

Instilling a risk aware culture in an organisation

*Frank Kominos **

Why is risk management important?

While many people argue that risk management is good business practice, the inescapable fact is that the world demands it.

Regulators across a range of industries now insist that companies have robust risk management practices in place. Financial services providers in particular, have to demonstrate such practices as a specific requirement of their licensing conditions.

Boards and senior management have a vested interest in the quality of the company's risk management programs. Therefore, they have increasingly taken an active interest in this area over the last few years. In addition, the sharemarket and ratings agencies are increasingly considering the quality of the company's risk management program as one of the factors used in determining the quality of the company and its management.

While the Risk Management Standard of the Joint Standards Australia / Standards New Zealand Committee provides a helpful framework and reference source for identifying and treating risk, financial services companies must comply with a multitude of other regulatory requirements related to risk management and compliance.

For example, Vero Insurance Limited (Vero), as a general insurer, is bound to comply with APRA's prudential standard on risk management.

This standard seeks to ensure that an insurer is well managed, has access to appropriate independent expertise and has systems for identifying, managing and monitoring risks that may reduce the ability of the insurer to meet its obligations to policyholders.

APRA's standard also notes that the Board and senior management are responsible for risk management and need to introduce effective systems and controls to address business risks. It also stipulates that companies develop, implement and maintain a sound and prudent risk management strategy. This strategy must be documented, approved by the Board, provided to APRA, and audited annually.

What does a risk management program look like?

The risk management program essentially documents your overall risk management framework, structure and people, as well as summarising your detailed risk management practices and processes.

Some of the important elements that you require for a robust risk management program include:

- Determining what the company's appetite for risk is
- Articulating the risk management methodology

- Developing the formal structure, including clearly defining all roles and responsibilities
- Determining whether dedicated resources are required to oversee the program
- Developing a comprehensive training and education program
- If necessary, introducing risk management software to help administer the program, and
- Deciding upon the level and timeframes for risk management reporting (in particular, how these will link with existing management reporting and business decision making routines).

At Vero, after a careful review of the above criteria, we developed and then implemented a risk management program over a number of years that fits in with our particular needs. It is vital that an enterprise view is taken. The risk management program will only add value if it is consistently applied across the company. In addition, the risk management program should be constantly renewed. Therefore, a company's risk management program must incorporate a process that is closely monitored, reviewed and enhanced accordingly.

What are the key challenges?

There are a number of key challenges that companies face when developing and implementing a risk management program. The important challenges include:

- Embedding the risk management culture
- Obtaining buy-in from the Board, senior management, business unit management, and staff
- Ensuring widespread understanding and the involvement of all business units
- Ensuring consistent risk profiling and risk management reporting
- Adhering to the continuously changing regulatory environment, and
- Acknowledging that you are managing risks in a dynamic and uncertain world.

The risk management program can fall down at any stage of the process. However, the two most important elements to focus on are the culture of the company and the involvement and support of management and all staff in the risk management process.

Vero's training and education system emphasises that everyone has a role to play in the process. Risk management and compliance are everyone's responsibility. At the micro level, this could simply involve all staff being pro-active in making improvements to their individual work processes. This is risk management in action, albeit at the simplest level.

As part of the designated roles and responsibilities, the Vero management team owns and drives the risk management program. This has ensured that the culture has been set from the top. "Culture" is a concept that is difficult to define in a few words. But at Vero we have simply actioned this to mean "how things are done around here" from a risk management perspective.

Vero undertakes an annual risk management survey of all management and staff. The survey asks a number of questions that are used to gauge the effectiveness of Vero's risk management and compliance program and provides an opportunity for

staff to suggest areas for improvement. This survey has led to increasingly positive results over the last few years, reflecting the fact that our program has matured.

Vero has consistently made improvements, especially to our training and education program, introduced a consistent methodology and streamlined risk reporting. Management and staff see the benefits of the program, and in particular its direct link to both good corporate governance on the one hand, and sound business practices on the other.

How do you address these key challenges?

Addressing the key challenges can appear overwhelming at face value. It is best to take a practical approach. Vero have embedded our risk management program into our standard business practices.

Vero did not want risk management and compliance to be seen as separate or distinct activities. The worst thing that can happen is that risk management exists in isolation, and is considered to be “somebody else’s problem”. Therefore, while the Board and senior management own the overall risk management program, each Vero business unit manager owns and is responsible for their particular risk profile and for resolving matters as they arise.

