In the fra

The next level for dealing with internal control, or an overblown distraction? Neil Baker looks at COSO's new enterprise risk management framework

ORGANISATIONS ARE adopting Enterprise-wide Risk Management (ERM) at great speed. In a recent Institute survey, 60% of companies and 64% of public sector organisations said they had adopted an ERM approach to risk and control. Three quarters of them had done so within the last two years. Many of those that had not adopted ERM planned to soon.

The drive to ERM will gain impetus from the recent publication of *Enterprise Risk Management – Integrated Framework*. This is a long-awaited "roadmap" to ERM from an umbrella group of professional bodies known as COSO (The Committee of Sponsoring Organisations of the Treadway Commission).

COSO says its framework describes the essential components, principles and concepts of ERM for all organisations, regardless of size. It identifies all the aspects that should be present in an organisation's risk management framework and provides advice on how they can be successfully implemented.

The framework "could not be completed at a more appropriate time," says COSO chairman John Flaherty.

COSO was working on its framework before Enron and other financial scandals rocked confidence in corporate management, he says, and it is not a response to those events. But "calls for enhanced corporate governance and risk management, new law, regulation and listing standards" that came in the aftermath made the need for an ERM framework "even more compelling," he says.

The laws Flaherty refers to are largely the US Sarbanes-Oxley Act 2002 – the main legislative response to Enron and other corporate scandals. Sarbanes-Oxley is driving companies to change the ways they deal with internal controls. In doing so, most are turning to an earlier COSO publication – *Internal Control – Integrated Framework* – for guidance.

Next level

The ERM framework builds on the earlier control framework. "Companies that want to move beyond internal control and get more out of their efforts, now have a framework that will help them go to the next level," says COSO.

"While the framework might provide a common language that people in the risk business understand, is it a tongue that boards speak – or jargon?"

The ERM framework includes the concepts and components initially developed in the internal control framework, so "expanding practices to incorporate risk management will be more evolutionary and not require [companies to] 'throw away' all ➲

me?

of the previous efforts."

According to COSO, internal auditors operating within the framework can assist management and the audit committee by "examining, evaluating, reporting, and recommending improvements on the adequacy and effectiveness of management's risk management processes." The ERM framework "provides a benchmark for internal auditors to use in the evaluation of their organisation's risk management efforts."

Value

ERM is not just about regulatory compliance. COSO says its framework "speaks to many of the issues currently facing organisations," such as how they decide what level of risk to take in their operations, what rewards they should seek in return, and how best to protect the value of the organisation.

The COSO framework argues that an organisation maximises value when management gets the optimal balance between goals aimed at growth and returns and risk, and deploys its resources in the best way to achieve those goals.

According to COSO, ERM helps organisations to: align the risks they are willing to take with their strategic goals; make better decisions about how to respond to risks; reduce "surprises" and consequent losses; identify risks that run across the organisation; seize opportunities; and allocate capital more effectively. In sum, it will "help an entity get where it wants to go and avoid pitfalls and surprises along the way."

Importance

The COSO framework is important because "so many companies deal with risk ad hoc," says Richard Steinberg, a US risk management expert and founder of Steinberg Governance Advisors. "They have long focused on specific risks, often centred on insurable risks and risks inherent in derivatives and other sophisticated financial transactions. But as organisations look at risk more broadly, a framework is needed to help provide the necessary discipline for broad-based risk identification, assessment and management."

"Another important reason is to enable personnel within an organisation, and indeed externally as well, to talk the same language. All too often we've seen two people using the term 'risk' to mean entirely different things, believing they're communicating well when in fact they're misunderstanding one another entirely. A common framework will help deal with this problem."

Miles Everson, a partner at PricewaterhouseCoopers and one of the authors of the COSO ERM framework, says in moving to ERM organisations change the way they think about risks. "ERM integrates risk management and entity performance management," he says, "which in turn improves an organisation's ability to know what risks it is taking and to be properly paid for the risks it chooses to take."

