resistance or outcomes. The organization's usual methods for monitoring operational change may be sufficient.

Risk management is not an excuse for the Board to interfere with operational details. In our example, the Board will obviously be involved since it affects the Board. However, in respect of the rest of the organization going paperless, the Board would probably receive only a high level report and assurance of progress. The report might be no more detailed than an updated copy of the Risk Register described above.

Before implementing the risk treatment plan, the data to be gathered when implementing the initiative should be identified. For example, for Boards going paperless, some of the data gathered might include:

- satisfaction surveys by Board members (especially to see if there is a change over time);
- information gathered data by IT staff as to whether the features of using electronic documents (e.g., search functions, hyperlinks) are being utilized;
- monitoring as to whether the amount of information being provided to the Board is increasing because it is electronic and whether this additional information is perceived as helpful or overwhelming; and
- surveys of Board members, senior management and others as to whether they perceive that the quality of the Board's decisions has improved.

In addition to the specific information sought, the organization should also ask itself whether there are any unexpected consequences to the risk treatment plan. For example, perhaps the Board members have used the technology to do their own research on "hot topics" and have added that information to the meeting materials for other Board members to review. Or perhaps Board members have started to enter and share electronic notes on documents. Are those unanticipated outcomes good or bad for the organization?

In addition, as more and more people within the organization become familiar with risk management concepts, they may identify emerging or unnoticed risks that should be considered. For example, front line staff might become aware of Council members taking their tablets to IT service and supply companies with repair issues and thereby exposing confidential information to public access.

All of this information should then be available to restart the regulator's formal risk management cycle process. Properly done, risk management never ends.