

My Perspective



JOHN DUGAN

Partner, Covington & Burling

John C. Dugan, formerly Comptroller of the Currency from 2005-10, is a partner in the firm's Washington, D.C. office and chairs the firm's Financial Institutions Group. He advises clients on a range of legal matters affected by significantly increased regulatory requirements resulting from the financial crisis, including: implementation of the Dodd-Frank Act.

As Comptroller, Mr. Dugan led the Office of the Comptroller of the Currency (OCC) through the financial crisis and ensuing recession that resulted in extraordinary regulatory and supervisory actions for national banks of all sizes, including government assistance provided under the Troubled Asset Relief Program (TARP); resolutions of large, mid-size, and community banks; and the successful implementation of regulatory "stress tests." Before serving as Comptroller, Mr. Dugan was a partner in the firm, specializing in financial institution regulatory matters from 1993-2005. He had previously served at the U.S. Department of the Treasury from 1989 to 1993, where he was appointed Assistant Secretary for Domestic Finance.

From 1985 to 1989, Mr. Dugan was Counsel and Minority General Counsel for the U.S. Senate Committee on Banking, Housing, and Urban Affairs, an active period during which the Committee passed the Competitive Equality Banking Act of 1987; the Proxmire Financial Modernization Act of 1988; and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989.

The OCC's Guidelines for Risk Management and Governance: First-of-Its-Kind Enforceable Standards of General Application

On September 11, 2014, the Office of the Comptroller of the Currency ("OCC") finalized its proposal to establish "Heightened Standards" for risk management and governance applicable to the largest national banks, federal savings associations, and insured federal branches of foreign banks ("covered banks"). This ambitious set of enforceable standards (the "Guidelines") is the result of the OCC's scrutiny of risk management and governance concerns that emerged during the financial crisis; its groundbreaking efforts to articulate generally applicable principles to address these concerns; and its calibrated but meaningful response to a robust set of industry comments—by The Clearing House and others—on the initially proposed version of the Guidelines.

I believe the final Guidelines are important not simply because they will require covered banks to meet a new set of generally applicable risk management and governance standards that will facilitate consistency and supervisory "benchmarking." They are also likely to establish an important precedent that other regulators, both in the United States and other countries, will look to as they articulate their own versions of enforceable standards applicable to risk management and governance.

I want to emphasize that the new standards have been issued as guidelines, not regulations. That is critically important. While the OCC has made clear that the Guidelines are enforceable and will be enforced, it has also made clear that implementation of the standards requires more flexibility to recognize legitimate differences in risk management frameworks than would be the case with more detailed, prescriptive, and rigid regulations. That is a wise approach, because this is a very new effort to translate a wide range of legitimate practices and approaches to the risk management of some very different businesses into a common language and a common set of principles. Indeed, I believe this is really the very beginning of a process that will require close consultation with each institution's supervisors on the ground to implement the Guidelines in a manner that is true to their goals, while at the same time recognizing that there can be different ways to achieve those goals in different organizations. The Guidelines expressly and appropriately embrace in a number of places this need for consultation, flexibility, and discretion. And given the "newness" of this effort, it would be very helpful for the agency to issue periodic interpretive guidance based on its implementation experience and the inevitable questions that will be raised.

Three Key Goals of the Guidelines

In the wake of the financial crisis, the OCC identified three key concerns

regarding risk management and governance at some, but not all, covered banks:

Lack of a Distinct Risk Management Framework for the Bank. For years, most large banking organizations have designed their risk management frameworks to focus on lines of business of the overall organization rather than on separate legal entities. In some cases the OCC became concerned that a covered bank was being used more as a shell or “booking entity” than as a distinct operating company, unduly exposing the bank to risks posed by its holding company or nonbanking affiliates.

Weaknesses in Bank Director Oversight. The agency believes that, in too many cases, boards of a national bank did not have adequate focus on the risk management issues of the bank as opposed to its holding company, and that its oversight was not as robust as it should have been.

Weakness in the Bank’s Risk Management Framework. The agency concluded that some banks were considerably more successful than others in adopting and implementing a robust risk management framework that provided adequate protection to the covered bank.

The OCC first sought to address these concerns through its informal supervisory process, communicating a set of “heightened expectations” regarding banks’ risk management and governance frameworks. Over time, however, the agency became convinced that it was important to tackle the very difficult task of translating these supervisory expectations into generally applicable, legally enforceable

standards that would lead to more effective, transparent, and consistent implementation. The Guidelines are the result, and they address each of the three concerns as described below.

Distinct Risk Management Framework for the Bank

The Guidelines establish the straightforward general principle that a covered bank must have a risk management framework that is its own—separately identifiable from its holding company’s framework. But two very important exceptions apply.



No agency has previously attempted to translate more general risk management supervisory principles into such granular and enforceable standards.

First, if the covered bank and its holding company are really “substantially the same” organization, then the bank can use its parent company’s risk management framework—so long as that framework itself satisfies the Guidelines. Perhaps not surprisingly, the Guidelines are very conservative regarding the type of organization that will satisfy the “substantially the same” test: in general, either the bank must constitute 95 percent of the assets of the holding company, or the

organization must persuade its supervisors that they should view the risk management frameworks of the bank and its parent as one and the same—which may not be easy to do.

