ABA Banking Journal
April 2013

Regulators raise the risk bar—big time!

Seven themes mark a renewed and greater emphasis on enterprise risk management—and everyone's invited to this party

By David Gibbons and Kathryn Dick, Promontory Financial Group

The global banking crisis began five years ago, and policymakers and companies are still debating the steps necessary to prevent the next one. Many conversations are loud and contentious—consider the ongoing Dodd-Frank implementation—but prudential regulators are using more subtle methods to convey lessons learned. They are using the discreet power of supervisory programs to elevate risk-management standards—most notably for large and mid-sized banks, though inevitably the impact will be felt by community banks. In doing so, regulators have set the long-term direction of bank supervision. The task bank executives and directors face in meeting regulators' heightened expectations also is becoming clearer.

"The OCC is very much focused on improving its supervision programs and absorbing the lessons we learned from the financial crisis," Comptroller of the Currency Thomas J. Curry told bankers last November. "We are no longer willing to accept audit and risk-management functions that are simply satisfactory. We are looking for excellence." Other senior supervisors have echoed his comments in recent months.

Such supervisory emphasis implies change for each of the traditional three lines of defense in risk management: 1. business units; 2. risk management and compliance; and 3. independent review functions (including the internal audit, credit-risk review, and model validation functions, among others). Heightened expectations also imply less tolerance for shortcomings, with swifter, harsher sanctions for those who fail to keep pace.

Next stage in risk-management evolution

Supervisors have, for years, pushed more demanding risk-management and measurement standards to support Basel II requirements, particularly in technology, data management, modeling, and risk-assessment methodologies. They also expected a comprehensive approach to the less quantitative attributes of enterprise risk management. But the emphasis on specific risk-management supervisory standards did not emerge in earnest until 2009. The Senior Supervisors Group released *Risk Management Lessons from the Global Banking Crisis of 2008*, definitively cataloging gaps in many banks' programs.

The study galvanized supervisors' insistence on excellence in risk management, and banks, including foreign banking organizations with significant U.S. operations, continue to feel their steady push. This pressure drives a broad reconsideration of all aspects of enterprise risk management: appropriate governance and organizational structure; stature of the function itself and its independence within the organization; expertise and talent of key risk-management staff; clarity and effectiveness of risk-appetite statements, tolerances, and limits; and defined expectations of independent review functions.

While large and mid-sized banks must look hard at enterprise risk management, community banks are well advised to do so, too. Regulatory history tells us that as supervisors reap new knowledge of best practices, the lessons will eventually be applied to smaller banks—though regulators will likely afford smaller banks more flexibility of application.

Expectations rise

Through reviews and examinations, supervisors have made it clear that they view enterprise risk management; capital and liquidity planning and management; and stress testing as interdependent disciplines, with none operating in isolation and all informing each other. Stress testing, for instance, should guide the establishment of risk appetites and measure capital and liquidity adequacy under adverse and severe business conditions. A weakness in one area can potentially render others flawed, with potentially negative effects on supervisory rating assessments, particularly the management rating for banks and thrifts and the risk-management ratings for bank holding companies.

Regulators expect every large bank to have a risk roadmap supported by credible enterprise-wide programs that adjust to changing business conditions. If, for instance, a bank testing capital and liquidity under stressed conditions finds shortcomings, the bank should respond through concrete actions to mitigate risk and, possibly, raise capital and improve liquidity. Indeed, regulators will not depend entirely on a bank's calculations, and will apply their own stresses to capital and liquidity plans, as well as look for meaningful variances against stated risk appetites. These are steps that institutions should view as preemptive application of prompt corrective action and early remediation requirements.

The collective goal now is to put *sharper teeth* into risk management

Some of the supervisors' new risk-management imperatives have been or will be codified in rulemakings. Others are being communicated through supervisory guidance and, more specifically, through the examination process. The collective goal is to put sharper teeth into risk management.

Before the crisis, these functions all too frequently looked good on the surface, but had limited authority and little support within their organizations. They were often constrained by too few resources and too little expertise.

Without the benefit of comparable information across various business lines—and with an even weaker perspective on how risks could spread throughout the enterprise—they were essentially flying blind. Prudential regulators are pressing seven key themes as they compel banks to fix weaknesses and push risk-management ratings from satisfactory to strong.

