



## COSO ERM & Implications for Internal Auditors .

Corporate Governance and Sarbanes-Oxley Hub Bulletins ,  
Volume 7 , № 6 , July 2005

[auditteam.org](http://auditteam.org)

# COSO ERM & Implications for Internal Auditors

## Introduction

The COSO draft risk management framework aims to provide organisations with a benchmark against which they can gauge their own risk management practises. As such, it joins a number of other risk management standards such as the AS/NZS 4360 1999 Risk Management standard and the UK AIRMI/ALARM/IRM 2002 risk management standard.

COSO, however, examines the subject in much more detail and arguably represents a document describing good management practices as well as good risk management practises. It is almost a framework for organising a business describing how the process of risk management permeates throughout the entity and the entity's objectives. The three components are inextricably linked and the words in the standard reinforce what many internal auditors already know: the key to good risk management is management.



The role and responsibilities of internal auditors, risk officers, the Board, management and the rest of the organisation are laid out in a somewhat prescriptive fashion towards the end of the standard.

There appears to be a tacit assumption that a one size fits all approach may be adopted when it comes to roles and responsibilities. Commercial reality and the efficient use of resources are likely to dictate otherwise and certainly based on my own experience, no two businesses organise their approach and responsibilities vis-à-vis enterprise risk management in exactly the same way.



## The Pointers of Standards and Auditors

But what does the standard mean for internal auditors? What are the key points that internal auditors need to consider as part of their approach to reviewing the processes that enable management to manage their enterprise risks and providing assurance to management that what they are doing is facilitating rather than hindering risk management?

Here are some pointers:

1. **Risk is a double-edge sword** – the framework recognises that risks not only have to be managed to protect the business but they have to be taken to grow the business. Opportunity management is something which the internal auditor will have to be aware of as part of the review of the risk management process and, in particular, how the strategic planning process links into the opportunities emerging from the process. Management in essence must be optimising risk and not necessarily minimising it.
2. **Embedding the risk management framework** – the standard describes the main activities of the risk management process and illustrates how the process must be embedded both at the strategic level and the business unit/operational/process level if it is to be truly embedded and “enterprise wide”. Internal auditors have to respond to this by providing assurance to management that the policies, procedures and processes developed to manage risk are being used across the whole organisation in a consistent and meaningful way.
3. **Aggregating risk exposures** – the interrelationship of risks is pointed out as being a key role for management and the internal auditor should in his review of a particular department or business unit consider this interrelationship. This will mean, inter alia, ensuring that the aggregate risk exposure at the entity level does not exceed the risk tolerance of the organisation. For example the loss of key staff in a sales function can impact upon many support functions and this interrelationship needs to be fully understood in order that appropriate mitigating action can be taken.
4. **Risk reporting and communication** – information about risks is the basis for communication and the organisation must have adequate reporting in place if the true risk profile is to be monitored and, therefore, managed. As part of their routine audit work, internal auditors will need to ensure that risk management reporting is sufficient, regular and adequate, in the sense that it reports on the key risk areas that affect the organisation. Furthermore, the internal auditor must ensure that management take appropriate action on the reports in order that risk is being effectively managed.

5. **Risk management process** – the standard describes in detail the eight steps of the risk management process beginning with creation of the right internal environment, in which a climate of risk awareness is built, through to monitoring, which ensures that the process itself is working satisfactorily. In reviewing the effectiveness of the risk management process and providing guidance to management about how to develop and enhance the process and achieve best practice, internal auditors can use the framework almost as a checklist to establish which components are missing and which are not working satisfactorily.
6. **Creating the right risk culture** – risk culture is described as a set of shared attitudes, values and practices that characterise how an entity considers risk in its day-to-day activities. Risk culture is one aspect of overall organisational culture and is arguably the key to achieving enterprise risk management throughout the organisation. However, the declared and desired common values of a risk culture may differ widely from the taken-for-granted assumptions of the workplace culture and the way that things happen in practice. Management will need assurance, particularly where there are highly decentralised operations, that the espoused values of the risk culture match with the reality on the ground. Internal auditors with their widespread knowledge of the organisation are in an excellent position to provide this assurance.
7. **Learning from risk events** – the development of risk event/near miss databases is seen as a useful tool for learning lessons. No more so than when events are captured that occur outside the organisation thus enabling management to stress test their own processes to see if they would prevent the event occurring internally. Risk events provide an excellent source of reference for the internal auditor and the way that they are captured, both internally and externally, analysed, and reported should be reviewed by internal audit on a regular basis.
8. **Risk fatigue** – the standard correctly points out that the whole process is people dependent – “enterprise risk management is accomplished by the people of the organisation, by what they do and what they say”. If people are to fulfil this role, they will need to be educated about risk management and how it benefits them and their organisation. This education process must hone the risk management skills of the people and ensure that, over a period of time, risk fatigue does not begin to set in. Maintaining a heightened sense of risk awareness is, however, easier said than done and there is no doubt that internal auditors can play a part both in the education process, as they undertake their audit work, and monitoring risk fatigue in the departments they review.

9. **Reviewing the risk management unit** – where such a unit exists then management will need positive assurance that they are structured correctly with the right people as well as performing their work in a professional manner. The audit of the risk management function is part of the internal auditors remit and the standard makes it clear that internal auditors would be expected to undertake a review of this type when such a unit exists.



## Conclusions

The COSO framework discusses the control activities as being an important element in the risk management framework.

Internal auditors are the experts in internal control and the adoption of this standard by organisations and the opportunities it offers to Internal Audit departments to become an integral part of the framework, illustrates even more the added value that they can bring to the organisation.

#### References :

1. Enterprise Risk Management Framework, COSO Draft Executive Summary, p. 11-32 , September 2004
2. Keith Blacker, Dr, IIA Council member, COSO Draft Enterprise Risk Management Framework , Implications for Internal Auditors , 2005



To view or purchase the COSO ERM Framework auditteam's products and solutions visit the website [www. auditteam.org](http://www.auditteam.org).



Corporate Governance and Sarbanes-Oxley Hub Bulletins ,  
Volume 7 , № 6 , July 2005  
[auditteam.org](http://auditteam.org)

If you would like us to deliver the products & solutions or to view our other publications , please visit our website at [www.auditteam.org](http://www.auditteam.org)

For more information on the topics discussed in this issue, contact **Nickolay Nickolov** at (02) 920-01-48 .