Both Everson and Steinberg stress the point that the COSO framework encourages organisations to think about risk *and* opportunity at the same time. "Importantly, managements are already recognising that the COSO framework helps them identify the upside of risk – opportunities that can be seized to further enhance profitability," says Steinberg.

Appeal

Asked to explain the appeal of ERM, Steinberg says: "Many company managements have been surprised by unseen events too often in the past. They realise that their organisations, from strategic planning level to business process implementation, are susceptible to a wide range of exposures. They want a more proactive way of dealing with an uncertain future on many levels."

"Also, boards of directors are focusing now more than ever on their oversight responsibilities. They are concerned about the long-term future of their companies, as well as their own personal reputations and liability issues. They want to be sure management knows what lurks around the corner and has plans in place to deal with exposures."

Bob McDonald, director of internal audit in the Australian government's Department of National Resources and Mines, offers another explanation for ERM's appeal. "This is a direct result of the corporate failures of the past few years," he says. "Many of the issues that came to fruition could have been identified as potential risks and appropriate controls or mitigation plans put in place."

"There is also a greater recognition that risk management is essential, because the biggest risk to an organisation is the ignorance of potential risks," he adds.

The "enterprise" element of ERM is also important, says McDonald – it points to an effort to get everyone in an organisation thinking about risks in the same way. "Many organisations have had parts of the company undertaking good work in risk management, while other parts have not worried about it," he says. "Of course, there are no prizes for predicting which part of the company is most likely to fall over."

"All too often we've seen two people using the term 'risk' to mean different things, believing they're communicating well when in fact they're misunderstanding one another entirely"

Overblown?

The COSO framework is not the only recognised approach to ERM. Indeed, when it was published in draft last year, critics said it was too prescriptive and too big – running to 154 pages. By contrast, the *Risk Management* standard published by Standards Australia runs to just 23 pages. This standard, which is widely used internationally in ERM programmes, is often praised for its simplicity and principles-based approach.

The Australian standard – which has just been revised – is "a model of clarity," says US risk management commentator Felix Kloman. "It is brief, complete and refreshingly well written. It

remains the gold standard for all others, worldwide."

Everson defends the size and detail of the COSO document. "It is comprehensive and logically sound," he says. "Simply listing a few principles without providing context of how those principles interact would not have accomplished COSO's goal of having a framework that could be used by many and stand the test of time."

He adds that the Australian standard addresses principles of risk management, "but does not address the relationship between entity performance management and ERM, nor does it explicitly address the relationship between ERM and internal control." Also, the final version of COSO has been redrafted and the number of pages reduced by about a third.

"Many of us would like important information in sound bites, so we can quickly grasp critical concepts and move on," says Steinberg. "Well, we can take from the COSO framework what we want. A quick read of the executive summary and first chapter provides a good overview. But for those who want a deeper knowledge of what ERM is all about, and how to be sure it truly adds value in their organisation, they can look further into the framework. And for those more fully involved in ERM implementation, a second volume on application techniques provides that additional guidance."

Implementation challenges

What challenges might internal auditors face if their organisations decide to adopt the COSO Enterprise Risk Management Framework? In an article for the October 2003 edition of *Internal Auditing & Business Risk* ("Putting COSO into practice") Sam Samaratunga of PricewaterhouseCoopers identified some key issues:

