Reframing risk

As the major revision of one of the world's most influential pieces of guidance on risk turns one year old, what does COSO ERM mean to the profession?

BY MARK BUTTERWORTH

Risk managers are increasingly under the spotlight in regard to the structure they bring to risk management in their organisations, and the credibility of their approach. In using a well-established code or framework the risk function can give management and other stakeholders the assurance they are seeking that risk is addressed in a coherent, formalised way. One year after the publication of updated guidance from the Committee of the Sponsoring Organizations of the Treadway Commission (COSO), *Enterprise risk management – integrating with strategy and performance*, analysis can be undertaken of the value that this framework adds.

The previous 2004 guidance had a long and successful "shelf life", majoring on a three-dimensional "cube" that blends eight features of risk management (for example, event identification, risk assessment and controls) with key objectives and looks at these from the entity level, division and subsidiary perspectives. The emphasis on the integrated framework has now evolved to become a management tool that addresses the critical issues of strategy and performance – seeking to enhance the chances of success and resilience in the face of increasing complexity in the risk universe.

> **By taking an 'audit' of the organisation's actual compliance with each of the COSO principles, a picture can be formed of the strengths and weaknesses of the current risk management approach**

> By demonstrating how risk management forms part of good governance and direction, the risk function sits firmly at the forefront of organisational management

New, helpful features

Other than for expert users, applying the COSO cube could be a daunting experience and lead to confusion and lack of focus for many risk managers and their organisations. There is no doubt that taking an enterprise-wide approach to addressing risk makes sense, and the 2004 guidance set many risk managers along this righteous path. The 2017 revised framework has an easy-to-follow and logical structure of five interrelated components – and each has explanatory principles, twenty in total.

The components make sense if your aim is to blend risk management seamlessly into strategy design and selection and performance monitoring. The COSO "double helix" as shown below weaves together the framework's components, ultimately flowing through to producing enhanced value for the organisation.

The list of 20 principles can be used by risk managers as a checklist of risk management maturity – indeed Principle 17 ("*pursues improvement in enterprise risk management*") is itself a call to develop further the organisation's risk management capabilities. By taking an "audit" of the organisation's actual compliance with each of the principles, a picture can be formed of the strengths and weaknesses of the current approach. A number of the principles may be partly addressed, and so I recommend that a scoring system is applied (red, amber, green, for example) from which priorities for action can be developed. The action plan, required resources and time frames should be agreed with senior management.

Culture

The importance of active culture management is gaining greater traction, not least following the publication by the Institute of Risk Management of its thought leadership guide: *Risk culture – resources for practitioners*. In COSO 2017 the principles require organisations to embed culture management within their governance practices. This is achieved by linking board risk oversight and support of executive management with commitment to core values and is manifested by defining and monitoring the behaviours that characterise the desired culture.

But measuring progress on risk culture management is not easy. Risk managers should spend time with colleagues to define the appropriate culture metrics, which indicate

ENTERPRISE RISK MANAGEMENT

Governance and culture
Governance sets the organisation's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviours, and understanding of risk in the entity.

Strategy and objective-setting
Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.

Performance
Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritised by severity in the context of risk appetite. The organisation then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.

Review and revision
By reviewing entity performance, an organisation can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.

Information, communication, and reporting
Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organisation.

> **COSO proposes that enterprise risk management needs to employ techniques such as visualisation of potential outcomes that detailed data modelling can give to organisations**

improvements in risk awareness, positive behaviours and risk management coherence. While some existing performance data will be helpful in judging the culture, such as employee absence rates, customer complaints and product quality, risk managers should expand the metrics to include culture monitors such as an analysis of employee satisfaction surveys, sign-up numbers for training programmes, media commentary analysis – positive and negative, employee involvement in corporate initiatives such as charitable time-giving, disciplinary factors and timeliness in risk and event reporting.

Analyses of reasons why firms fail often cite poor culture as a key factor. Setting a plausible strategy and monitoring performance could be undermined if culture metrics are inappropriate or even ignored.

Challenges

As with all aspects of risk management, gaining tangible senior management buy-in is crucial. Nothing new there, so how is the COSO framework going to help risk executives achieve the partnership approach to risk? Certainly a thorough and effective communication (and if necessary, training) programme is required as a platform for shared knowledge, but COSO really requires a redefinition of the risk function.

Given the emphasis on strategy and performance in the framework, the risk executives need to be involved in the essential initial phase – strategy setting, or what COSO calls strategy selection. This is not easy – conceptualising and developing strategy is often held close to the chests of the main board or senior managers. The challenge for risk managers is to show how effective risk analysis can lead to better decision making. Assisting senior executives with scenario analyses and modelling of potential outcomes to the strategic options that the board are considering gives much greater assurance that the selected strategy is achievable, with acceptable potential downside.

The COSO focus is on getting the best from upside risk. Certainly good risk management practices identify and address the negative aspects of risk, but real organisational value comes from a mindset of gaining a thorough understanding of the risks associated with the selected strategy. Risk managers will seek to reduce volatility in outcomes by moderating the effects of risks that do occur.