Theme 1: Board and risk committee governance

Heightened expectations extend to board members and board risk committees—traditionally the top of the governance pyramid. Members of boards and risk committees are expected to take an active and informed role in assessing institutional risks and the overall efficacy of the institution's risk-management and independent control functions, including internal audit, credit-risk review, and model validation. Boards should:

• Participate in the determination and formal approval of

risk appetites, tolerances, and limits.
- Approve key risk policies, including those governing credit, markets, liquidity, and capital.
- Monitor major strategies and initiatives producing risk.
- Influence behavior through informed and credible challenging of management.
- Oversee the institution's risk-management program.

It's not easy. These expectations increasingly require board members to have a clear understanding of critical risk-management issues. As a result, they need to require better quality, clarity, and candor in the risk and business data that management provides. Mechanisms to accomplish this include board and risk-committee meetings in executive session—that is, without management present. And provision must be made to "show their work"—and documentation of how boards and board risk committees are fulfilling their responsibilities.

No rubber stamps are accepted anymore: Supervisors expect board and committee members to pose informed and credible challenges to management. They expect familiarity with the word "no." *They expect board members to show little or no tolerance for undesirable behavior.*

Theme 2: Independence

Supervisors expect risk and risk-review functions to be independent in form and substance. Risk-management functions are expected to set ground rules for risk taking, and to ensure appropriate risk measurement, monitoring, and reporting activities and protocols. Independent risk-review groups (audit, credit review, and model validation, among others) are increasingly recognized as *policing* functions. Supervisors frown on thinking of these functions as "business partners" or "consultants."

The chief risk officer (CRO) should report her findings directly to the board's risk committee, similar to the role of internal audit. In this way, the CRO has unfettered access and communications with those who can *demand* better risk controls and influence the institution's reaction to existing or developing risks. Directly reporting findings also typically makes it easier for risk functions to secure the resources they need, including appropriate staffing, expertise, and depth, as well as IT and systems support to identify, measure, monitor, report, and manage the risks of the institution.

Regulators expect independent directors to chair board risk committees, and may *require* it through rulemaking. For smaller banks without board-level risk committees, the key is to ensure the board has appropriate data to assess the organization's risk-management capabilities.

Theme 3: Stature of risk and risk-control functions

Requiring the CRO and heads of independent review functions to report directly to the board emphasizes the importance and stature of their roles. But here, too, regulators expect much more than a reporting line and prime positioning on an organization chart. They will look for explicit and implicit support of risk-management and independent review functions by the board, CEO, and other members of executive management. They want to see evidence of such support in institutional culture, "tone at the top," and in action.

The CRO and staff need to be at the table when strategies are formulated, and in the early stages of product and process development. The purpose: to give the best chance at identifying and quantifying potential risks, and to take action that will control, mitigate, or avoid them outright. The stature and effectiveness of the function suffers if it is brought in at the last minute, or after the fact, when strategies and tactics have already been set.

Regulators also expect the risk function's views will be actively sought and used in compensation and performance-management decisions, and the CRO and staff have the expertise and leadership within and among the businesses to command respect and further build the function's stature within the organization.

Theme 4: Management

The "three lines of defense" risk-management model requires that business lines own, identify, and manage their risks. Supervisors increasingly evaluate the competence of business-line leadership and staff in implementing proactive, self-regulating, risk-management and control infrastructures appropriate to the risks their businesses assume. These evaluations also explore whether the expertise is deep, and whether organizations have succession plans in place to guarantee the risk-management discipline remains vigorous.

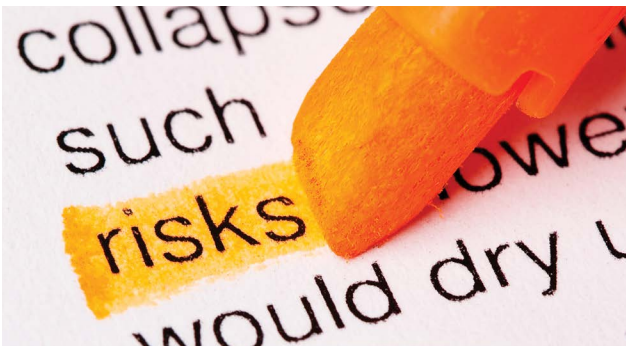

PHOTO: AARON AMAT/SHUTTERSTOCK.COM

Business units, in most cases, are expected to identify their own risks rather than rely on dedicated risk and control functions, or regulators. Supervisors increasingly assess the strength of key risk indicators and risk self-assessments, and their effectiveness in measuring risks and supporting management in staying on top of trends.

