ERM in the Aftermath of the Credit Crisis

Poor risk management practices may have caused the global financial recession. The time has come for banks to implement stronger enterprise risk management programs.

By Jennifer F. Burke, CPA, CRP, CFS, Partner Crowe Horwath LLP

As the credit crisis slowly recedes, increasing and more complex risks will pose a significant governance challenge for financial institutions. A competitive global marketplace, stricter legal requirements, shorter product cycles, complicated business transactions, and the explosion of technology all multiply the risk exposure of financial firms.

The collapse of several high-profile banks in 2008 and 2009 served as a wake-up call to the financial sector. Their failures exposed dangerous weaknesses common in financial institution risk management and governance, including:

- Gaps in risk expertise.
- Lack of influence of the risk function.
- Lack of responsibility and accountability at all levels.
- Overemphasis on profit-oriented compensation structures.
- Business models too reliant on ample market liquidity.
- Complex products in the marketplace.
- Excessive focus on short-term gain.
- Lack of healthy skepticism at all levels (e.g., auditors, regulators, boards, and management).

Such risk management deficiencies have had a ripple effect throughout the financial industry. The mortgage meltdown and the declining real estate markets led many banks, to tighten their lending requirements. Heightened regulatory expectations have produced a rise in bank failures, difficulties in managing portfolios, and mounting regulatory actions.

The credit crisis and its repercussions have prompted a growing number of financial institutions to examine their risk management policies and procedures and consider implementing enterprise risk management (ERM) (see “Calls for Improvement”). By implementing ERM, financial institutions can take advantage of current opportunities to gain long-term competitive advantages.

Understanding ERM

The Committee of Sponsoring Organizations of the Treadway Commission’s (COSO’s) Enterprise Risk Management–Integrated Framework defines ERM as “a process, affected by an entity’s board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.” More simply put, ERM integrates an organization’s risk management functions to align strategies, people, technology, and knowledge on an enterprisewide basis. It allows a financial institution to focus on interrelated risks throughout the organization.

ERM contrasts with the traditional “silo” approach to risk management, in which organizations manage each type of risk—including legal, strategic, operations, and IT risks—by business unit (see “What’s the Most Critical Risk?”).

This bottom-up approach often leads organizations to underestimate the effects of certain risks. For example, when financial institutions conceive of credit risk, they often think of credit risk in the lending portfolio. As the credit crisis demonstrates, many organizations had significant credit risk in their investment...
portfolios as well as concentrations of investments in mortgage-backed securities. Thus, some organizations underestimated the effect of the decline in home values and increase in delinquencies on their institutions. Using an effective enterprisewide risk assessment process, risks can be aggregated across business units from the top down, leading to a more accurate understanding of the risks across the organization.

ERM has its limitations, of course. By definition, risk relates to the future, which is inherently uncertain. ERM cannot provide absolute assurance against the occurrence of risk. Even the most sophisticated risk management process remains vulnerable to errors in judgment, breakdowns in the process, overriding of controls, and surprises.

Despite these limitations, ERM has proven valuable for financial institutions. It positions an institution to better predict risk and establish the processes necessary to react to extreme risks. For example, a bank in Louisiana could take steps to better prepare for the risks associated with the next major hurricane and design specific responses to those risks, such as establishing a backup processing site in a state not subject to hurricanes. ERM activities may result in increased productivity, enhanced reputation, improved regulatory compliance, and better resource allocation. In turn, revenues may climb and overall costs may drop. After effectively implementing ERM, a financial institution’s management team will notice numerous changes in the organization’s risk management:

