**Paradigm paralysis in ERM & internal audit**

Boards and CEOs around the world are being told repeatedly from multiple sources that they need to do a better job managing and overseeing risk, and, most recently, ‘risk culture’. Unfortunately, current methods of providing stakeholders with assurance that risk management processes are effective are not working to the satisfaction of management and boards.

The internal audit profession needs to reinvent itself to better respond to the emerging expectations facing senior management and boards.

ERM paradigm flaws

The primary drawback of this risk-centric ERM paradigm is that it looks at risks in isolation from the company’s top value creation and value preservation objectives (see the sidebar for the authors’ definition). This approach does not allow decision makers to see the current state of residual risk linked to the achievement of the company’s most important objectives. All of the risks relevant to individual objectives are not looked at in totality in terms of their collective effect on the achievement of specific objectives. The process does not produce information to evaluate the acceptability of the current residual risk status (i.e. is it within risk appetite/ tolerance?). It also creates confusion and uncertainty around who is really responsible for the risks identified, as assigned ‘risk owners’ may not align with those responsible for achieving the linked objective(s).

This risk-centric approach has also tended to focus more on value preservation objectives (e.g. ‘three lines of defence’ rather than a balance, which puts at least equal emphasis on value creation/strategic objectives.

**VALUE CREATION OBJECTIVE**

Objectives key to the long-term success of the enterprise that will create enhanced shareholder value (e.g. increase market share by 20% per year).

**VALUE PRESERVATION OBJECTIVE**

Objectives that, if not achieved, have significant potential to erode stakeholder value (e.g. ensure reliable financial statements).

Another flaw is that the process is typically completed as a static annual or semi-annual exercise with a heavy compliance connotation. The risk assessment matrix used to populate the risk register and risk heat maps is often not the same assessment approach used by internal audit to complete internal audits, or the assessment approach used by other specialists, groups, such as safety, compliance, insurance, quality, etc. It is also important to note that the dominant ERM method is fundamentally about hazard avoidance and defence – not a key support tool to take risks and disclose risks and residual risk status.

Another significant concern is that the areas that are generally low risk from a culture and decision making and a healthy risk culture. Another significant concern is that areas of the enterprise that will create enhanced shareholder value (e.g. ensure reliable financial reporting and IT security). Those schools that do cover risk management fundamentally about hazard avoidance and defence – not a key support tool to take risks intelligently and drive increased stakeholder value.

The IIA has not actively supported a shift from traditional risk-centric ERM methods and control and process-centric methods to an objective-centric risk self-assessment approach. IIA guidance on how to assess the effectiveness of ERM frameworks does not call for an evaluation of the approach by assessing identified risks linked to a company’s top value creation and value preservation objectives.

**BARRIERS TO CHANGE**

- **Influential ERM guidance sources**, including COSO and ISO 31000, while defining risk in terms of its ability to effect achievement of objectives, implicitly endorse risk-centric approaches to risk management that use risk registers, not objectives registers, as a foundation. COSO and the authors of ISO 31000 do not advocate that the process should start by identifying and prioritising objectives, then make conscious decisions on which objectives warrant the cost of formal risk assessments. The COSO ERM exposure draft issued in June 2016, while increasing the focus on value creation objectives, stops short of calling on companies to create and use objectives registers as a foundation for ERM.

- It may be a very uncomfortable and unfamiliar exercise for the board and management to agree on the top value creation and value preservation objectives. This reluctance prevents efficient entity level resource allocation and decision making. An objective-centric approach focuses first on defining the top objectives key to sustained long-term success – it seeks a balance between value creation and value preservation. A risk-centric risk register ERM approach is often quite vague on its linkages to top value creation/ preservation objectives and rarely makes a link to performance.

- Management has to take on substantially greater ownership and act as primary risk assessor/reporter for the company’s top objectives, including providing a report and opinion on the overall residual risk status for each objective. This is a fundamental shift that requires changes to how management and traditional ERM and internal audit teams interact and discharge their responsibilities. It may also include a fundamental risk culture shift, where candidly described significant negative residual risk positions is rewarded, not punished by internal audit and senior management.

- A global shortage of staff with the knowledge and skills to implement an objective-centric risk self-assessment framework. Business schools are still in their infancy in producing enterprise risk management curriculum beyond traditional internal audit and accounting courses that teach control-centric models heavily linked to effectiveness of internal controls over financial reporting and IT security. Those schools that do cover risk management fundamentally about hazard avoidance and defence – not a key support tool to take risks intelligently and drive increased stakeholder value.

- There is a global shortage of staff with the knowledge and skills to implement an objective-centric risk self-assessment framework. Business schools are still in their infancy in producing enterprise risk management curriculum beyond traditional internal audit and accounting courses that teach control-centric models heavily linked to effectiveness of internal controls over financial reporting and IT security. Those schools that do cover risk management fundamentally about hazard avoidance and defence – not a key support tool to take risks intelligently and drive increased stakeholder value.

**The way forward: a board-driven ERM paradigm shift**

Boards and ERM specialists need to work together to understand the substantial differences between risk-centric and objective-centric assessment frameworks. More information on the business case for objective-centric risk management vs traditional risk-centric approaches would help these registrars as a foundation.

**Require a robust management-driven, objective-centric risk self-assessment approach**

In an objective-centric risk self-assessment framework that uses an objective register as the foundation, it is expected that objective registers would be aligned with the top value creation and preservation objectives to ensure optimal capital allocation. The objectives register would include the company’s top value creation and value preservation objectives.

These should be defined by management and reviewed by the board. Owners/sponsors should be assigned to each objective (see the sidebar for the authors’ definition). Owners/sponsors are responsible for assessing and reporting on the state of each objective. These registers are linked to the CEO and the board using an ISO 31000 compliant assessment methodology (for an example of an objective-centric approach see the RiskStability assessment approach shown on page 50). Conclusions should be made on the target level of risk assessment rigour and independent third parties should receive regular reports on the residual risk status of the objectives in the registers.

The objective residual risk status (CRBSR). A sample set of definitions for CRBSRs is also on page 50.

**Require that the CEO or his/her designate regularly (bi-annually or quarterly) provide the board with a consolidated report on residual risk status linked to the company’s top value creation and value preservation objectives.** This simple step has great potential to drive the necessary changes to the management and all of the specialist assurance groups do their work.
This repositions the role of internal audit within the company's risk management framework and reliability of the consolidated reports from the CEO to the board – information the internal auditors often claim their audit methodology is 'risk based'.

Ironically, most internal audit departments claim their audit methodology is risk-based. The audit plan often does not cover the company's most important value creation/preservation objectives and report consolidated risk status information. The current composite residual risk status is already extremely material and any given year. Results of individual internal audits are reported to management and the board – information the internal auditors often claim their audit methodology is 'risk based'.