COSO framework overview

Most internal auditors have heard the word 'COSO', some will hopefully be familiar with the internal controls cube and the enterprise risk management cube that followed....In 2017 there was a major update to the risk cube.

This piece will not only bring you up to speed on the latest COSO thinking regarding enterprise risk management (ERM) but provide an overview of COSO; maybe answering some of those questions that you don't want to ask as audit leaders.

Who or what is COSO?

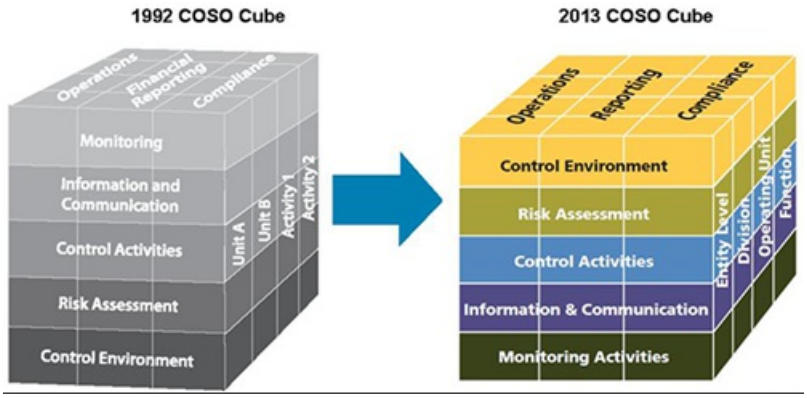
COSO (Committee of Sponsoring Organizations of the Treadway Commission) began in 1985 as an independent private sector fraud initiative in the United States comprising of five organisations, including IIA Global. They provide thought leadership through the development of frameworks and guidance on enterprise risk management, internal control and fraud deterrence.

Richard Chambers, president and CEO of IIA Global sits on the COSO board.

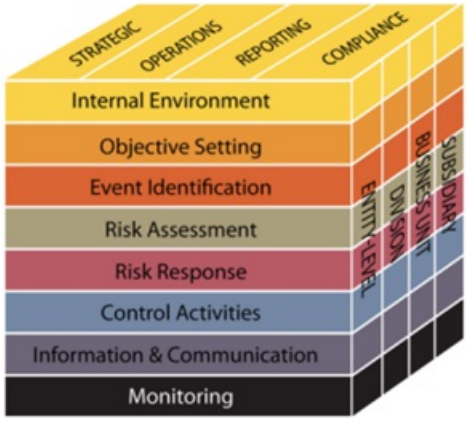
Is COSO about internal controls or risk management?

It is both. There are two frameworks.

Originally focused on internal control, the well-known COSO Cube was first published in 1992. The Internal Control – Integrated Framework was revised in 2013. All COSO internal control activity links to objectives in three areas; Operations, Reporting and Compliance. The framework sets out seventeen principles across its five component areas; these are the foundations for the provision of comprehensive internal controls assurance. Audit leaders unfamiliar with this may find it useful to read the detail and consider the completeness of their current controls assurance activities.



In 2004, COSO published a version of the cube for Enterprise Risk Management (ERM). It expanded on the risk assessment component of the internal controls framework, to include event identification and risk response. It also introduced the objective area of strategy recognising the importance of risk on the board agenda.



Several thought papers have been produced relating to ERM which COSO build on in the 2017 ERM update.

Some internal auditors may be wondering what the difference is between ERM and risk management?

Imagine ERM as a toolbox from which a variety of specialist tools can be selected depending on the job in hand. ERM is holistic, considering culture, strategy and value. It is comparable to the Governance, Risk and Compliance (GRC) concept that is more familiar to internal audit. Risk management refers more to the method of identifying, assessing and responding to risks.

Although in the pursuit of simplicity and business integrations, the 'E' of ERM is omitted and most risk practitioners think of risk management as the whole not an isolated, disconnected activity.

2017 Enterprise Risk Management update

COSO identified a need for an improved approach to managing risk. The environment in which organisations operate has changed considerably in the last decade in every respect from digitalisation and technological advances to environmental expectations and increased consumer activism.

The new framework Enterprise Risk Management — Integrating with Strategy and Performance, integrates risk into the business model, highlighting its importance in strategy-setting and driving performance.

Main changes

The most striking change is COSO's move away from their famous cube model.

The new graphic illustrates the linkage between risk, strategy and performance. Its shape is the same as the structure of DNA. Just as DNA holds the information for organic life, ERM holds the information for organisational success.

The graphic integrates risk into the traditional business model unlike the original cube which had the unintended consequence of creating a disassociated risk process; a key learning for COSO.

This new focus on integration will help organisations to:

- Identify risks more explicitly
- Increase options for managing risks through earlier identification/anticipation
- Pursue opportunities with confidence
- React quickly and consistently to deviations in performance
- Report on a broader portfolio of risk
- Improve collaboration, trust and information sharing

It is business focused in style, with revised language to help make risk conversations relevant at all levels within the organisation; enabling effective management of risk from the strategic through to transactional.

The new framework continues to adopt a components and principles structure with each of the five components underpinned with a series of principles.

Governance and culture are placed to the fore in the new framework. This emphasis will be familiar to internal auditors as culture is a pivotal factor in decision-making and the day-to-day activities of an organisation. This positioning supports the requirements of the UK Corporate Governance Code. Practitioners are encouraged to link culture behaviour to risk along a traditional risk spectrum. The framework explores the possible effects of culture on decision making and explores the alignment of culture between individual and organisational behaviour; this pairs well with the Institutes research.

