PRICEWATERHOUSECOOPERS

Organizing a Financial Institution to Deliver Enterprise-Wide Risk Management

By Kaan H. Aksel
PricewaterhouseCoopers

Everyone seems to be talking about enterprise-wide risk management (ERM): boards of directors, management, regulators, the business press. It has achieved the status of a buzz word among financial institutions and even in other types of companies.

The two underlying premises make sense: The first premise is that risks are often interrelated. Consider, for example, a bank that has an active program to securitize loans. As a result of securitization, the credit risk may decline, while the operational risks and risks to the bank's reputation may increase.

The second underlying premise of ERM is that risk management should be approached in a consistent, balanced, and integrated manner. The advantages to an integrated approach are many. First and foremost is the impact of enterprise-wide risk management on the bottom line. If ERM is effective, it should help reduce the volatility of the company's earnings, thus enhancing shareholder value. With an organized approach to risk, a firm can better manage its risks and returns to make more informed decisions about capital and investments.

For example, two different lines of business may have achieved equal profit at different levels of credit risk or operational risk; once the different risk levels are identified, they can become a factor in future strategic decisions.

Much of the current dialogue about ERM focuses on two areas: systems to measure exposures across an organization and ways of measuring the integration of market and credit risk. Progress has been made along both of these lines. Enterprise-wide measurement of exposure is now feasible, though it requires a large investment in systems and methodologies. The effect of market risk on credit exposure—for derivatives and other instruments—is being computed by increasingly sophisticated models. Other models address issuer or specific risk by quantifying the impact of downgrades in credit or changes in investor perceptions on market value.

With all the attention focused on measurement systems, not enough discussion has been devoted to the realities of *implementing* ERM. A particularly thorny aspect of implementation is the requisite organization structure. This is a significant issue since the organizational model for ERM sets the tone for the culture and processes that spell a successful enterprise-wide approach.

Organizational Issues

How should a company be organized to deliver ERM? This question is so new that no best practice yet exists. Organization structures—and indeed definitions—for ERM vary widely, often dramatically, from company to company. Some companies measure market risk around the world and call it enterprise-wide risk management. Others consider ERM to be measuring credit risk in all their locations. Many companies now integrate market and credit risks. A few more ambitious companies are also attempting to include operational risk under the umbrella of their ERM effort.

There are many benefits to centralizing the entire spectrum of an organization's risks—including credit risk, market risk, and operational risk. Rather than managing these risks by a committee or a series of committees, the most effective way to assure continuity and consistency in risk management is with a *single organizational unit* that bears direct responsibility for supervising the entire risk management process. Typically, such a unit is headed by a Chief Risk Officer (CRO)—sometimes called an Enterprise-Wide Risk Manager or Risk Czar—who is responsible for overseeing all the organization's business and financial risks.

Having a dedicated organizational unit addresses a disconnection that has troubled financial institutions for some time. Risk management efforts occur throughout the organization—in business units as well as company-wide functions such as the chief credit function, Information Technology, operations, and compliance units (e.g., Legal and Internal Audit). Consequently, the agendas of the various functions may differ, or--even worse--large risks may escape notice.

With a single organizational unit responsible for ERM, a company has a strong foundation for a successful risk-management process and culture. The centralized risk management function can develop a common risk framework, policies, and measurement methodologies. This commonality of approach gives senior management and decision-makers a clearer view of the interrelationships among various risks. With a framework that includes the full spectrum of risks, the company can make better cost/benefit decisions in its risk management and mitigation efforts, basing these decisions upon a balance between financial analytics and common sense. Such a comprehensive outlook on risk also facilitates proactive thinking about future risks.

The first step in designing an enterprise-wide risk management structure is to assess the organization's current approach to risk management. The following questions are relevant:

- Does the institution currently have an enterprise-wide risk management framework?
- What are your mission and strategic objectives for enterprise-wide risk management?
- Are these objectives known throughout the organization?
- Who is responsible for authorizing, taking, controlling, and evaluating each type of risk?
- Who is responsible for setting risk-adjusted performance methodologies?
- As an institution, is the risk culture one of advice or control (the carrot or the stick)?
- Are committees organized with clear accountabilities?

