

# RISK GOVERNANCE A FOUNDATION FOR EFFECTIVE RISK MANAGEMENT

---

The economic crisis has led organisations to reconsider their approach to risk management. **Mike Sullivan** looks at the foundations that support a strong risk management programme.



---

“WHATEVER THE DRIVERS ARE FOR YOUR ORGANISATION, ACHIEVING EFFECTIVE RISK MANAGEMENT REQUIRES A SOUND FOUNDATION OF RISK GOVERNANCE — THE STRUCTURES, CULTURE AND PROCESSES THAT SUPPORT GOOD BUSINESS DECISION-MAKING.”

---

**C**an risk management actually help to protect business? It's a question that has been asked regularly since the start of the economic crisis. However, evidence suggests that the companies that fared best in the downturn were those that had a clear, realistic understanding of their risks; had actually taken steps to address their key risks; had defined clear roles, responsibilities and accountability for managing risk and had a culture that encouraged open discussion of risk and emerging issues. So it may be fairer to say that the economic crisis exposed a weakness in the risk governance of many organisations. Perhaps a recognition of this weakness is highlighted by the fact that 89% of surveyed CEO's tell us that they plan to change their approach to risk management in 2012.

It's not that risk management hasn't been on the agenda for most organisations. But we are now seeing it rise further up the agenda and become core to surviving in a

turbulent world. The drivers behind this are varied and include:

- ▶ The scale of uncertainty in every market place and in every aspect of business means that risk considerations have to be a key factor in all business decisions;
- ▶ The emergence of risks that previously would have been thought of as remote or theoretical. For example, some organisations are doing scenario planning around the possible collapse of the euro and the practical implications for their operations and finances. Two years ago this type of risk would not have been on the radar of most companies;
- ▶ For regulated entities, particularly in financial services, governance requirements are becoming more onerous and regulatory reviews more common. Those reviews are detailed in nature and, as part of these reviews; organisations large and small are being asked to demonstrate

how they are managing risk. Risk management policies, risk registers, internal control procedures and the output of internal audit activity are all looked for as part of the reviews – and key staff are being interviewed to assess their awareness of the policies;

- Outperforming the competition. In an economy where you need to consider how critical parts of your supply chain are managing their own risks, companies are turning to suppliers who are “safe to do business with” and who can demonstrate a culture of sound risk management. Trust in the reliability of your service provider is key and companies are willing to pay a price premium to suppliers who they feel they can trust to be with them for the long term.

Whatever the drivers are for your organisation, you need to establish a solid foundation of risk governance as a basis for an effective risk management program. This foundation should reflect the appropriate structures, culture and monitoring mechanisms that will help steer the organisation towards measurable and sustainable success. Let’s remind ourselves of the key elements of risk governance.

## **ELEMENTS OF STRONG RISK GOVERNANCE**

### **1. Putting the right structures in place.**

Effective risk governance should provide the operating model and decision-making framework needed to identify and respond to risks. To be effective, all the pieces of the framework need to be in place and operating. It starts with the board and senior management.

The board should not be involved in day to day risk management. However, through its oversight role, the board should review and approve the policies and infrastructure that management have put in place to manage risk. Their role involves reviewing and approving the organisations risk appetite by reference to the overall strategic objectives. While it ultimately remains their responsibility, the board often uses their committee structure to help in carrying out certain of their risk functions. For example, the Audit Committee can help the full board oversee the effectiveness of the enterprise risk management system. Recent corporate gover-

### **Suggested practical steps**

1. Perform a health check of your risk governance strategy, structure, culture, resources, processes and responsibilities. Use the assessment to identify any gaps and determine appropriate responses.
2. As part of the check, companies should consider the role of the Board and Audit/Risk Committee? Do the members fully understand their role and responsibilities? Are the skills and experience right for your organisation? Are the members getting what they need from your Risk function? From Internal Audit? Are members getting the right information to help meet their risk management oversight responsibilities?
3. Define and document your organisations risk appetite.
4. As a board, committee or management team, take some time out to self-assess your organisation against the risk culture attributes listed and determine if there are any areas that may need to be addressed or improved.
5. If you haven’t already done so, establish a risk-information system to capture information about your major risks and monitor them continuously.
6. If you are already reporting on risk management, review how your reporting at all levels (operational, senior management and board) measures against the criteria noted. Use the assessment to look at ways of improving the effectiveness of your reporting.

nance changes have seen the role of the Audit Committee and its members become more difficult and challenging than ever. Along with increased expectations from shareholders, regulators, and other stakeholders; there is a heightened scrutiny when things go wrong; more defined responsibility for risk management; and more focus on the need for fraud prevention.

Senior management are responsible for developing and implementing the organisations risk management policies and supporting processes. These should be designed to allow the business to develop a comprehensive view of risks and ensure risk management is an actively considered in all key business processes, operating units and decision making activities. Together with the board, senior management should over-see the implementation and effectiveness of risk management roles, responsibilities and processes at three levels:

- At business unit level;
- In an independent risk function; and
- Through internal audit.