Strategy has always been important in the ERM model and it is now given prominence and an additional model. It now requires consideration to be given to risks ***to*** the strategy and risks ***of*** the strategy in addition to implications ***from*** the strategy. This comprehensive view gets to the heart of organisations and has the potential to add real value to organisations.

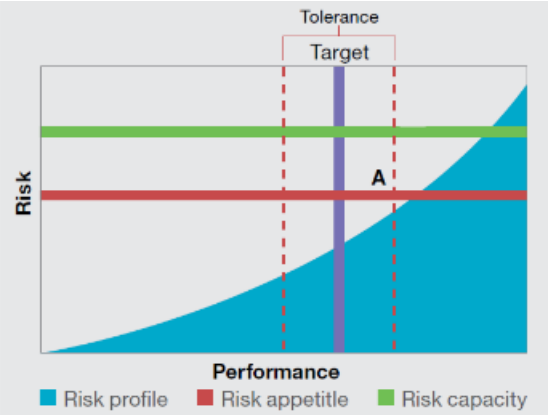
Performance and with it stakeholder value is a key theme. A new, simplified definition of enterprise risk management has been introduced, accentuating the relationship between risk and value.

The culture, capabilities and practices integrated with strategy-setting and its execution that organisations rely on to manage risk in creating, preserving and realising value.

Value is emphasised throughout the framework from its creation, preservation and realisation. It is:

- prominent in the new definition of ERM,
- embedded in the principles,
- linked to risk appetite and the management of risk to acceptable levels.

COSO has also introduced a new risk profile diagram incorporating risk, performance, appetite and capacity. It aims to promote more risk-aware decision making.



A new phrase 'acceptable variation in performance' has been introduced to interchange with 'risk tolerance'; one of the attempts to simplify the complexity of risk appetite to make it a more useful concept for non-risk professionals.

An important component for internal audit is review and revision. COSO acknowledges the speed of change and development within organisations and the need for risk to maintain pace and adapt; not only risk identification and assessment but the process and functions that support risk. This links directly with the remit of audit leaders to provide assurance over risk management activity within their organisations.

Technology has advanced considerably since 2004 and the framework now incorporates thinking on issues such as big data, artificial intelligence, automation and digitalisation; its influence on strategy, performance and risk management. Communication and reporting of risk and associated themes have been up-weighted and linked to decision-making and oversight accountabilities.

What does this mean for audit leaders?

COSO have focused on culture, strategy and performance as underpinning good risk management. This synchronises with the thought leadership from the Institute for internal audit; culture and strategy must be common features on the audit plan accepting that they might be challenging areas to access, evaluate and effect change in.

The attention placed within the ERM framework on risk awareness in decision making is an important aspect for internal audit. A visit to the doctor will invariably confirm
that prevention is better than a cure and the same applies to the management of risk; informed decision making enables controls to be designed into systems rather than added at a later date. The COSO diagram opposite shows a variety of elements within the risk profile linked to decision making, all are potential areas of internal audit input and assurance.

Internal audit and risk professionals often co-operate and work together, sometimes within the same function. The challenges of this are well recognised and a variety of core and legitimate roles within the realm of risk management as defined by the Institute in the fan diagram shown below.

When evaluating risk management and providing assurance, internal auditors need to be aware that there is no single framework mandated for organisations to use. It is unregulated. Consideration should be given to

the needs of the organisation and the sector within which it operates to determine the best approach.

The UK Corporate Governance Code requires that boards should maintain sound risk management systems; as with COSO the Code is principle based with no prescribed approach on how it is best achieved.

For organisations that have ISO accreditations in operational areas, there may be synergy and board appreciation of following the ISO risk standard, for public sector organisations there may be a preference for the OCEG framework, whilst the generalist IRM risk standard may resonate with others.

Audit leaders with accountability for both internal audit and risk teams will need to reflect on the new COSO framework for improvements to the current risk management approach.

The ERM frameworks are complementary to the 2013 internal controls cube. Ideally they are designed to work together or can be used independently of each other.

Questions audit leaders may wish to think about

- Is the board appropriately skilled in risk to perform their oversight duties?
- What is the risk culture of your organisation – averse, neutral, aggressive?
- How does this culture/tone from the top impact day-to-day activities?
- Is risk communication open and transparent?
- Do performance incentives and targets drive appropriate risk behaviour?
- How well is risk identified and assessed during strategy setting processes?
- Is risk appetite understood, defined, communicated and monitored effectively?
- Could enhancements be made in identifying and assessing non-strategic risks?
- Are risk appropriately prioritised?
- How robust is the monitoring of activities to manage key risks
- In what ways could the reporting of risk be improved?
- Is the risk team sufficiently resourced to support the organisation?
- What near misses in terms of risk should be learnt from to address weaknesses?
- How integrated is formal risk management at the moment?

Closing Thoughts

The marketplace within which organisations operate, whether commercial, charitable or public sector is an increasingly volatile, uncertain and complex arena. COSO has called on leaders to be more adaptive to change through enhanced risk management processes; integrating risk with strategy and performance. Internal audit has an important role to play in this. As one of the three elements within its remit of governance, risk management and internal control, staying abreast of developments is essential to delivering valued assurance and consultancy advice.

"Continuous improvement is better than delayed perfection"

Mark Twain