The Many Roles of a Chief Risk Officer

The organizational focal point for ERM is the position of Chief Risk Officer (CRO). Yet defining the role of a Chief Risk Officer is no simple matter. This job requires a range of knowledge, experience, and skill that is rarely if ever found in one individual. Most risk managers have a background in market risk, credit risk, or operational controls. Very few are experts in all three—and that's not all. To be effective, a CRO must possess the "people skills" needed to coordinate risk management activities across the entire institution and to navigate the inevitable realities of corporate politics.

The roles and responsibilities of a Chief Risk Officer vary according to the needs of the organization and the qualifications of the individual. The most important role is instilling a consistent level of risk awareness throughout the company. This is achieved by developing and implementing a risk management process to identify, measure, and control the full spectrum of risks using consistent economic capital measures.[1] Only by maintaining a comprehensive, company-wide perspective can a CRO ensure that the various risk strategies are sufficiently diversified.

An effective CRO is proactive, focusing not only on current risks but also on future exposures, generating discussion about what levels of risk are acceptable and what actions are needed to mitigate risks. Such a proactive approach necessitates thinking across risk types and performing stress tests.[2] An effective CRO is also a communicator who reports exposures and changes to senior management on a daily basis and inspires enough trust to be actively included in the company's strategic decision-making processes.

The role of a Chief Risk Officer is relatively clear in the areas of market and credit risk. Handling operational risks is much more challenging since these exposures occur in virtually every component of the organization—from sales and trading to the back office, finance, and information systems. Not only are operational risks spread out within the organization; they are also difficult to define and to measure.

Fortunately, recent advances have been made in devising processes that can identify, measure, and assess operational risks with growing precision. More and more companies are using such "indicative" measures as number of errors, unreconciled accounts, computer downtime, employee turnover, late reports, etc. Self-assessment processes -- based on comprehensive checklists and qualitative evaluations—are becoming increasingly well-developed.

Furthermore, risk quantification models have been devised to convert these numerical scores into dollars. The dollar figures can then be used for senior management or economic capital reporting. For example, at one large commercial bank, there is an operational risk team which performs assessments of the risks in each business line. Besides producing a comprehensive list of key controls, this team performs scenario analysis to estimate the probability and potential severity of operational losses for various risk scenarios. They have been evolving toward a more statistically based approach to risk, an approach that is based on a combination of their assessment data for each business line with internal and external loss experience.

If operational risk can be quantified with some accuracy, the Chief Risk Officer can then hope to achieve a comprehensive framework that extends across the whole organization and potentially covers all risks.

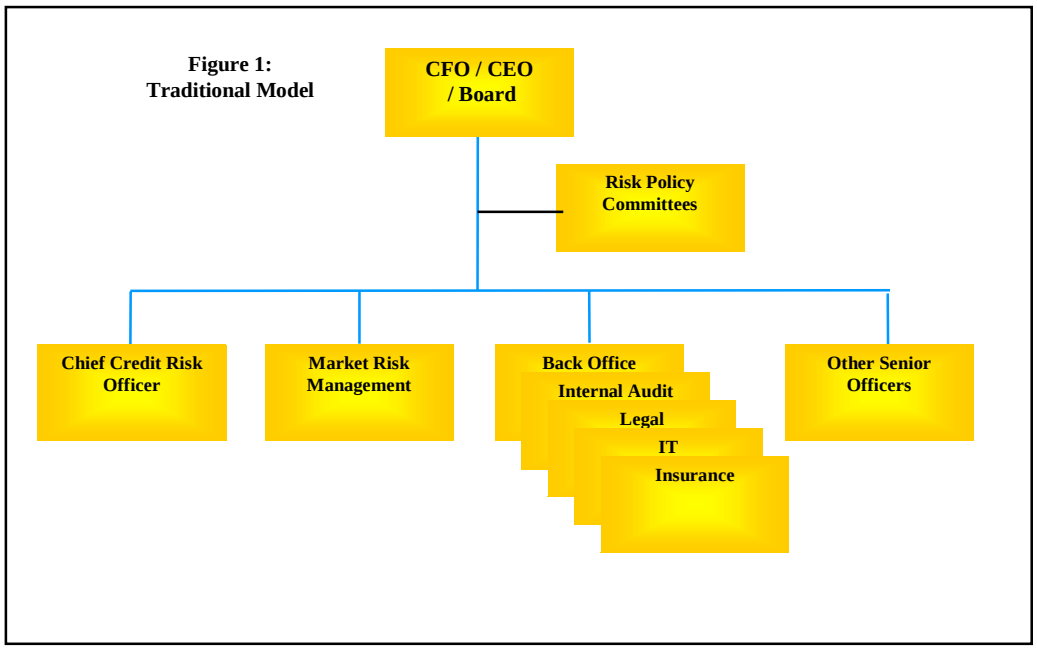
[1] I.e., dollars.
[2] Tests that examine the ramifications of extreme future scenarios in order to mitigate their effects.

