Top 10 Questions Boards Should Ask About Enterprise Risk Management

Executive Summary: The complexity of ERM poses special difficulties for P/C insurance company board members who are being asked to play a larger role in risk governance. To adequately assess ERM program effectiveness, board members must cut through the usual ERM updates and get answers to more incisive questions, says ERM Consultant Sim Segal, who proposed 10 questions to help directors better understand the ERM programs of their organizations.

By Sim Segal

Board members are being asked to play a larger role in risk governance. Regulatory requirements, rating agency criteria and evolving management practices are increasing the volume and frequency of board information related to enterprise risk management (ERM).

Board members must understand and interpret this information to arrive at an evaluation of the quality of the company's ERM program.

However, ERM presents a special challenge for board members due to a lack of widely accepted practice standards, disparate nomenclature and inadequate sources of board training. As a result, board questioning of ERM practices often misses the mark and can result in board members overestimating the organization's shock resistance.

To better assess an ERM program, board members must get answers to revealing questions such as the following:

1. Are we excluding some areas of the enterprise?

Enterprise is the first word in enterprise risk management. Nevertheless, ERM programs are not always consistently applied to all parts of the organization.

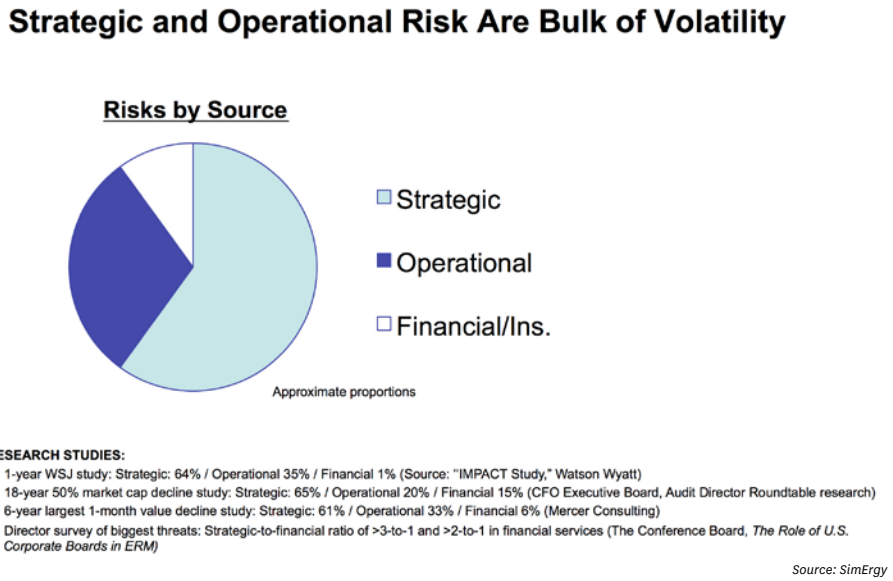
High-growth or high-profit business units may resist scrutiny by corporate ERM, using their political power along with a presumption that the gains outweigh any potential risks. Unfortunately, a failure to include these areas often exposes the organization to an unacceptable level of risk, since areas that lack transparency and accountability typically are more susceptible to sudden, massive losses.

In addition, small or immature businesses are sometimes excluded from the ERM process because they are deemed immaterial. This is also dangerous. Risk exposure is not always proportional to traditional volume measures.

2. Are we omitting the most important types of risks?

Board members expect ERM measures of firm volatility to be based on a full consideration of all key risks. ERM programs usually do capture the volatility arising from financial risks, such as market risk and credit risk, and they also capture the volatility of insurance risks, including mispricing. What most fail to quantify, however, are strategic and operational risks. Strategic risks include strategy execution, competitor, regulatory and governance risks, while operational risks are risks such as human resources-related risks and technology risks.

The failure to capture the volatility of these risks is particularly disturbing because industry studies consistently show



that strategic and operational risks account for the bulk of firm volatility, even for financial services companies. (See chart.)

Failing to include strategic and operational risks in expressions of firm volatility represents a massive distortion and underestimation of the organization's risk exposure.