Second, for the substantial majority of covered banks that are unlikely to satisfy the “substantially the same” test, the Guidelines make clear that it will be possible for the bank to “leverage” certain elements of its parent company’s risk management framework without having to recreate them at the bank level—so long as the bank consults with and receives the approval of its supervisors to do so. This exception is critical. In the preamble to the final

Guidelines, the OCC expressly stated that, though it did intend for a bank to have a separately identifiable risk management framework, it did **not** intend for the bank to always have an entirely distinct framework with entirely separate management, systems, audit, etc. Indeed, it made clear that “dual hatting” of chief risk executives and chief audit executives is permissible and potentially desirable, depending on the circumstances. And it made clear that the Guidelines will permit a covered bank to

use components of its parent company's risk governance framework that are appropriate for the bank, for example, where there is similarity between the bank's and the parent company's risk profiles. The key will be to consult with an institution's examiners to determine where it is appropriate to leverage an aspect of the parent company's framework—a prime example of the type of discretion and flexibility that the Guidelines permit.



While the standards are plainly intended to be prescriptive, they are not intended to be so prescriptive as to apply a “one-size-fits-all” straitjacket to every aspect of risk management.

Enhanced Director Oversight

The Guidelines address the OCC's concerns about bank director engagement by requiring a covered bank's board to, among other things:

- require bank management to establish and implement an effective risk management framework for the bank;
- provide active oversight of bank management;
- exercise independent judgment;

- include at least two board members who are independent from management using criteria for independence that are the same as that used in a recent Federal Reserve Board regulation;
- provide ongoing training to all directors; and
- conduct an annual self-assessment that includes an evaluation of the board's

effectiveness in meeting the director standards set forth in the guidelines.

Importantly, the final Guidelines reflect modifications in a number of places to address strong concerns raised by The Clearing House and many others that the proposed Guidelines risked creating strict liability for directors, and would impose new fiduciary duties on directors and potentially modify existing ones. In addition, while the final Guidelines make clear that director oversight should be strengthened, they also recognize that the board's role is not to engage in management activities; for example, the proposed requirement for extensive

board involvement in human resources development, recruitment, and succession planning was substantially scaled back.

Risk Management Framework and the “Three Lines of Defense”

Finally, I think the most challenging aspect of the Guidelines is its set of provisions that attempts to establish a generally applicable risk management framework applicable to all covered banks. While firms have appropriately devoted a great deal of resources to developing robust management frameworks, business models are different and approaches to risk management have also been different. The OCC and other regulators have historically permitted a great deal of diversity in such frameworks, so long as key risks were appropriately measured, monitored, and controlled. As a result, different firms have often had different definitions of roles, responsibilities, and reporting relationships for the “three lines of defense” that are often used to describe risk management frameworks: frontline units; independent risk management; and internal audit. And different firms have employed varying degrees of specificity in articulating and documenting such things as risk appetites and risk limits.

In the wake of the financial crisis and the obvious risk management breakdowns at some firms, regulatory bodies around the world have begun to feel the need to develop a better set of generally applicable principles that can be applied to the largest firms to facilitate risk management that is stronger, more consistent, and more easily measured and monitored. The Guidelines

are the OCC's effort to do this, but unlike some earlier efforts, they are intended to be more prescriptive in their application, with a more detailed set of general requirements, definitions, and common terminology setting a baseline for minimum supervisory expectations. This has been hard, precisely because of the heterogeneous nature of risk management frameworks, including differences in very effective frameworks. It is also very consequential, because no agency has previously attempted to translate more general risk management supervisory principles into such granular and enforceable standards; what the OCC does here with respect to the risk management frameworks for covered banks could set an important precedent for supervisors of other banks and financial firms, both in the U.S. and abroad.

That is why I believe it is so important that the new risk management framework has been articulated in the form of guidelines rather than regulations, and that the agency has indicated that certain differences in approach will be permitted in consultation with an institution's examiners. While the standards are plainly intended to be prescriptive, they are not intended to be so prescriptive as to apply a "one-size-fits-all" straitjacket to every aspect of risk management. For example, different reporting relationships appear to be permitted, such as the compliance function reporting to either the general counsel or independent risk management.

Likewise, in response to a number of comments on the proposed Guidelines, the final Guidelines make clear that certain company functions may not neatly fall completely—or at all—into one of the three lines of defense. Legal and human

resources, for example, would generally not fall in these boxes, and other units might have parts fall in one or more of them depending on the nature of a particular activity carried out by a business unit. Thus, finance would be in the front line to the extent it makes decisions about cutting other units' expenses in ways that could



Even with a new set of common principles, standards, and terms, discretion and judgment will be required to recognize legitimate idiosyncratic differences among firms.

increase exposure to risk, but in the second line of independent risk management to the extent it exercises a control function in the financial reporting process. Likewise, compliance could fall in all three lines of defense to the extent its activities are focused on individual line of business risks, aggregate risk, or testing activities associated with audit.

The point is that, even with a new set of common principles, standards, and terms, discretion and judgment will be required to recognize legitimate idiosyncratic differences among firms in order to promote the fundamental goal of effective risk management. These qualities will also be required to answer the many inevitable questions that will arise (and have already arisen) with respect to the implementation

of a such a consequential new regulatory regime. The Guidelines afford such flexibility, and covered banks should work closely with their examiners to ensure that such discretion and judgment are exercised wisely. In addition, periodic interpretive guidance from the OCC would be most welcome.

The Heightened Standards Guidelines are a very important milestone in post financial crisis supervision and regulation, but their evolution as an effective tool will depend on thoughtful adjustments and fine-tuning over time based on implementation experience. ■