THE KORN/FERRY INSTITUTE

PROMONTORY

New risk rules pose big changes for financial services

By David D. Gibbons and John E. Petzold

March 2012

New rules proposed by the Federal Reserve Board of Governors to remedy causes of the financial crisis include very specific prescriptions for risk oversight, including increased stature for the CRO, ensuring independence for the role, and requiring expertise on the board's risk committee.

Buried deep in a new 172-page rule from the Federal Reserve Board of Governors (FRB) are seven pages that could redefine the role of the chief risk officer (CRO) and risk committees at large financial institutions. Published for comment January 5 by the FRB, the Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies (12 C.F.R. 252) sets out very specific and prescriptive requirements to repair perceived failures in independence, stature, and expertise that the FRB believes contributed to the financial crisis.

All aspects of the FRB's proposed rule—which addresses a multitude of topics, including liquidity, stress-testing, and enterprise risk management—deserve serious consideration. But the purpose of this alert is to focus attention on what it might mean for regulation to dictate independence, stature, and expertise, which are among the most fundamental principles of effective risk management. At financial institutions with $10 billion or more in assets, particularly "covered companies,[1]" these proposed changes could have notable repercussions for chief executive officers (CEOs), CROs, lead directors, and those who head human resources.

[1]A "covered company" includes any bank holding company with $50 billion or more in total consolidated assets, and any foreign bank or company that is treated as a bank holding company under section 8(a) of the International Banking Act of 1978 and has $50 billion or more in total consolidated assets, and any nonbank financial company that under section 113 of Dodd-Frank must be supervised by the board.

Parts of the proposed rule are applicable only to covered companies; others are applicable to all publicly traded bank holding companies with $10 billion or more in assets. While the rule sets the bar somewhat higher for financial services companies above $50 billion in total assets ("covered companies"), in the past we've seen regulatory expectations migrate, and be applied in practice, to the rest of the rule's constituents.

As currently written, the rule's formal requirements, and its spirit and intent, have considerable implications in a number of areas, first in the area of risk committee operations and membership:

- Each publicly traded bank holding company with assets of more than $10 billion is required to establish a risk committee of the board of directors to document and oversee, on an enterprise-wide basis, the risk management practices of the company.
- Risk committees must be chaired by an independent director.
- At least one member of the risk committee must have risk management expertise that is commensurate with the company's capital structure, risk profile, complexity, activities, size, and other appropriate risk-related factors, and also should have experience developing and applying risk management practices and procedures, measuring and identifying risks, and monitoring and testing risk controls with respect to banking organizations (or, if applicable, nonbank financial companies).
- Risk committees must have a formal, written charter that is approved by the company's board of directors.
- Risk committees must meet regularly and as needed.
- Companies must fully document and maintain records of risk committee meeting proceedings, including risk management decisions.
- At covered companies, the risk committee must be a standalone committee that reports directly to the full board, and may not be housed within another committee or be part of a joint committee.

Other aspects of the proposed rules will affect risk management programs in general and the recruitment, selection, and compensation of CROs and their support staff:

- Each covered company must appoint a CRO to implement and maintain appropriate enterprise-wide risk management practices.
- The CRO is required to have risk management expertise that is commensurate with the covered company's capital structure, risk profile, complexity, activities, size, and other appropriate risk-related factors.
- The CRO must report to the risk committee and to the covered company's CEO.
- The compensation of a covered company's CRO must be appropriately structured to provide for an objective assessment of the risks taken by the covered company.

What is clear is that the FRB strongly believes that failings by CROs and inadequate risk functions contributed to the financial crisis, and so it has decided to regulate the meaning of "independence," "stature," and "expertise." Whether the FRB's tack is correct will surely be the subject of much debate and comment among the affected constituencies. That said, the spirit and intent of the FRB's proposed rule is quite reasonable.