In defining the position of Chief Risk Officer, a company needs to resolve the following issues:

- What core functions are necessary for a Chief Risk Officer to be successful?
- What skill levels are needed for the CRO?
- To whom should the CRO report?
- Who should report to the CRO? What are their roles and responsibilities?
- What authority should the CRO have vis-à-vis other individuals or committees to approve market limits, credit limits, exceptions, policies, and expenditures?
- Who is trusted to make decisions about the company's various risks?
- Is sharing and cooperation across the institution sufficient to permit dotted-line or peer relationships to work?

The Traditional Approach to a Risk Management Organization

Before enterprise-wide risk management became the standard, most financial institutions took a fragmented approach to risk, managing each type of risk in a separate organization or department with little or no effort at integrating these areas. Many organizations still follow a traditional model. A chief credit officer, who reports to the President or the Board, sets credit policy and approves exposures. Similarly, the market risk management function independently sets policies and measures and reports on market exposures and limits. Like the chief credit officer, the market risk executive is independent of the trading floor and might report to the CFO or the President.



Operational risk management is even more fragmented. Separate and uncoordinated groups such as Legal, Internal Audit, and Insurance are in charge of reviewing controls and risks. Managers of business lines incur risk and manage it as it arises in the day-to-day functioning of the business. Thus, many individuals around the company are responsible for a piece of the company's risk, and eventually, all report to senior management. Some individuals, such as a chief credit officer for example, may be responsible for risks across the organization, but only within their specific domains.

In the traditional system, all major risks are managed. Enterprise-wide functions are assigned to one or more enterprise-wide committees, which generally consist of representatives of such risk disciplines as finance, compliance, internal audit, and legal, as well as heads of some business units. One or more committees are typically responsible for credit risk, market risk, assets and liabilities, operating risk, and liquidity.

Committees make it difficult to achieve uniformity in methodology, measurements, or policy. The question becomes "Who, if anyone ensures that the agenda covers the most substantial risk exposures?" Nor is it clear who is accountable during the intervals between the committee meetings.

For example, in one U.S. investment bank, there is a separate unit that monitors credit risk and reports to the CFO, while another unit monitors market risk and reports to the CEO. Various operations throughout the bank incur risks and manage them separately. An executive management committee--representing business units, credit, finance, risk management, and legal and operational personnel—monitors asset and liability risks, risk concentrations, and model risks. This committee is charged with establishing reserves.

Organizational Models for Enterprise-Wide Risk Management

We have noted that financial institutions organize their risk management efforts in a variety of ways. The specific organization chart depends upon the company's strategic objectives and history, as well as the skills of the individuals involved. As important as objective standards are internal politics and who trusts whom. Accordingly, we have found that the authority and responsibility of the Chief Risk Officer vary dramatically from firm to firm. Nevertheless, the organization structure of the risk management function in most of the financial institutions that have designated a Chief Risk Officer can be classified according to one of the following models:

The financial risk model. The essence of this risk management model is the integration of financial risks only and the existence of a Chief Risk Officer to whom the market risk and credit risk functions report. However, the weakness of this approach is that responsibility for operational risks remains fragmented among various organizational units or, perhaps, is addressed by a separate committee. The risk management function typically focuses on risk policy, measurement, and analysis, but does not have the authority to approve exposures. Often there is a separate position for a Chief Credit Officer who approves limits and transactions.