Business units have the primary responsibility for managing risk on a day to day basis in line with the organisations risk appetite. Clearly defining business unit managers risk responsibilities within their business units allows companies to manage risk at the

operational level. If managers have a clear understanding of the overall risk framework and risk appetite, they are well placed to be given autonomy to make business unit level decisions in keeping with the organisation’s overall business objectives.

Independent risk functions help in implementing the organisations risk management policies – defining the standards, developing the processes and driving the awareness that is needed to help build a risk aware culture across the organisation. They also play a key role in coordinating and reporting on enterprise wide risk activities including the identification of interdependencies between areas of risk or across business units. This helps ensure that the board and senior management are provided with an enterprise wide view of risk.

Internal Audit provides independent assurance to the board and Audit Committee that the organisations risk management policy and processes are designed appropriately and operating effectively. The role can include reviewing the management of key risks and evaluating specified risk management processes including giving assurance around the identification, evaluation and reporting of risks. To support the business, Internal Audit should provide advice and challenge on managements decisions on risk, as opposed to making risk management decisions.

---

“IT’S IMPOSSIBLE TO ELIMINATE ALL RISK; IT’S UNHEALTHY EVEN TO TRY. YOUR LONG-TERM SUCCESS WILL DEPEND ON ENSURING THAT YOU TAKE THE MOST APPROPRIATE RISKS FOR YOUR BUSINESS.”

---

While establishing the appropriate risk governance structures is a key step, the structures themselves are only a foundation. They require the right investment in resources and management effort if they are to actually support effective risk management.

## 2. Getting the culture right

Effective risk governance starts at the top – with the board and senior management. If the highest levels of the organisation see benefits in managing risk, then they are likely to establish a positive risk culture. Establishing an effective risk culture involves:

- Setting the right tone at the top. If the board and senior management are seen to champion the purpose and goals of risk management, employees are more likely to engage in the risk-considered behaviours that support it. Organisations should look to recruit, retain and reward people who view risk management as a personal responsibility and as a core part of their job description.
- Defining business strategy and risk appetite. Risk governance starts at strategy-setting with the board and senior management developing clearly defined business objectives and risk appetite. Once the risk appetite is defined, managers have a risk measure against which they can make the business decisions that are within their remit. Too much risk endangers organisations, but too little prevents it from exploiting new opportunities to create value.
- Rewarding the right behaviours. Effective risk governance depends on an incentive structure that rewards the right, risk considered behaviour. A clear message emerging from the current crisis is that reward structures should recognise a focus on long-term value rather than short-term gain.

values and behaviours present that help shape risk decisions. No matter how clearly you define your risk appetite and controls, your people won't consistently make the 'right' decisions unless your culture reinforces the principle of 'doing the right thing'. But a strong risk culture is not something that is quickly developed or easily defined. Organisations with strong risk governance typically demonstrate the following:

- *Responsibility and Accountability.* Clearly defined roles and responsibilities that establish accountability for risk at all levels of the organisation.
- *Openness and Transparency.* Early identification of issues and the development of a timely response is common in a culture where employees are encouraged to admit mistakes and take responsibility without fear of repercussions. Our recent history suggests that this culture was not as common as we would like to think.
- *Risk Monitoring.* Continuous monitoring of risk throughout the enterprise identifies business opportunities and guards against emerging threats.
- *Uncertainty is accepted.* Rather than basing strategy around fixed assumptions, risk aware managers use scenario planning to factor possible alternatives into their decision making process.
- *Continuous Improvement.* A culture of consistently reviewing what went right and what went wrong after unexpected events is a best practice that is, at best, inconsistently applied in organisations.
- *Status.* Risk function management have a sufficiently senior status to ensure they have a strong voice at the management table.

Remember, people and organisations are creatures of habit, and changing habits is much harder than changing structures and systems.

## 3. Effective monitoring and reporting of risk

Is risk management reporting a regular part of your management reporting packs? Or is it a once a year exercise? In an effective risk governance model, the board and senior management have a clear understanding of the organisations full portfolio of risk and can consider these against the entities risk appetite. They also need to ensure that those risks are being responded to appropriately in order to mitigate threats and pursue opportunities. However, a challenge for many organisations is actually getting effective reports to senior management and the board. Risk reporting needs to be:

- Clear, timely, relevant, accurate and actionable;
- Focused on key risks;
- Appropriate for executive level – i.e. limiting content to help focus on actionable information;
- Supported by relevant data;
- Solution focused; and
- Balanced in presentation.

Effective reporting should provide the board and senior management with an integrated view of risk across the organisation and the actions and decisions required to mitigate the threats and take the opportunities that held deliver business objectives.

## CONCLUSION

It's impossible to eliminate all risk; it's unhealthy even to try. Your long-term success will depend on ensuring that you take the most appropriate risks for your business. Getting this balance right is crucial. In choosing your strategy, keep in mind the risks and uncertainties of each choice. But remember that risks aren't static; they have lifecycles and change as new options, competitors or circumstances emerge. Therefore your risk management responses can't be static either.

Sound risk management is key in all organisations and a pervasive organisational culture of risk governance should underpin effective risk management. No matter how diligent a risk management program, its effectiveness cannot rise above the values of the people who create, administer and monitor it. ■

---

Mike Sullivan, FCA is a partner in the PwC Risk Management

A company's risk culture is the system of