

ERM AND THE RATING AGENCIES

The subprime debt collapse and the ensuing credit crisis have spotlighted enterprise risk management (ERM). The result has been a significant heightening of interest in ERM as well as increased scrutiny of ERM theory and practice. How did it happen that the banking industry, which has historically implemented the most explicit ERM requirements, suffered enormous and, in some cases, fatal losses from risks that in hindsight were obvious?

Another significant development in the world of ERM (perhaps fueled by the banking crisis) is the emergence of ERM as a factor that major rating agencies evaluate when rating organizations outside the financial sector.

Within much of the financial sector, particularly the insurance industry, an organization's ERM is already a major rating consideration. There is clear evidence within the sector that the importance of ERM to ratings will only increase in the coming years.

THE RATING AGENCY PERSPECTIVE

Rating agencies are primarily concerned with the ability of an organization to repay creditors in a full and timely manner. Within the insurance segment, the assessment of a company's ability to honor obligations to policyholders – known as insurance financial strength ratings – is critical, but within the broader spectrum of



ratings, agencies are primarily concerned with the ability of an organization to repay rated debt. They are less concerned with earnings volatility that may be associated with losses except to the extent that the volatility can lead to a default or perhaps a downgrade.

Nevertheless, surprises from ineffective risk management have historically led to defaults. This begs the question: Does a corporation with a strong ERM program, all other things being equal, default less often than one that doesn't have one?

It appears that each of the rating agencies believes that ERM is a component of sound management but has a somewhat different take on how to address the topic, with S&P leading the way in terms of attributing value to ERM.

STANDARD & POOR'S ERM APPROACH

S&P has taken the most explicit steps toward incorporating the evaluation of ERM in their rating process. In the fall of 2007, they issued a draft ERM evaluation framework for public comment and are now in the implementation phase. S&P's basic plan can be summarized as follows.

- During Q3 2008, they will begin to include ERM questions in rating discussions with rated companies, focusing on culture and strategic risk management
- In Q4 2008, they will include commentary on the organization's ERM capability on a case-by-case basis
- Ultimately they will provide investors with a specific rating on their company's ERM capabilities (this will likely be no earlier than 2009)

Leading up to this last stage, S&P will be building a database to benchmark ERM practices within market sectors, industries and geographies.

S&P has issued material on ERM that amounts to a definition of what ERM is – and is not. Below we summarize key points of the S&P ERM definition and what implications Willis believes those points may have for an organization being rated.

According to S&P, ERM is:

- An approach to assure that the firm is attending to all risks
Implication: *There must be a discernable process to identify and prioritize risks and deal with those requiring attention.*
- A set of expectations among the board, management and shareholders about the risks the organization will or will not take
Implication: *There must be disclosure to shareholders of the risks the company will and will not take. This may also require defining a risk appetite or tolerance.*
- A method to shift from cost/benefit to risk/reward analysis
Implication: *Risk awareness should be embedded in the decision processes.*
- A way to fulfill the fundamental responsibility of a company's board and senior management
Implication: *An effective risk management system needs to be fully integrated from the top down.*
- A toolkit to identify risks and to mitigate them
Implication: *The program should employ risk management processes that deliver clear results.*
- A language for communicating the firm's efforts to maintain a manageable risk profile
Implication: *There should be a common risk language and ERM should be a defining characteristic of the firm's culture.*

In the S&P view, ERM is *not*:

- A method to eliminate all risks
- A guarantee that the firm will avoid losses
- A tossed-together collection of disparate practices

- A rigid set of rules
- Solely a framework for compliance and disclosure
- A replacement for internal controls
- Exactly the same for all sectors in all years
- A passing fad

S&P cannot audit assertions of clients, but they will compare statements about ERM with past performance and will look at ERM in light of significant earnings drops or similar adverse events. (Comments on how ERM is addressed at Moody's Investor Services and Fitch Ratings appear below.)

CHOOSING AN ERM APPROACH

S&P's approach is not the only one, and its recent arrival serves to underscore the fact that over the past 20 years, as ERM has become more accepted and moved beyond financial institutions to most industry sectors, many approaches have developed. The most widely known of these may be the COSO (Counsel of Sponsoring Organizations) framework.