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management activities are informal and not documented.</td>
<td>The risk management process is formalized.</td>
</tr>
<tr>
<td>Risk is inconsistently defined and understood.</td>
<td>The CEO and the board understand the organization’s specific risks.</td>
</tr>
<tr>
<td>Risks are considered solely within functions or business units.</td>
<td>Risk is considered in the context of overall business strategy.</td>
</tr>
<tr>
<td>The risk universe is poorly defined.</td>
<td>A formal and prioritized risk universe is established.</td>
</tr>
<tr>
<td>Reporting is haphazard and focused on easily quantifiable historical data.</td>
<td>Both qualitative and quantitative data are analyzed to provide insight for decision-making.</td>
</tr>
<tr>
<td>Reporting is fragmented or nonexistent.</td>
<td>Reporting is structured within an ERM governance process and appropriate detail is provided to all levels of the organization.</td>
</tr>
<tr>
<td>Ownership of risks is not defined.</td>
<td>Ownership of risks is clearly defined and understood at all levels.</td>
</tr>
<tr>
<td>Monitoring is informal or inconsistent.</td>
<td>The ERM process, risks, and risk management effectiveness are formally monitored.</td>
</tr>
</tbody>
</table>

Calls for Improvements

Even before the crisis, regulators, credit rating agencies, and other voices were advising the financial industry to strengthen risk management. Deloitte’s 2007 Global Risk Management Survey highlighted the state of risk management in the banking industry before the crisis. In responding organizations, 70 percent of boards had oversight responsibility, and 84 percent had a chief risk officer. About one-third had an ERM program in place. Seventy-five percent reported that the ERM program’s value exceeded its cost. Strikingly, 80 percent believed risk management was extremely or very effective for credit and market risk.

Today, most banks are revisiting their approach to risk oversight, according to a recent KPMG survey, *Never Again?: Risk Management in Banking Beyond the Credit Crisis*. Ninety-two percent of responding organizations are reviewing their risk management process, but only 42 percent have made or will make fundamental changes. Seventy-seven percent say they will work to improve their risk culture. But changing risk culture could be an uphill fight – more than three-fourths of the senior risk managers surveyed report that the risk management function is stigmatized as a support function.

Looking more closely at where risk management broke down, most KPMG survey respondents say incentive and remuneration policies were most at fault for the credit crisis. The level of risk expertise on the board was another significant weakness, with 45 percent saying theirs boards lack the necessary risk knowledge and experience.

Before After

Risk management activities are informal and not documented. | The risk management process is formalized. |
Risk is inconsistently defined and understood. | The CEO and the board understand the organization’s specific risks. |
Risks are considered solely within functions or business units. | Risk is considered in the context of overall business strategy. |
The risk universe is poorly defined. | A formal and prioritized risk universe is established. |
Reporting is haphazard and focused on easily quantifiable historical data. | Both qualitative and quantitative data are analyzed to provide insight for decision-making. |
Reporting is fragmented or nonexistent. | Reporting is structured within an ERM governance process and appropriate detail is provided to all levels of the organization. |
Ownership of risks is not defined. | Ownership of risks is clearly defined and understood at all levels. |
Monitoring is informal or inconsistent. | The ERM process, risks, and risk management effectiveness are formally monitored. |
ERM in the Aftermath of the Credit Crisis

For ERM to succeed, it must become an integral part of the organization’s culture. A top-down approach is critical and everyone in the organization must assume some degree of responsibility. The board provides governance, guidance, and management oversight. Management, especially the CEO, sets the tone and is charged with ultimate responsibility for the ERM process. In practice, most CEOs designate a risk champion, such as a dedicated chief risk officer or the general counsel to oversee the process. Some organizations have created an executive committee to handle the responsibility. The risk officer works with other managers to establish and maintain effective risk management in their areas of responsibility. And internal auditing monitors ERM and the quality of its performance.

Corporate Governance

Strong corporate governance is essential to sustaining a financial institution over the long term. In times of crisis, financial institutions must take extra care to keep their stakeholders in mind when making short-term business decisions with potentially long-term consequences. For example, one large bank responded to major problems with credit card balances and defaults by tightening credit lines and increasing fees for all of its customers. The bank may have found short-term relief but at the cost of alienating loyal customers over the long term. Similar considerations apply when an institution attempts to cut short-term costs through layoffs, which can eliminate crucial controls and create or expand risk exposure.

ERM supports sound corporate decision-making by:

- Aligning the organization’s risk appetite and strategy.
- Linking growth, risk, and return.
- Enhancing risk response.
- Minimizing operational surprises and losses.
- Identifying and managing cross-enterprise risks.
- Providing integrated responses to multiple risks.
- Seizing opportunities.
- Rationalizing capital.

