© Steven Barlow and IRM

Getting to grips with embedding risk management

While there is a lot of talk about embedding risk management, there is little agreement as to what it means. Steve Barlow offers some critical steps to get things moving

Most organizations have a stated intention to embed risk management and integrate it in key business processes. This is easy to say but difficult to achieve in practice.

Risk functions still tend to operate as silo, compliance-based activities which tend to be mainly backward looking. The risk registers and information they produce do not drive business decisions or focus enough on the achievement of objectives. Risk management should be all about increasing the level of confidence that objectives will be achieved.

The following are critical steps to embed risk management and steer the strategic direction of the business:

1. **Focus the approach to risk management on objectives rather than risks:** objectives are "what gets measured" and are therefore the basis for "what gets done". Objectives provide the context for the identification and assessment of risks and are the first stage in implementing effective and embedded risk management.

   Objectives should be "SMART": *Specific* (e.g. a specific area for improvement); *Measurable* (quantify or at least identify an indicator of progress), *Agreed* (specify who will do it), *Realistic* (what can realistically be achieved given available resources) and *Time related* (when the results will be achieved).

   An organization should keep the number of objectives to a manageable level i.e. perhaps 4 financial objectives, 4 strategic/operational and 4 people related. Anything more than about 12 objectives would be too many.

The views expressed in this article are Steven Barlow's and do not represent the official view of IRM

The Chief Executive should hold the objective owners accountable for the achievement of their respective objectives ***together with the management of the associated risks.*** The objectives should be included in the personal objectives of each Chief Officer and the latter should cascade them to their direct reports.

2. **The Chief Executive should appoint an owner for each business objective:** this should be the "*single point of accountability*" not only for the objective **but also** the management of the associated risks. This:
    a. ensures integration of risk and performance management "at source"; and
    b. confirms that the objective owner, not the risk function, is responsible for identifying and assessing the associated risks and developing the related action plans.
3. **Design and implement a "corporate objectives performance scorecard":** to measure and monitor the achievement of each objective. The performance scorecard should be the **key monitoring and control framework for the organization**. It should report the current and forecast status of achieving each period at the period end together with the actions being taken to ensure the objectives will be met.
4. **Define the organization's overall risk appetite**. The amount of risk, on a broad level, an organization is willing to accept to achieve its objectives (*COSO definition).* Use of risk appetite helps measure whether objectives are being delivered in a **sustainable** manner over the long term. The statement should define clear boundaries of what is acceptable e.g.
    - Governance model compliance (terms of reference, delegation of authorities, policies).
    - Avoid unethical practices and reputation risks.
    - Avoid significant business disruption.
    - Low tolerance to control weaknesses assessed by internal audit to be significant.

- Meeting business plan targets - action plans required to mitigate high risks of not achieving targets.
- New business plans and proposals should only be approved if: a) they meet target rates of return; b) include thorough risk analysis; and c) there is a high confidence returns will be achieved.

5. **Define the organization's risk tolerances:** The amount of risk that is tolerable in achieving objectives and related thresholds not to be exceeded. Tolerances determine acceptable/ unacceptable performance; and drive action plans to: a) reduce uncertainty in achieving objectives; and b) protect assets and reputation. The tolerances should be linked to the risk scoring assessment and the performance management scoring for incentive purposes.
6. **Calibrate the performance scorecard using risk tolerances:** to define acceptable/not acceptable performance thresholds related to each objective. Use of the risk appetite and tolerances in this way further integrates risk and performance management.
7. **Design/implement the "*balanced*" element of the performance scorecard:** develop measures (from the risk appetite) to help assess *whether objectives are being achieved in a sustainable way* e.g. the number of governance breaches; adverse media coverage; major IT system downtime; major cyber incidents; major business continuity disruption and Health & Safety events; overdue remediation of critical internal control issues.
8. **Integrate the performance management process with the performance scorecard design/outputs:** thereby ensure achievement of objectives by owners *and management of the associated risks* is directly linked to their personal performance evaluation.

Embedding risk should be driven top down (based on the key principle that *"what gets measured gets done"*) by integrating the way objectives, risks and performance are measured/monitored.

© Steven Barlow and IRM

When everyone sees achievement of objectives/management of risks has a ***direct impact on their bonus/incentives***, the culture and attitude to risk will change. Risk management will focus more on the future/strategic direction and become integral to the way the business is managed.

Steven Barlow has been a chief risk officer in the United Arab Emirates for almost 7 years and is former Chief Audit Executive of Novartis, Prudential, Pearson and the UK Department of Energy.

The views expressed in this article are Steven Barlow's and do not represent the official view of IRM