Vero have always tried to embed a culture that views good risk management and compliance as being good business practice. It is not just a form filling in exercise. At a minimum, a risk management program needs to meet the requirements set down by the regulators. The regulations must be kept at the forefront of planning, development and implementation of successful risk management and Vero strongly adheres to this.

However, the culture within a company is something that you cannot get from the risk management standard or from regulatory requirements. This comes down to the people within the company and will develop over time. There is no magic ingredient or quick fire solution. At Vero, we think that a practical approach is the best approach. Some of the elements to consider in building a “risk aware culture” within your own company are:

- Regularly communicating the risk management program to management and staff so that it is visible, ongoing and embedded at various levels within the company
- Developing a team based approach where risk management is seen as a collaborative effort
- Fostering an environment where staff and management are encouraged to identify and manage risk, or alternatively, know who to escalate it to
- Adopting common risk management terminology
- Developing a risk management software tool that is easy to use and understand (this can help to administer the program and/or streamlines risk management reporting)
- Developing human resource practices that encourage a risk aware culture
- Encouraging positive risk management behaviour and actions through the use of recognition and reward initiatives, and

- Conducting surveys of management and staff on their attitudes to risk management.

Another practical way that Vero has embedded a risk management culture across the company is by linking the program to Vero's existing continuous improvement process. As noted earlier, it makes sense to embed the risk management program into existing business practices as far as possible.

One desired outcome would be to see risk management and compliance questions and matters being raised by staff and reported to management. Another outcome would be to see an appropriate person always taking ownership of particular risks and associated controls. To help this process along, Vero have included risk management into the company's overall balanced scorecard, and where appropriate, it is incorporated into an individual manager's performance measures.

Vero's own experience suggests that adhering to a mandated standard is only one of a series of steps companies need to take to successfully implement a risk management program.

These may range from consistent risk profiling and risk management reporting in the context of ongoing commercial uncertainty; adhering to a constantly shifting regulatory environment; and obtaining buy-in from the Board, senior management, and business unit management and staff.

An enterprise-wide view is critical - the risk management program will only add value if it is applied consistently across the company.

All these factors are important considerations when implementing an effective risk management program. However, the most important – and difficult – challenge is that of instilling a robust risk management culture.

Although the management team needs to own and drive the risk management program to ensure the culture takes root at the top, a company-wide training and education system should emphasise the role that all management and staff play in the process.

A practical approach to risk management will help to “embed” a company's risk management program in its standard business practices.

By all means, use available reference material such as the risk management standard and the experiences of other companies to guide your journey, but remember to tailor these to your own company's culture, and existing business practices and reporting processes.

An example of determining risk categories

It is important that business unit risk profiles have a consistent range of relevant and material risks to avoid the “garbage in – garbage out” problem. Another obvious benefit is that it makes the aggregation of risk at a corporate level much easier.

One way of achieving this is to provide a consistent set of risk categories that should be used by the business units in maintaining their detailed risk profiles.

The risk categories should be based upon the requirements of the particular company. In the case of Vero, the Board agreed that the following eight risk categories are applied across the business.

- Business Risks – This risk includes the sub-categories of Underwriting, Claims, Pricing, Reinsurance, and Emerging Risks. This risk category essentially needs to incorporate your company's main operating areas
- Customer Risks – This risk covers areas such as Distribution Channels, Alliances, Advertising and Marketing
- Strategy Risks – In other words, the risk of not following your company's stated strategy
- IT / Infrastructure Risks – This risk includes areas such as Systems, Management Information, and Disaster Recovery Planning (DRP)/Business Continuity Planning (BCP)
- Compliance Risks – This risk incorporates all Legal, Regulatory and Corporate Governance related areas
- Reputation Risks – This risk includes potential Brand damage
- People Risks – This risk includes all People Management related risks and Staff Retention/Succession Planning issues
- Financial Risks – This risk incorporates areas such as Capital Management, Investment Management, Liquidity, and Credit Ratings

The company's agreed risk categories, which will differ from business to business, should be embedded within the software tool used to maintain risk profiles and report on risk management outcomes. These standardised risk categories will form one part of the risk management methodology applying within the company.

Using common risk management terminology leads to everyone in the organisation - at all levels within the company – speaking the same language.

** Frank Kominos is Head of Risk & Finance at Vero Insurance Limited, one of Australia's leading general insurance companies.*