The Three Lines of Defence Related to Risk Governance

Enterprise risk management (ERM) facilitates management’s desire to effectively govern and manage the enterprise’s approach to risk management and to create sustainable value to its stakeholders through business objectives such as capital growth (i.e., share value), increased dividend stream and satisfactory customer service. No enterprise operates in a risk-free environment, and implementation of ERM does not create such an environment. Rather, enterprises operate in environments filled with uncertainty, requiring proactive action to address risks in order to survive and prosper.

Effective ERM involves the strategic implementation of three lines of defence as the first principle of the risk management framework (refer to figure 1). At each line of defence there needs to be risk governance guidance to support the ERM framework.

FIRST LINE OF DEFENCE
The first line of defence is the front-line employees who must understand their roles and responsibilities with regard to processing transactions and who must follow a systematic risk process (such as that documented in ISO 31000, see figure 2) and apply internal controls and other risk responses to treat the risks associated with those transactions.

Depending upon the size of the organisation, the enterprise’s business unit (division) may have a risk management committee. This risk management committee is the first line of defence of the risk governance framework. This committee is empowered with the responsibility and accountability to effectively plan, build, run and monitor its department’s day-to-day risk environment. The committee provides direction regarding risk response (i.e., treatment) for those risks that are outside of the business unit’s risk tolerance.

Line management has the responsibility to identify and assess risks and to ensure that the control activities and other responses that treat risk are enforced and monitored for compliance. The information that line management should report to the business unit’s risk management committee to enable it to achieve this objective includes:

- Risk footprint, heat map (critical and highly rated residual risks)
- Key risk issues, planned mitigation actions and person to act (PTA)
- Status of existing mitigation actions to mitigate risk
- Key risk indicators (red or amber)
- Control effectiveness indicators (red or amber)
- Incidents and breakages (including historical/trend analysis/statistics, status of mitigation actions and lessons learned)

Figure 1—Risk Management Three Lines of Defence

<table>
<thead>
<tr>
<th>Risk Governance Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Strategy</td>
</tr>
<tr>
<td>Governance and Management</td>
</tr>
<tr>
<td>Execution</td>
</tr>
</tbody>
</table>

Do you have something to say about this article?
Visit the Journal pages of the ISACA web site (www.isaca.org/journal), find the article, and choose the Comments tab to share your thoughts.
• Outstanding Sarbanes-Oxley-related deficiencies or internal/external audit items that are past their action due date

The risk report and minutes of the business unit’s risk committee are forwarded to the enterprise risk management function for review. This information is then collated with other risk reports and assessed and reported, both independently and directly, to either the second- (executive risk committee) and/or third-line risk governance committees (board risk committee), who are charged with the role of representing the enterprise’s stakeholders in respect to risk issues.

The second (risk and compliance) and third (audit) lines of defence often request the same information as the first-line management and governance committees. In practice, often this independently assessed risk information conveys a mixed message with the result that there is an arc of miscommunication, i.e., what is reported does not always align with the risk reality as perceived by front-line management. This difference in perspective is what adds value to the enterprise as a whole and to the ERM framework in particular. It is for the senior enterprise risk governance committee to evaluate the reports from these multiple sources and determine (or advise the main board on) the direction the enterprise should take.

**SECOND LINE OF DEFENCE**

The second line of defence is the enterprise’s compliance and risk functions that provide independent oversight of the risk management activities of the first line of defence. The compliance and risk functions may have their own management and governance committees that are part of the ERM framework, or they may have direct reporting lines into appropriate ERM framework structures.

The responsibilities of these second-line functions typically include participating in the business unit’s risk committees, reviewing risk reports and validating compliance to the risk management framework requirements, with the objective of ensuring that risks are actively and appropriately managed.

Depending upon the size and complexity of the enterprise and its business, there may be a management board risk committee (MBRC), which serves as the second line of risk governance. The enterprise’s compliance and risk functions report to the MBRC. The MBRC is to have a charter, which sets out its role mandate and authority to manage the enterprise’s risk environment.