At one money-center bank, a Chief Risk Officer heads a group that includes credit and market risk management. The group is charged with seeking ways to optimize the firm's risk-based return on capital. This group maintains a common risk management framework, establishes and controls market risk limits and credit risk concentrations, and oversees the allocation of balance sheet capacity and adherence to capital targets. The CRO chairs the risk management committee. Other committees include an operating risk committee, a liquidity risk committee, a capital committee, and an investment committee.

The all-risk model. The distinguishing characteristic of this model is a Chief Risk Officer who is responsible for the full gamut of the company's risks—including operational risks as well as credit and market risks.

Typically, the role is a consultative one. The Chief Risk Officer maintains awareness of risk issues throughout the organization, sets risk policy, measures risk, reports exposures, and proactively thinks about operational risk. He or she does not manage the back office, Information Technology, or other areas in which risks occur. Nor does he or she manage the control functions such as Legal and Internal Audit. All these risk-related areas do, however, have a dotted-line relationship with the Chief Risk Officer. Those who have the authority to take actual risks are in the business units, credit offices, and committees.

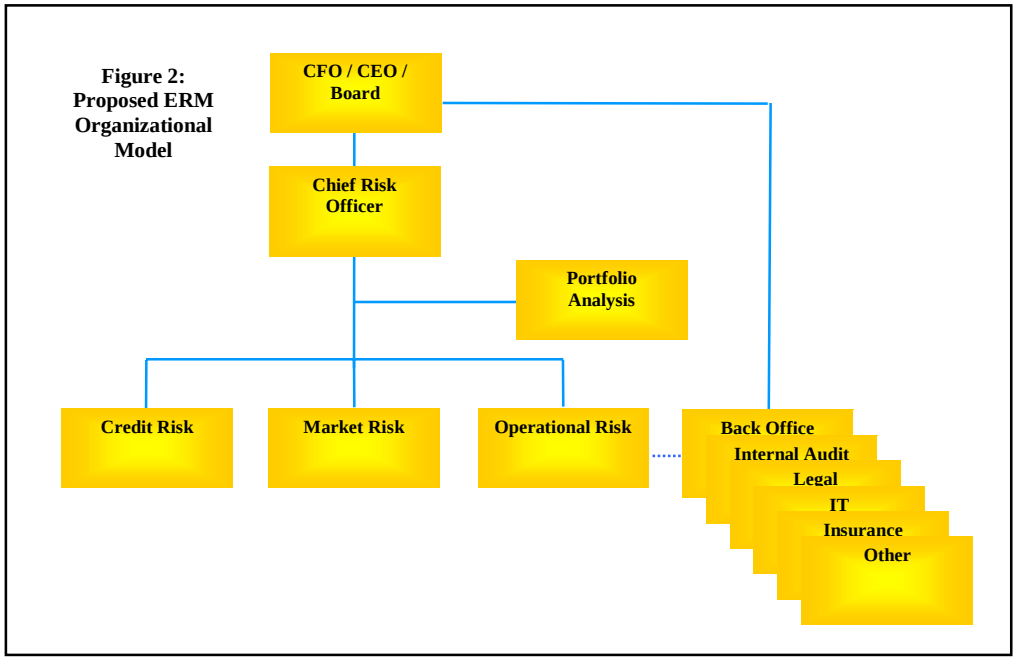
One investment management firm follows an all-risk approach in which one unit creates the risk framework and performs analysis and reporting functions across all business units. The Chief Risk Officer takes a consultative role, monitoring and reporting rather than making decisions or approvals. The Chief Risk Officer describes his role succinctly: "My job is to monitor and assess risk. Risk-taking decisions are in the business."