Recently RIMS has sponsored the development of a risk maturity model that addresses ERM in terms of the culture, processes and tools that represent best practices in implementing an effective ERM program. The RIMS approach includes seven core, measurable competencies.

- 1 ERM integration across risk management, internal audit, IT and other risk-related functions
- 2 Weaving ERM processes into other business processes
- 3 Risk appetite management
- 4 Root cause discipline
- 5 Uncovering risks
- 6 Performance management
- 7 Business resilience and sustainability

Clearly there is no one set of generally accepted ERM principles. Organizations will have to assess their own constituencies and needs to decide what framework makes the most sense for them. In the final analysis, selection of an approach to ERM has to be made in the context of what will best deliver consistent, discernable and practical value over time.

POTENTIAL PITFALLS

It is likely that some organizations will be motivated to adopt an ERM strategy purely as a response to rating agencies handing out ERM report cards. If the sole reason an organization implements ERM is to satisfy rating agencies, however, they may be making a serious mistake. When ERM is treated as a form-filling exercise, it usually fails. We expect the rating agencies will be on the lookout for this and will try to assess whether an organization's ERM approach will deliver real value or exists only to influence rating agency perception.

Another risk that organizations face when moving toward ERM is adopting one of the existing approaches and following it to the letter. ERM works best when organizations implement an ERM framework that is aligned with and reflects what is unique about their operations and exposures. A flexible approach to ERM may take some time to develop but is likely to bring the best results.

WILLIS' ERM PERSPECTIVE

Our perspective on ERM can be broadly characterized as follows.

- Because of the intrinsic value in tailoring a framework to fit the structure, objectives and culture of each organization, a canned approach can be counterproductive.
- While the key risk assessment processes supporting the program need to reflect the complexities of the organization, they must also be simple and intuitive in order to facilitate their assimilation into the organization's culture and risk management strategy.
- Boil-the-ocean approaches that entail detailed analysis of every risk, major or minor, across an entire organization all at one time, are vulnerable to failure. Conversely, implementing a program incrementally allows an organization to learn what works best for them while winning internal buy-in.
- Along with articulating, assessing and processing the known risks of an organization, the ERM program should be visionary enough to unearth previously unrecognized and emerging uncertainties.
- Finally, an effective ERM program will enhance the organization's business, not simply by reducing undesirable risk, but by encouraging effective and prudent risk taking.

ERM AT THE OTHER RATING AGENCIES

MOODY'S

While Moody's does not have explicit ERM criteria or even specific risk management criteria that apply to all organizations, it does have very specific guidelines for rating about 50 industry segments. In these guidelines, Moody's does not typically refer to ERM explicitly, but the nature of the risk management criteria they use will implicitly favor ERM. For example, for one segment, they refer to "management's risk control culture and capabilities."

Moody's view of an organization's risk management varies by industry segment. For example, Moody's analysis of processing and trading companies is almost totally based on those companies' explicit management of risk. Its guidelines for the non-bank global securities industry have an explicit 12% weight on risk management: 3% for governance, 3% for management, 3% for quantification and 3% for the environment. For food companies, the explicit risk management structure appears to count for far less, although the factors that do apply – scale, diversification, franchise strength, cost efficiency, liquidity under stress – may benefit substantially from an effective ERM strategy.

An interesting industry segment is the global commodities processing and trading industry, where the key rating factor is commodity trading risk, and the related supply chain risk management. Moody's provides enormously detailed guidance. Moody's risk management considerations encompass risk appetite, controls, limit allocation, mitigation, measuring, monitoring, reporting and infrastructure, including data, models and systems. Apart from market risk, there is little mention of credit risk, safety, etc. Moody's considers what it calls "industrial risks," such as safety, outside of its scope unless there is an indication that the organization is not committed to the highest standards.

Because there is such a range in the degrees to which risk management is critical to Moody's, any organization wanting to evaluate how Moody's might view the benefits of enterprise risk management should review the appropriate segment discussions and perhaps have direct discussions with Moody's.

FITCH

Fitch has no explicit risk management standards for corporate debt ratings. They consider the risk management acumen of management as a part of the overall rating without incorporating formulaic measurement of ERM.

CONTACT

For more information about ERM and to learn about Willis' ERM capabilities, please contact:

Steve Saporito

Managing Director

Willis Enterprise & Risk Finance Practice

+1 617 351 7404

steve.saporito@willis.com