By Craig Hughes

Managing **Enterprise Risk**

Few things have been made clearer in the midst of the current turmoil than the need for businesses to do a better job of managing risk. For banks in particular, if the market conditions have not made the point adequately clear, then the regulators and auditors will.

While most of us are looking forward to additional details of Treasury Secretary Timothy Geithner's planned regulatory overhaul to better understand what it all will mean for us, it is clear that the goal is stronger and more consistent regulatory oversight, with an even greater sense of accountability instilled within institutional leadership. Flawed though it may be, the Sarbanes-Oxley Act of 2002 (SOX) is here to stay, and there is ample evidence that even small and midsized privately held banks are beginning to accept the regulation's mandate for risk assessment and documented controls as best practices that all should follow.

For many in the mortgage industry for whom risk management has heretofore been limited largely to interest rates, hedging and credit, the notion of enterprise risk management (ERM) is relatively new and not particularly well-understood. (Not to mention the very fact that "enterprise" is largely viewed as jargon, with most banks much preferring to speak in terms like "cross-functional risk.")

This column addresses some of the concepts and tools of ERM, but space limitations preclude this serving as a primer on the subject. I would readily refer those looking for greater detail to seek out *Enterprise Risk Management—Integrated Framework,* a publication of the Committee of Sponsoring Organizations of the Altamonte Springs, Florida–based Treadway Commission (COSO), from September 2004, originally authored by New York–based Pricewaterhouse Coopers. It is available at www.coso.org.

COSO rightly recognized that the important first steps in managing cross-functional risks across the corporate enterprise needed to start with a common understanding of terminology and concepts, even if their application varied widely across organizations. Hence its initiation of an effort to create a common framework in 2001, the year before SOX became law.

Few things have been made clearer in the midst of the current turmoil than the need for businesses to do a better job of managing risk.

In the most basic terms, enterprise risks are those events that would negatively influence or constrain the organization's ability to achieve its strategic goals (including the most basic of goals, such as being profitable and returning value to stakeholders). Managing enterprise risk consists of identifying those risks, establishing well-defined controls to mitigate those risks in accordance with an articulated risk appetite, and monitoring the effectiveness of those controls.

Typically this is an iterative and ongoing process, striving for a spirit of continual improvement. SOX mandates that certain attributes of ERM (specifically SOX sections 404 and 302) be performed annually, but best practices would call for continual, frequent updates.

Key to the COSO ERM framework is a series of activities an organization follows to manage its risks. First, you must understand your internal environment (e.g., philosophy, culture, structure, risk appetite), then you must set your strategic objectives—two activities well-understood and followed by virtually every organization.

Next comes the identification of "events," meaning those factors, including both risks and opportunities, which influence the strategy and attainment of those objectives. These events are organized into related groupings or categories, and interdependencies are identified. Once the events are understood, the risks are assessed to determine likelihood and severity of impact, generally with weights and measures attributed to each such that a highly likely event of significant potential severity is seen as a much greater magnitude of threat than an event of low severity and likelihood.

The framework continues with an evaluation of possible responses to the events, followed by the articulation of controls aimed at mitigating the risks. Controls can vary from the general to those more specific to a department or function, and can be either preventative or detective in nature (designed to prohibit or merely to recognize the

occurrence of an event, respectively).

Finally, the series of risks and controls are documented and communicated so that they are understood throughout the organization, and the results are monitored. When controls fail to safeguard as intended, incidents of loss are documented and the controls are evaluated and improved as needed.

While this process may seem logical and intuitive, the real trick lies in the ability of the organization to really understand the variety of risks it faces and its interdependencies. An organization that is relatively immature in assessing risk may be capable of detailing a few dozen across the enterprise, while a more seasoned or complex organization may recognize hundreds and a single risk may well have several controls associated with it.

Given the complexity of performing this increasingly critical process, it is not surprising that a new breed of technology has emerged to assist companies throughout the framework. ERM systems, sometimes broadened to incorporate the whole of governance, risk management and compliance (GRC), typically provide the ability to catalog risks within risk categories, attribute weights and measures, associate them with business functions within the organization and link controls to them.

Most support SOX provisions by giving senior executives the ability to electronically certify the process and effectiveness of controls, as well as providing dashboards and reports to monitor progress. More sophisticated offerings allow for capturing loss incidents, track projects related to control remediation and perform detailed trend-analysis monitoring performance over time. Some even combine workflow engines and document repositories to more fully incorporate the SOX 404 documentation requirements.

ERM systems have emerged to support banks along the entire spectrum of sophistication and complexity. Market leaders offer robust and feature-rich tool suites that cover the full GRC range that appeal strongly to larger organizations; included in this tier are systems from Cokato, Minnesota–based Paisley, a Thomson Reuters company; Palo Alto, California–based MetricStream Inc.; and Waltham, Massachusetts–based OpenPages Inc. Examples of competing systems include two that grew out of the project experience of leading risk-management consultancies—Menlo Park, California–based Robert Half International's subsidiary Protiviti Inc.'s Governance Portal; and Emeryville, California–based LECG LLC's Washington, D.C.–based subsidiary Secura Group's confERM (Consolidated Financial Enterprise Risk Manager) (developed in partnership with CC Pace).

The need to manage risk is critical, regulatory pressure to do so is clearly on the upswing, and a variety of tools exist to help you with the process. If that isn't compelling enough to move you to action, feel free to sit back and do nothing. Your auditor will be stopping by soon enough.

Craig Hughes is the vice president in charge of mortgage consulting at CC Pace, a nationally known financial services consulting company based in Fairfax, Virginia. He can be reached at craig.hughes@ccpace.com.