Exercises in neat manuals gathering dust are *out*. Practical application is *in*. Regulators expect that early-warning metrics will drive business decisions.

Business-line responsibilities also include risk and issue resolution, with governance and oversight by the

risk and control functions, as well as the board. Regulators are looking for clear accountability for risk and control issue resolution, and for active triaging, progress tracking, and reporting. And they want to see evidence that business units are held accountable for the risks they incur and how they handle them.

Regulators also will expect to see evidence from the board of a low tolerance for inadequate resolution and for recurring risks.

Theme 5: Management and board reporting

Management information systems and reports to executive management and boards are increasingly expected to be an "early warning," rather than merely recognition of what has already happened.

Supervisors are pressing for risk-management information and reporting that:

- Use forward-looking measures, including key risk indicators and performance testing under stressed conditions.
- Measure the risk implications of external and internal operating conditions and events.
- Identify trends in risk levels relative to plans and expectations, and to earnings and capital.
- Gauge compliance with key limits and potential drift from stated risk appetites.
- Analyze information so that executive management and boards understand the risks and their potential implications well enough to inform their governance and oversight.

Supervisors are not likely to be sympathetic to technology and data challenges that compromise effective management information systems and analysis.

Theme 6: Independent review functions

Independent review functions, such as internal audit and credit review, continue to be viewed, and will need to act, as policing mechanisms for risks and risk controls, as well as for overall risk-management programs and processes.

Increasingly, regulators are calling on these functions not only to assess adherence to policies and procedures, but also to assess the propriety of these risk and control mechanisms: An audit or credit-review function that renders an opinion on management's compliance with a policy also is expected to render an opinion about the policy itself. That is a substantially higher hurdle than formerly accepted practices, which were seen as too frequently designed to be consultative and more or less agnostic as to the sensibility and prudence of risks and risk controls. *These functions now have a mandate to demand and instigate change.*

Theme 7: Stress testing

The Senior Supervisors Group study focused on institutions' overreliance on trailing measures of risk as a particularly crucial flaw that enabled the banking crisis. That problem has been addressed through required stress testing for all banks, thrifts, and their holding companies with greater than $10 billion of assets; those with greater than $50 billion have already implemented stress testing in conjunction with required annual capital plans. Stress testing is not new—mandating its use in risk-management and capital-adequacy assessment *is*.

Strong planning and risk oversight practices can help improve supervisory ratings

The application of stress-testing also is expanding, and is increasingly expected to inform risk-appetite and risk-mitigation decisions beyond the capital-adequacy context. Many firms are not only using stress testing to improve how the enterprise risk-management function anticipates emerging threats, but also to help risk managers develop additional early-warning tools that safeguard assets.

While supervisors have afforded smaller banks more flexibility in the application of stress testing, they clearly are expecting smaller banks to consider the downside effects of stresses on concentrated credit portfolios and asset classes on capital and liquidity adequacy.

What's over the horizon

More, along the lines of what's written here, is coming. In the months ahead, we expect each of the regulatory agencies to begin issuing rules, regulations, and guidance, incorporating heightened supervisory expectations, particularly with respect to governance, risk management, internal audit, and stress testing.

These issuances, along with other supervisory guidance, will memorialize expectations that regulators have communicated formally and informally in the past few years, as they have digested lessons learned. Banking companies that adopt strong and sustainable business-planning and risk-oversight processes and practices will be best positioned to secure improvements in their supervisory ratings. ▯

David Gibbons and Kathryn Dick are managing directors at Promontory. Gibbons advises clients on regulatory and compliance matters, and specializes in enterprise-risk and credit-management issues. Dick advises clients on a wide range of regulatory and supervisory issues, governance and risk-management challenges, systemic-risk issues, and complex credit and capital-markets activities.