Like the other models, an all-risk approach can vary widely with the culture of the company and the talent that is available. In one money-center bank, for instance, a "Global Risk Management Group" performs analyses, sets risk-management methodologies, and reports on all types of risk. Outside of the group is a Chief Credit Officer who approves transactions and sets credit policy.

The risk governance model. An intriguing alternative to the all-risk approach is one that combines risk measurement with the related control functions under a single Chief Risk Officer. This approach is less consultative and more managerial. The Chief Risk Officer assumes a "watchdog" role and is responsible for Internal Audit and other compliance functions. The credit and market risk officers, who are responsible for approvals, work very closely with the Chief Risk Officer and may either be inside or outside the risk management structure.

A Proposed Model

Although there is no one approach that is suitable for all institutions, our proposed model can serve as a starting point for designing a risk management organization. Our proposed model is an outgrowth of the all-risk model, which is truly enterprise-wide since it integrates all the company's risks under a single Chief Risk Officer who can influence the firm's risk philosophy and strategy. Rather than cast the Chief Risk Officer in a "risk police" role, the all-risk approach is consultative.



Our proposed model adds to the all-risk model what we call a *risk portfolio analysis* function. The risk portfolio analysis group provides a staff that can address cross-risk issues such as integration of market and credit risk, allocation of capital, risk-adjusted performance measurement, and analysis of new products and/or acquisitions. The risk portfolio analysis staff gives the Chief Risk Officer the support he or she needs to be effective in coordinating the three major types of risk.

The measurement function is a central one for the portfolio analysis group. In a financial institution, capital is the logical means for quantifying and comparing risks. The portfolio analysis group can develop methodologies that consistently translate risks into dollar terms for all aspects of the company's business. It can proactively think about all the company's risks in an integrated way. It can perform "stress tests" in which extreme scenarios--such as a stock market crash or devaluation of a major currency--are examined, their implications assessed, and their effects mitigated in whatever degree is considered appropriate.

The proposed model establishes a Chief Risk Officer with close reporting ties to the CFO, the CEO, and the Board—ties that structurally facilitate the risk officer's input into risk-related decisions. The CRO may chair or be a member of various risk governance and approval committees, ranging from the assets and liabilities committee (ALCO) to the market risk, credit risk, and operational risk committees. Those who head the three major risk management disciplines report directly to the CRO. A multi-disciplinary approach is encouraged by dotted-line relationships to IT and to such control functions as Finance, Internal Audit, and Legal.

Implementation Issues

The proposed model is only a starting point. We fully expect that there will be variations in how the model is actually implemented in various organizations.

Interestingly, the key implementation issue is not to be seen on an organization chart. It hinges on how much authority and power are given to the Chief Risk Officer and other individuals. Let's assume, for example, that the CRO has straight-line responsibility for credit risk policy. Is the CRO also the Chief Credit Officer, does the Chief Credit Officer report to the CRO, or does a Chief Credit Officer report to someone else? One area that is particularly challenging is operational risk. Some of the business units and/or the relevant compliance units might actually report to the Chief Risk Officer, either in direct relationship or a dotted-line relationship. To empower the CRO in operational risk areas, there needs to be a staff to set policy and measure operational risk.

A company's decisions about authority, staff support, and reporting lines can determine the effectiveness of the Chief Risk Officer as well as the whole enterprise-wide risk management effort. Such decisions are based upon two basic factors: the background of the Chief Risk Officer and, more importantly perhaps, the degree to which he or she is trusted with various areas of responsibility.

Ultimately, the success of ERM depends heavily on such "soft' factors as people and culture. Much of the responsibility for managing risk falls to the Chief Risk Officer; however, cooperation from the company's business units is also critical. Since the CRO's role is consultative, the danger is that he or she may be in the precarious position of having considerable responsibility but no real authority. For the CRO to be truly effective, management must support him or her in disseminating a risk culture throughout the organization. In essence, the goal is for each employee to become a risk manager who can balance risk and return considerations in making daily business decisions.