By facilitating effective corporate governance, ERM can also increase the confidence of stakeholders, including regulators.

ERM in the Real World

ERM evolves – it cannot be triggered with the flip of a switch. Not surprisingly, the level of enterprisewide risk oversight today remains immature despite pressures stemming from the financial crisis. A recent study by the Enterprise Risk Management Initiative at North Carolina State University reports that most organizations have not fully embraced the need for a top-down, enterprisewide perspective on risk oversight. The increase in the volume and complexity of risks that confronts organizations in the wake of the credit crisis reinforces the need to re-evaluate existing risk management processes. While many organizations continue to take the silo approach to risk management, they increasingly seek to progress through the three stages of the risk management continuum: reactive, aware, and strategic. The reactive stage is characterized by poor board and senior management risk oversight; a silo-style, ad hoc approach to managing risk; and gaps in risk coverage. At the aware stage, some board and senior management support for ERM exists, and a risk leader has been identified. The organization profiles risks periodically and has developed a common vocabulary for defining key risks. In the final strategic stage, the board and senior management are proactively involved in ERM, risk is managed and assessed across the entire organization using a common language and approach, and the risk portfolio is analyzed in real time.

Most companies currently straddle the reactive and aware stages. According to the ERM Initiative study, though, boards are placing greater attention on risk, and management in many organizations is trying to create a more structured approach to risk oversight. These organizations understand the danger of overconfidence in the effectiveness of less-formal approaches. By beginning with risk fundamentals in mind, organizations can develop a disciplined, structured process that leads to consistent risk identification and measurement throughout the organization.

Keys to Success

Successful ERM processes share several features, such as agreement on, and understanding of, the organization’s risk appetite, clearly articulated risk management goals and objectives, linkage of risk management activities with other management activities, a clear governance structure, improved risk expertise at senior levels, strong oversight and validation of the ERM process, and accountability. In addition, organizations must clarify their risk terminology, leaving no room for disagreement between risk-averse and risk-seeking individuals over the acceptable level of risk.
The current environment offers opportunities for financial institutions to position themselves as strong competitors going forward. An effective ERM program improves corporate governance, increases the confidence of regulators and other stakeholders, and provides a competitive edge over institutions without such a program. When implemented correctly, ERM can become a strategy, rather than a defense in these difficult times.

About the Author
Jennifer F. Burke, CPA, CRP, CFS, is a partner in Risk Consulting with Crowe Horwath LLP in Lexington, Ky. She has more than 20 years of internal audit experience and serves as a national speaker and consultant in areas of risk for financial institutions.

This article originally appeared in the October 2009 issue of FSA Times, published by The Institute of Internal Auditors.

What’s the Most Critical Risk?
Employees view and prioritize risk differently, according to their respective vantage points. An organization’s most critical risk often depends on who you ask. While the CEO takes a broad view of risk, perhaps defining it in terms of the failure to meet strategic objectives, a teller may define risk in terms of failing to balance the cash drawer at the end of the day. Although both views are valid and warrant consideration, one challenge faced in implementing ERM is reaching agreement on the most critical risks. Capturing the different views of risk depicted in this chart makes for a dynamic and thorough risk assessment.

<table>
<thead>
<tr>
<th>Perspective</th>
<th>What’s the most critical type of risk facing the organization?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Financial Officer</td>
<td>Financial</td>
</tr>
<tr>
<td>Executive</td>
<td>Business Development</td>
</tr>
<tr>
<td>Corporate Counsel</td>
<td>Litigation</td>
</tr>
<tr>
<td>Operations Manager</td>
<td>Infrastructure</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Human Resources</td>
</tr>
<tr>
<td>Chief Information Officer</td>
<td>Community Relations/Public Relations</td>
</tr>
<tr>
<td>Boards/Audit Committees</td>
<td>Planning and Compliance</td>
</tr>
<tr>
<td>Internal Auditing</td>
<td>Accounting Information and Internal Controls</td>
</tr>
<tr>
<td>Controller</td>
<td>Financial</td>
</tr>
<tr>
<td>Compliance Officer</td>
<td>Regulatory</td>
</tr>
</tbody>
</table>

What’s the most critical type of risk facing the organization?