3. Are we focusing on the wrong key risks?

It is common practice to use a qualitative risk assessment (QRA) process to narrow down a lengthy list of potential risks to the key risks that can significantly impact the firm. This involves asking a broad group of individuals to suggest potential key risks and to score their likelihood and severity using qualitative categories such as "very high," "high," "medium," etc. The key risks are selected using a ranking produced by these scores. This is a necessary and widely adopted first step in the ERM process cycle. Unfortunately, many ERM programs directly attempt to use this information for decision-making, such as which risks to focus upon, which to mitigate and to what level to mitigate them, etc.

"Typically areas that lack transparency and accountability are more susceptible to sudden, massive losses."

This can lead to an inappropriate level of mitigation and, more importantly, often leads to selection of the wrong key risks. The QRA process is a preliminary prioritization suitable only as an initial screening, which must be vetted in the next step in the ERM process cycle: risk scenario development and quantification. This involves developing and quantifying a set of robust risk scenarios for each potential key risk using a rapid but deeper-dive process.

The prioritization produced by the risk scenario development and quantification process replaces the one produced by the QRA process because it is superior in three ways:

- It leverages information from subject matter experts for each risk rather than relying on a broad group of individuals.
- It develops information on specific risk scenarios rather than on an amorphous risk, allowing better focus. For example, rather than worry about "data breach" risk, we learn that we are really most concerned with "data breach in system X by system administrators with access to 100 percent of customer privacy data records."
- It provides quantitative point-estimate impacts rather than qualitative categories that often span wide ranges (e.g., "high" may be from 10 percent to 20 percent impact on a given ERM metric).

4. Are we missing some of the biggest threats?

Many ERM programs quantify the impact of each risk scenario on the organization. In situations where no single risk event may be found to be devastatingly large, many infer that the organization is invulnerable, since it can withstand any potential risk event.

This can provide a false sense of security. What most often takes down a firm is a combination of two or more risk events occurring simultaneously. To identify the biggest threats to survival, ERM programs must use models that simulate multiple concurrent risk events.

5. Are we ignoring our own experts' risk and business intelligence?

Many ERM programs develop risk scenarios using stochastic methods, which rely on formulas and randomly generated numbers to produce computer-generated scenarios. This can be useful. It provides another perspective that can assist in selecting which risk scenarios will represent a risk in the ERM model that estimates firm volatility.

A critical mistake made by many ERM programs, however, is to plug stochastically generated scenarios directly into the ERM model, bypassing their internal subject matter experts—those closest to the risk and to the business to which it relates.

Studies show that risk scenarios that fail to incorporate intelligence from experts and rely solely on statistical information are inferior and can lead to poor decision-making.

ERM programs should provide their risk experts with any and all available relevant information, including stochastic information. But they must allow these experts to interpret the information; filter it with their own knowledge, experience, expertise and intuition; and then select a set of deterministic risk scenarios for use in the ERM process.

For a case study revealing how a life insurance company ignored risk experts in favor of model results, see the cover story of the June-July 2013 issue of *The Actuary* magazine, "How Model Risk Devastated an Organization," also authored by Sim Segal.

Sim Segal is President and Founder of SimErgy Consulting, a firm specializing exclusively in enterprise risk management. He is also the author of "Corporate Value of Enterprise Risk Management" (Wiley, March 2011) and the host of "Risk Radio," a weekly radio show featuring discussions and interviews on ERM topics. Segal is Interim Director of ERM Programs at Columbia University, leading the development of an ERM master's curriculum.

Headquartered in Manhattan, SimErgy provides ERM consulting services to companies in all sectors, primarily in the U.S. and Canada, as well as executive education on ERM, including seminars, workshops and webinars, globally. Reach Segal at sim@SimErgy.com.

6. Do we use incomplete risk scenarios?

ERM programs often include some risks that are not properly defined by source but rather by outcome. For example, "reputation risk" or "ratings downgrade" are intermediate outcomes rather than sources of risk; there are many different sources of risk that can trigger either reputational damage or a ratings downgrade, and each source may be its

continued on next page

own unique risk in need of separate consideration and treatment.

