10 strategies to keep risk management alive

After developing a formal enterprise risk management framework, one of the ongoing challenges is to keep your risk management program up-to-date. Tony Harb and Mitchell Morley, risk management, audit and governance specialists from InConsult, provide a number of strategies to help keep risk management alive.

Just like every other management system, risk management requires ongoing and regular attention at all levels of the organisation.

AS/NZS ISO 31000:2009 Risk management - Principles and guidelines certainly provides guidance on 'what' organisations should do with respect to monitoring, review and continual improvement, but leaves it up to each organisation to determine 'how'.

So, what do leading organisations do to keep their risk management framework alive?

1. Get sufficient resources

Risk management will require a 'minimum' level of activity to keep the framework functioning well. Therefore ensuring the organisation is adequately resourced is essential.

Many organisations have one, multi-tasked risk manager who also undertakes a range of other activities such as insurance claims, quality, compliance or business improvement. These other activities all compete with risk management specific activities.

Two strategies to help "resource up" risk management are to create 'risk liaison' roles within business units and, where available, utilise internal auditors to assist in some initiatives like risk workshops and training.

Risk management and audit can play 'tag team' by aligning some of their activities.

2. Set clear responsibilities

Risk management is only as effective as its weakest link. Therefore, risk management responsibilities should be clearly documented in the organisation's Risk Management (RM) Policy and RM Plan.

Ensure the RM Policy and RM Plan are clearly communicated to risk owners.

For risk owners, ensure that job descriptions contain general responsibilities for identifying, evaluating, communicating and monitoring risks and ensuring appropriate internal controls are maintained at all times.

3. Regular review of risk registers

Risk managers are not solely responsible for managing risk. Ultimately risk owners are responsible for ensuring risks are identified, evaluated and controls or treatment plans are in place.

ISO 31000 outlines 11 important principles of effective risk management. One principle states "Risk management is based on the best available information" and another "Risk management is dynamic, iterative and responsive to change". Therefore a regular

review of risk registers and incidents is necessary to ensure information is current, relevant and reflects change in circumstances.

These reviews should be conducted on an ongoing basis or as deemed 'necessary' by the risk owners particularly after an incident. Whilst risk management should be ongoing, at minimum, we suggest a formal review no less than twice per year.

Logistically, we recommend risk managers conduct one-to-one risk register review sessions with one or two risk owners per month, rather than having to meet all 25 risk owners in the one month!

4. Continually change context of risk assessments

Risks arise from many sources and can have many and multiple consequences...recall the bow-tie diagram?

ISO 31000 recommends periodically reviewing whether the risk management framework is still appropriate, given the organisations' external and internal context.

It is critical that risk profiles be reviewed and enhanced continually with a different context or angle.

Most organisations on a limited budget start with risks that could impact objectives, and then move to process level risks, regulatory risks, stakeholder risks and so on.

5. Involve risk owners in other department risk workshops

Risk management provides opportunities for organisations to break down departmental communication and process silos within an organisation.

We encourage supporting departments such as finance and IT to attend risk workshops of other departments to help them gain a deeper understanding of risks and the importance of financial and system controls in managing those risks.

6. Establishing a Risk Management and/or Audit Committee

Establishing a Risk and/or Audit Committee with independent experts is another way of helping to keep risk management alive. In most organisations, these committees meet from 4 to 6 times per annum.

Why not have risk owners present their risk profiles to the committee?

Risk owners will need to get a good understanding of their risks and controls. The committee will have an opportunity to 'quiz' risk owners about their department, objectives, resources, risks and controls.

7. Quarterly newsletter

Risk management practices need to remain "front to mind" not "out of sight, out of mind"!

An effective way to maintain a strong risk and governance culture is to publish a quarterly newsletter and send it to all staff. This is an excellent way to update staff on new compliance requirements, potential issues, emerging risks or perhaps a friendly reminder for risk owners to update their risk register.

Alternatively, you can incorporate a risk, audit and governance section in a corporate newsletter.

8. Track completion dates of key activities and report to Audit Committee

Risk management is all about getting things done. For example, doing the risk assessment, completing the treatment plan and investigating the incident.

ISO 31000 recommends organisations measure progress against, and deviation from, the risk management plan. Risk managers should report on risks, progress with the risk management plan and how well the risk management policy is being followed.

Failure to undertake these activities could result in risks not been adequately managed and exposure to risk events outside the organisation's risk appetite.

Effective monitoring of tasks (both over-due, completed or upcoming) is critical for keeping risk management alive. This is where risk management technology can really add value.

9. Pursue continual improvement

In line with ISO 31000, risk managers should be asking how the risk management framework, policy and plan can be further improved.

It is therefore critical that risk managers involve risk owners in continual improvement and refinement of the risk management framework.

Risk managers should implement formal feedback mechanisms which could include surveys, questionaries and one-to-one meetings.

Attending conferences, extensive reading and networking with other risk managers both within your industry and outside your industry enables risk managers to get new ideas and apply them.

10. Independent review

ISO 31000 recommends a periodic review the effectiveness of the risk management framework.

Ideally the review should be conducted by a person independent of the framework and should not just be a simple compliance review against the existing framework, but also a benchmark against other organisations and various risk management maturity models.

Bottom line

Risk management is not a one-off activity. It is a management system that requires ongoing monitoring, review and 'tweaking' to ensure risk management is part of the organisation's DNA not only to protect it from threats, but to help achieve organisational objectives.

Tony Harb & Mitchell Morley can be contacted on 02 9241 1344 or tonyh@inconsult.com.au