For many enterprises, the reaction to the global financial crisis (GFC) has been to question its second line of defence—the compliance and risk functions. In so doing, the following are being questioned:

• The risk management culture
• The understanding of the ERM framework
• The business unit’s risk capacity
• The risk appetite and tolerance allocation for each risk category
• The adequacy of the risk budgets
• The skill and capabilities of its risk resources
• The risk governance approach
• The risk monitoring and reporting activities
• The risk metrics to alert the business of the emergence of risk
• The capability to adjust the business unit’s risk capacity, appetite and risk tolerances for changing economic conditions

As part of the first line of defence, these are aspects of the ERM arrangements set by the MBRC charged with the role of representing the enterprise’s stakeholders in respect to risk issues. However, should the MBRC be questioning the...
effectiveness of its own risk decision making based on the information that was provided by the second line of defence? Enterprises have invested heavily in their risk and compliance functions, including the use of complex risk models; however, very few have invested in identifying why they received poor risk information, or in the quantum, the timing or the relevance of the information, to enable themselves to make adequately informed and, therefore, effective risk decisions.

Alternatively, should executive management have a closer look at itself? Would it find that it is at fault? Does executive management have the necessary experience, skills and authority to make the decisions? Is it too strongly influenced by rewards, such as bonus incentives, and the fear of shareholder demands to ignore or take risks that may lead to regulatory intervention or, even worse, financial failure?

THIRD LINE OF DEFENCE

The third line of defence is that of internal and external auditors and the US Sarbanes-Oxley Act compliance team (where applicable) who report independently to the senior committee charged with the role of representing the enterprise’s stakeholders relative to risk issues.

The internal and external auditors and Sarbanes-Oxley teams regularly review the first and second line of defence activities and results, including the risk governance functions involved, to ensure that the ERM arrangements and structures are appropriate and are discharging their roles and responsibilities completely and accurately.

The results of these independent reviews need to be effectively communicated to executive management and, more important, to the board of directors in cases in which these groups ensure that appropriate action is taken to maintain and enhance the ERM framework.

As stated earlier, the body that has the highest level of risk governance is the senior committee (such as the enterprise’s board of directors or some other body, e.g., the audit committee or a specific risk committee) that is charged with the role of representing the enterprise’s stakeholders in respect to risk issues. This committee has the responsibility and accountability to provide effective oversight of the enterprise’s risk profile. In particular, this committee should ensure that the enterprise’s executive management is effectively governing and managing the enterprise’s risk environment.

The senior committee charged with the role of representing the enterprise’s stakeholders relative to risk issues is ideally composed of directors and non-executive directors (where appropriate), with the committee chair reporting to the chair of the board of directors. The enterprise’s chief risk officer reports to the chair of the senior committee on a periodic basis (typically recommended to be no less than quarterly). The chair of the senior committee reports to the board of directors on the status of the enterprise’s risk environment on a periodic basis (typically recommended to be no less than biannually).

The senior committee is typically required to have a charter that clearly sets out its role, responsibilities and accountabilities in providing risk governance to effectively discharge the requirements delegated by the board of directors.

The critical issue facing the senior committee is risk information. Too often, there is too much information (i.e., risk noise), which overwhelms the committee. The committee members need to know the critical risk issues that require their attention. The senior committee needs to state clearly what risk information it requires (i.e., relevance), and the format and timing of such information.

CONCLUSION

For many enterprises, the setting up of a risk governance structure and supporting ERM arrangements is relatively simple. The real challenge is ensuring that the expectations and perceptions of risk governance and management and the senior risk committee are aligned, and that risk-related information is effectively and consistently obtained, analysed and used. In reality, there is often an arc of misconception, i.e., management has its view of the enterprise’s risk profile, and the added value of the second and third lines of defence is not incorporated effectively within the overall governance approach to optimise achievement of enterprise objectives.