Risks not properly defined by source may have incomplete risk scenarios because they fail to begin at the source, often missing multiple potential downstream parallel events and their corresponding impacts. For example, a "ratings downgrade" risk scenario might capture the impacts of a resulting increase in cost of capital and decrease in sales, but

"A critical mistake made by many ERM programs is to plug stochastically generated scenarios directly into the ERM model, bypassing their internal subject matter experts—those closest to the risk and to the business to which it relates."

it may fail to capture impacts of a likely cause of downgrade, such as a failure to execute the strategic plan. Incomplete risk scenarios can result in significantly underestimating risk exposures.

7. Is our risk appetite statement inadequate?

Most risk appetite statements include elements from the company's mission statement or strategic plan, qualitative statements about risks to avoid and quantitative risk limits from the investment guidelines. Unfortunately, this is not adequate for use in the risk governance process.

Risk appetite statements must clearly and quantitatively express the acceptable limits of aggregate enterprise risk exposure. Without such a robust risk appetite statement, management is unable to manage exposures to within risk appetite (the primary purpose of ERM) or to answer the question being asked by regulators and rating agencies alike: "If you were to hit each of your individual risk limits, would your enterprise risk exposure still be within your risk appetite?"

8. Is ERM informing our most important decisions?

ERM programs are intended to enhance risk-reward decision-making. At financial services companies, ERM typically is used for capital allocation and corporate reinsurance decisions. Too often, these ERM programs inform little else.

- They do not quantify strategic and operational risks and therefore cannot inform any decisions related to strategy or operations, which constitute the bulk of important decisions.
- They only develop downside (often only extreme downside) risk scenarios, accounting for the risk but not the return side of the risk-return equation, and therefore cannot support decision-making in general.
- They do not quantify the impact of risks on the value of the firm but rather only on capital, and without providing a before-and-after picture of changes in value, decision-makers cannot act confidently.
- The ERM model is too complex or unreliable, resulting in a lack of buy-in by key decision-makers.

9. Do we have inconsistent decision-making processes?

All business decisions—whether they are related to managing the level of risk exposure or to routine business—should use a single, consistent decision-making process based on whether or not the action increases company value. However, most ERM programs cannot identify an optimal level of mitigation by quantifying how it increases company value; instead, they select mitigation levels based on somewhat arbitrary risk limits that must be satisfied.

This approach abandons strategic planning and other routine business decision-making to a separate decision-making process. In addition, it leads to suboptimal results due to mitigation levels not aligned with increasing company value.

10. Are our risk disclosures suboptimal?

A robust ERM program provides an opportunity to communicate to external stakeholders—particularly regulators, rating agencies and shareholders—the company's superior capabilities in managing risk and how this enhances shock resistance and increases the odds of achieving strategic plan goals. However, many companies miss these opportunities, send the wrong signals and even expose the organization to great risk through suboptimal risk disclosures.

Communications to regulators and rating agencies often fall short of their potential due to suboptimal selection of which risks or ERM program elements to emphasize or de-emphasize; not fully understanding perspectives of regulators or rating agencies or their representatives; or flawed translation of company risk nomenclature to that of the regulator or rating agency.

Even more dangerous is a mismatch between ERM information gained internally versus that represented in shareholder disclosures, which may give a misleading impression of the risk profile.

Suboptimal risk disclosures may well be the most overlooked risk in most ERM programs.

As these questions reveal, ERM is a complex, broad-ranging process that poses special difficulties for board members. To adequately assess ERM program effectiveness, they must cut through the usual ERM updates and get answers to more incisive questions. These 10 are a good start to more clearly revealing the true underlying strengths and weaknesses of an organization's ERM program. CM **carriermag.com/t4udy**

See related online articles:

- Carrier CROs See Evolution in Board Worries at **carriermag.com/c53e4**
- Inadequate Shareholder Disclosure and Other Killer Risks at **carriermag.com/ezigs**
- Talent Risk: A Killer Torpedo? at **carriermag.com/8j4ds**