Stature: embedding genuine support

Independence, stature, and expertise are prerequisites for successful risk management, and experience has shown that the first two historically have existed more in form than substance. Postmortem reviews of financial institutions' organization charts show that in the pre-crisis world, most CROs occupied senior roles and were detached from their companies' business and risk-taking functions. However, there were other aspects of independence and stature, apart from reporting lines or position on an organization chart, that may have undermined their effectiveness. For example, many CEOs and business leaders were vigorous supporters of sound and strong risk management—unless it meant slowing revenue

growth, incurring higher expenses, or stopping a deal. Other CEOs window-dressed the issue, making the CRO the leader of an office of enterprise risk management, a coordinator without stature, authority, or expertise. Such responses fly in the face of best practices. The CRO and the risk management function cannot thrive without the full support of the CEO and board. Such support should be reflected in the company culture.

When genuine support for risk management is embedded in an organization, good things start to happen. The CRO, and by extension his or her staff, are "at the table" when strategies, products, or processes are being developed. The board and the CEO articulate that this is their expectation. Significant new product, process, or business strategies are no longer presented to the risk team at the last minute. There is no tolerance for circumventing risk processes and no expectation of a rubber-stamp approval. The stature of risk management is elevated, and it supports the business lines' effectiveness.

Finally, the CRO's stature is enhanced by having input into the compensation of business leaders. Goals given to business leaders should be shaped, in part, by risk parameters and desired risk-related behaviors. The CRO should have input into what those parameters are, if not into how well they were met.

Independence: beyond reporting lines

As for independence, there are a number of important aspects to be considered beyond mere reporting lines. Like an internal auditor, the CRO needs to have authority to get whatever information, cooperation, or resources are needed to ensure that risks are identified and adequately managed. That demands unfettered access to the board or a committee thereof. Those who would argue that a CRO does not need the kind of independence afforded a chief auditor should consider that a CRO may need to adjust the behavior of the CEO, or the CEO's latest golden boy or girl. Only the board, or board members, can truly intervene with the CEO if the CRO's message goes unheeded.

Other influences related to CRO independence that may have shaped the FRB approach to the proposed rule are a general lack of resources dedicated to risk, including sufficient numbers and qualifications of staff, IT and systems support, etc. Risk organizations do not generate revenue and, as a result, are often low priorities for resources, or targets for cost-saving. Director involvement may well be needed to secure and/or protect the resources necessary to ensure effective risk management. At the end of the day, CRO independence requires two things: that what needs to be said is heard, and that what needs to be done can get done.

Expertise: more blurring than clarity

The proposed FRB rule seems on the surface to be relatively straightforward on the matter of expertise. Those responsible for risk, whether at the board or management level, need to have risk expertise appropriate to the kind of risks that the firm takes, and on the scale at which the firm takes its risks. At least one member of the board's risk committee should have managed the types of risk that the firm takes.

What talent profile will fit the FRB bill?

The existing talent pool in the CRO function is extremely varied in terms of both stature and expertise.

In many cases, the financial services industry has forced a specialization around credit, market, and operational risk for its most senior executives. Many of the sitting CROs, then, have come up from within a singular risk discipline and drafted a strong supporting cast around them. But will this prove satisfactory given the FRB's hardened parameters?

In other cases, where banks' risk functions have matured at a faster rate, they already have well-rounded enterprise CROs with experience in all areas of credit, market, and operational risk. However, the FRB seems to think even this structure has had its downfalls given the state of the industry.

Finally, some organizations have appointed (and may continue to appoint) senior general managers and business leaders into the CRO role. These executives will have taken risk as a business person—most likely having some bumps and bruises along the way. These executives may also have had the C-suite exposure and gravitas expected to drive through a difficult transformational agenda. That being said, the FRB mandate seems to highlight the fact that this first line of defense business risk management has failed in the past as well.

While these are not novel talent ideas, the arrival of a regulatory mandate around the selection and background of such talent is. There are multiple examples of failed enterprise-wide CROs, or business leaders turned CROs—so it remains to be seen which, if any, will prove a panacea.

But it's more complicated than that. The proposed rule has serious ramifications for governance, talent management, and recruiting, at both the board and management levels. Clarity around roles and responsibilities is also blurred. Among the challenges and potential implications of the proposed rule:

Who owns risk? The requirement that at least one member of the risk committee have essentially the same qualifications, expertise, and experience in managing risk, and applying risk management programs and practices, as the CRO could easily lead to confusion about who is actually responsible and accountable for managing the risk of the institution. It could blur lines between traditional board oversight responsibilities and managerial responsibilities.