Many commentators observe that risk managers' influence at board level should be developed further. The focus of COSO 2017 on strategy and performance gives clear positioning of risk management in regard to the essential focus of the board, that of building a sustainable, resilient strategy and proactively measuring performance. Directors have an inherent interest in understanding the status of risks that could influence performance and how well these risks are being controlled. By demonstrating how risk management forms part of good governance and direction, the risk function sits firmly at the forefront of organisational management. COSO adds that going forward, intelligent use of the framework will bring identifiable financial benefits that more than offset the cost of risk management activities, again affirming the enhancement of value by the risk function.

International relevance

While COSO is strongly US oriented, it is equally relevant to all types of organisations, across all geographies. It is also a practical framework for uniting risk management approaches throughout a divisionalised organisation. Indeed, the COSO publication

COMPONENTS AND PRINCIPLES

1. **Exercises board risk oversight** – The board of directors provides oversight of the strategy and carries out governance responsibilities to support management in achieving strategy and business objectives.
2. **Establishes operating structures** – The organisation establishes operating structures in the pursuit of strategy and business objectives.
3. **Defines desired culture** – The organisation defines the desired behaviors that characterise the entity's desired culture.
4. **Demonstrates commitment to core values** – The organisation demonstrates a commitment to the entity's core values.
5. **Attracts, develops, and retains capable individuals** – The organisation is committed to building human capital in alignment with the strategy and business objectives.
6. **Analyses business context** – The organisation considers potential effects of business context on risk profile.
7. **Defines risk appetite** – The organisation defines risk appetite in the context of creating, preserving, and realising value.
8. **Evaluates alternative strategies** – The organisation evaluates alternative strategies and potential impact on risk profile.
9. **Formulates business objectives** – The organisation considers risk while establishing the business objectives at various levels that align and support strategy.
10. **Identifies risk** – The organisation identifies risk that impacts the performance of strategy and business objectives.
11. **Assesses severity of risk** – The organisation assesses the severity of risk.
12. **Prioritises risks** – The organisation prioritises risks as a basis for selecting responses to risks.
13. **Implements risk responses** – The organisation identifies and selects risk responses.
14. **Develops portfolio view** – The organisation develops and evaluates a portfolio view of risk.
15. **Assesses substantial change** – The organisation identifies and assesses changes that may substantially affect strategy and business objectives.
16. **Reviews risk and performance** – The organisation reviews entity performance and considers risk.
17. **Pursues improvement in enterprise risk management** – The organisation pursues improvement of enterprise risk management.
18. **Leverages information systems** – The organisation leverages the entity's information and technology systems to support enterprise risk management.
19. **Communicates risk information** – The organisation uses communication channels to support enterprise risk management.
20. **Reports on risk, culture, and performance** – The organisation reports on risk, culture, and performance at multiple levels and across the entity.

Source: *Enterprise risk management – integrating with strategy and performance, COSO, June 2017*

> It is essential that the risk function agrees the nature of reporting with senior management so that causes of diversion from the strategy, mission, vision and values can be acted upon without delay

cites entity-wide identification and management of risk as a key benefit of applying the framework. This of course requires a risk policy that adopts a hybrid approach consisting of a single centralised reporting framework, applied in a flexible and dynamic fashion within divisions and subsidiaries.

Many organisations adopt elements of the IRM risk management framework or the ISO31000 risk management guidelines, so what does COSO add? The answer lies in the positioning of the COSO approach firmly in the strategy space, aligning the selected strategy with the organisation's mission, vision and core values. Risk managers would benefit from adopting the strategic concepts in COSO, with operational aspects of risk management based on or derived from the IRM or ISO31000 processes. It's about selecting the most beneficial aspects of these frameworks and using the terminology and processes effectively.

Risk reporting

One of the constant challenges to the risk function is managing the flow of information from operational teams through to decision makers. Assessment of the implications of the chosen strategy, ie monitoring the known and emerging risks, is a key management tool. Thought should be given to the nature and timing of reporting – linked to the perceived volatility of the relevant risks. For example, for a holiday tour firm, the status of security in the countries visited would be assessed on a daily basis, whereas staff turnover statistics may be subject to monthly reporting. The importance of timely risk information cannot be over-stressed – management response relies on a dynamic reporting regime.

COSO 2017 notes that "*the most significant causes of value destruction are embedded in the possibility of the strategy not supporting the entity's mission and vision, and the implications from the strategy*". It is therefore essential that the risk function agrees the nature of reporting with senior management so that causes of diversion from the strategy, mission, vision and values can be acted upon without delay.

Forward looking

The updated COSO framework has been around a year, and during that time we have seen widespread discussion on the benefits, and dangers, of data analytics. COSO proposes that enterprise risk management needs to employ techniques such as visualisation of potential outcomes that detailed data modelling can give to organisations. Further, COSO emphasises the benefits of leveraging artificial intelligence in identifying previously unrecognised relationships. Modelling the relationships and risks such as in the supply chain will provide increased resilience to interruptions.

For many risk managers this advancement in their role could represent a skill they don't have. Recruitment into risk teams could in the future focus much more on analytics and modelling proficiency.

Enterprise risk management will need to be agile and adaptable to be able to reflect the changing risk environment. If the strategy for an organisation is dynamic, responding to the fast pace of change, then risk management must be fully integrated with this process and inform the decisions driving the strategy.

Mark Butterworth is managing director at the governance and risk consultancy Condie http://condierisk.co.uk