- **Skills.** This is a particular challenge for small and medium-sized audit functions, which may lack the depth of skills base needed to assess a risk management framework covering all risks across the organisation. As organisations move along the risk continuum, internal audit will face changes to its resourcing requirements, its skills profile and the effort required to evolve in parallel with the risk management capability.
- **Training and development.** A shortage of necessary skills raises the problem of how and where to source and develop those capabilities in a cost-effective way.
- **Knowledge management.** Once the necessary skills are acquired, it is critical that they are developed, retained and shared on an ongoing basis. In a large organisation, the internal audit function may have its own knowledge managers and training personnel, but such luxuries are beyond the reach of smaller functions. Also, irrespective of size, internal audit may struggle to attract and retain people of sufficient quality and knowledge to assess whether the risk management framework is working properly, and to talk on equal terms to operational and risk management experts across the business.
- **Communication.** Communication between risk management and internal audit needs to be effective in order to ensure alignment of their goals. For those organisations where compliance is an issue, the compliance function should also be involved in design and implementation of ERM processes. Internal audit needs to bring its own perception of risk to the party. Risks identified in its work need to find their way into the risk management process through feedback loops. Internal audit needs to promote awareness of ERM with its key stakeholders, including the audit committee, which needs to be comfortable with its approach and how it supports the overall governance structure.
- **Consistent terminology.** Effective communication requires consistent terminology. Inconsistencies lead to confusion and undermine the synergies to be achieved in aligning the risk-based internal audit approach with the ERM framework.

Skimping

There are also concerns that a high-level focus on risk at the enterprise-wide level can cause organisations to skimp on the details.

"It would be possible to take something like COSO and focus a lot of time at a very senior level getting people to understand that this is a framework, and perhaps lose sight of the lower-level activities," says Colin Cray, a senior manager in Ernst & Young's business risk services group. "That's where you need to rely on functions like internal audit to remember what is core to internal control within the organisation."

"The downside of ERM is the definite potential for gaps. It's essential to have training, documentation, registers and a coordinator or chief risk officer"

"The downside of ERM is the definite potential for gaps," says McDonald. "That's why it's essential to have training, documentation, registers and a coordinator or chief risk officer."

"It comes back to setting the right context – what are the risks being assessed? I see opportunities to break risk up into a number of areas. The board and chief executive, for example, should be undertaking a strategic risk assessment for the organisation to meet its goals and objectives. Business area managers should be undertaking a business risk assessment on the business risks in meeting the strategic plan. The rest of the organisation should then concentrate on the operational risks."

"Assessment can be ➲

➲ further broken into specific elements: environmental, workplace health and safety, the 'old' accounting cycles (accounts receivable, accounts payable etc.), functional (production, warehousing, delivery, marketing etc) and should include a specific focus on issues such as fraud and corruption."

"Companies that want to move beyond internal control and get more out of their efforts, now have a framework that will help them go to the next level"

"It's important to set the context and ensure then that the 'enterprise' is covered in the ongoing process."

Enthusiasm

Many in the risk management industry are clearly convinced of the benefits of ERM and the COSO framework. But will senior executives and audit committees – already up to their necks in new financial laws and best practice advice – see it as just another distraction? And while the framework might provide a common language that people in the risk business understand, is it a tongue that boards speak – or jargon?

"You need to keep frameworks in their proper place," says Cray. "If you start drifting away from the language that the business is comfortable with using, then you start to lessen the impact of the message."

"Organisations tend to have come unstuck on ERM when they have turned it into a cottage industry and have detached it some how from the way in which the organisation operates," he adds.

Supporters of the COSO framework say it is important for that very reason – it makes thinking about risk part of what everyone does.

But London School of Economics professor Michael Power has argued recently that "We live in the age of the risk management of everything." In a pamphlet for the Demos think tank, Power said that the rise of risk management since the mid-1990s reflected a misplaced ambition by organisations to control all threats to their future operations.

He has cautioned against a "faddish risk description of everything" and called instead for an "intelligent" approach to risk management. This, he says, is one which "would not allow control systems, and their advocates, to swamp managerial attention and independent critical imagination." Such concerns do not seem to have dampened the enthusiasm for ERM. Anyone looking for an Intelligent Risk Management framework may have to wait a while yet.

For information about the COSO publication *Enterprise Risk Management – Integrated Framework*: www.coso.org. For information about Standards Australia's *Risk Management* standard: www.standards.com.au