Doubling demand for CRO experience. This same requirement will make recruiting risk committee members more difficult, as each institution will now need two people with CRO qualifications, and the talent pool is already limited.

Committee assignments: Given the importance of the risk committee, and its natural linkage to the audit and compensation committees, the rule may require, indirectly, that the risk expert also serve on those committees as well. This will have implications for director workload, recruiting, and director compensation.

Must the risk committee handle all risk? The proposed requirement that all things risk must be governed by the risk committee may conflict with some existing governance structures, where some risk matters are handled by other committees. Often compliance and operating risk are handled by audit committees, for instance. Does the rule mean to imply that these structures are no longer acceptable?

Expertise qualifications. The proposed rule seems to imply that the board's risk committee expert and the CRO must have experience in all aspects of risk management equal to the risks in the institution. Is this meant to imply that if a banking company's risks are evenly spread between credit, market, and operating risks, both the board risk committee member and the CRO will need to be equally qualified in assessing and applying risk management

techniques to each of those risks? If so, there may be no way to fill these roles in an industry that, over many years, has evolved toward specialized knowledge and skills (credit, markets, compliance, operating risk, IT risk, etc.). Could some companies have to replace their board risk committee experts or CROs if they do not meet the letter of these standards?

Experience requirements. The proposed rule is vague around the risk management expertise and experience in applying risk management programs required of at least one board risk committee member and the CRO. Does that mean only those people who have worked in traditional "second-line of defense" risk management units? What about business leaders who have managed the risk in their businesses? If the former, the talent pool is likely to be diminished further.

Who manages the CRO? The requirement that the CRO have a dual reporting line to the risk committee and the CEO may well cause confusion. Is each half responsible for the management of the CRO, including goals, performance assessment, compensation, and administration matters such as the budget for risk?

During the twelve months leading up to the release of the FRB's proposed regulatory changes, several top-20 U.S. banks made changes at the CRO seat. While some institutions have made traditional hiring decisions—that is to say, appointing an executive with a credit, market, or operational risk background that matches the profile of the company—others have appointed senior business leaders and seasoned general managers to the role. The success of these different CRO profiles will become clearer as time progresses. But long before then, the regulatory dust will settle, and each organization's board and CEO will have to take a hard look in the mirror to determine if its structure and leadership will pass muster with the FRB.

David D. Gibbons is a managing director at Promontory Financial Group. His specialties include credit and enterprise risk management issues, such as processes and controls, and financial and risk management assessment. He also handles troubled institution resolution, designs and implements turnaround strategies, and performs portfolio due diligence reviews.
dgibbons@promontory.com

John E. Petzold is a Principal at Korn/Ferry International, and a member of the Firm's Global Financial Market and its Risk Management Center of Expertise. Petzold, based in New York, advises financial services firms on talent solutions in all areas of credit, market, and operational risk, as well as at the level of enterprise chief risk officer.
john.petzold@kornferry.com

About Promontory Financial Group

Promontory is a leading strategy, risk management, and regulatory compliance consulting firm for the financial services industry. Promontory's professionals have deep and varied expertise gained through decades of experience as senior leaders of regulatory bodies and financial institutions. Promontory assists clients in meeting regulatory requirements and in enhancing governance, risk management, strategic plans, and compliance programs.

About The Korn/Ferry Institute

The Korn/Ferry Institute generates forward-thinking research and viewpoints that illuminate how talent advances business strategy. Since its founding in 2008, the institute has published scores of articles, studies, and books that explore global best practices in organizational leadership and human capital development.

About Korn/Ferry International

Korn/Ferry International, with a presence throughout the Americas, Asia Pacific, Europe, the Middle East, and Africa, is a premier global provider of talent management solutions. Based in Los Angeles, the firm delivers an array of solutions that help clients to attract, engage, develop, and retain their talent.

Visit www.kornferry.com for more information on the Korn/Ferry International family of companies, and www.kornferryinstitute.com for thought leadership, intellectual property, and research.