Regulatory brief

February 2014

A publication of PwC's financial services regulatory practice

Risk governance: OCC codifies risk standards, paving the way for increased enforcement actions

The Office of the Comptroller of the Currency (OCC) recently issued a Notice of Proposed Rulemaking to establish formal guidelines incorporating thirteen standards for a bank's risk governance framework, and six standards for a bank's board of directors (Guidelines).[1] Public comments are due by March 28, 2014.

The Guidelines are consistent with the heightened expectations for strong risk management frameworks that the OCC has been communicating as part of its Large Bank Program post-financial crisis, and are also generally consistent with practices adopted by the G-SIBs under the Federal Reserve's watch. However, the formalization of these standards will greatly enhance clarity around the OCC's expectations and more importantly make these standards "rules," thus significantly enhancing the OCC's enforcement power and authority.

The following are the Guidelines' key takeaways:

- ***The Guidelines are proposed pursuant to Section 39 of the Federal Deposit Insurance Act,[2] thereby giving the OCC the authority to issue formal, public enforcement actions in response to significant noncompliance.*** Due to the more discretionary nature of risk governance supervision vis-à-vis more rules-based supervision (e.g., AML), the prospect of such an enforcement action further increases the complexity for banks in their management of reputational risk. While the Guidelines make clear the OCC's expectations, they also provide the OCC with sharper teeth in terms of enforceability.
- ***The Guidelines apply not only to institutions that are part of the OCC's Large Bank Program, but to all large insured national banks, insured federal savings associations, and insured federal branches of foreign banks with average total consolidated assets of $50 billion or more.*** We anticipate the group of banks in scope will include the 19 banks in the Large Bank Program and 8 additional midsized banks. The OCC has reserved authority to include institutions below the $50 billion threshold if the entity's operations are highly complex or otherwise present a heightened risk. However, the Guidelines also allow the OCC to delay or modify application to certain banks – e.g., the OCC notes that it expects to tailor certain standards for the boards of federal branches of foreign banks.

---

[1] See *OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches* (January 16, 2014).

[2] Section 39 of the Federal Deposit Insurance Act authorizes the OCC (and other US banking regulators) to prescribe safety and soundness standards in the form of a regulation or guidelines. The OCC has proposed to issue guidelines rather than regulations, as the former provides the OCC with greater flexibility in considering which remedial actions are most appropriate in dealing with the specific circumstances of noncompliance, including a bank's self-corrective and remedial responses.

pwc

- ***Many covered midsized banks will need to enhance their risk management practices to meet the Guidelines, particularly around risk appetite, strategic planning, and risk data aggregation and reporting.*** Some midsized banks may benefit from the Guidelines' provision that allows a bank with a risk profile that is substantially the same as that of its parent company, to use the risk governance framework of its parent to satisfy the Guidelines. To take advantage of this provision, the risk profiles of the two entities must be "substantially the same," meaning the latest call report must show that the bank's average assets, average assets under management, and total off-balance sheet exposures represent 95% or more of the parent's in the three categories. This requirement thus requires a bank to be about the mirror image of its parent, including in size
- ***Certain institutions, particularly Foreign Banking Organizations, will need to carefully navigate differences between the OCC's Guidelines, and other agencies' standards.*** Although guidelines are typically issued on an interagency basis, neither the Federal Deposit Insurance Corporation (FDIC) nor the Federal Reserve Board (FRB) joined the OCC's proposal. The Guidelines present potential conflicts with the FRB's proposed Enhanced Prudential Standards (EPS) for systemically important financial institutions (SIFIs) applied at the holding company level, and with FRB/FDIC policies for resolving insured banks. Such differences will be particularly felt by Foreign Banking Organizations (FBOs) that own an OCC-supervised institution and will be required to establish an Intermediate Holding Company (IHC) under the proposed EPS for FBOs. For instance, under the EPS, FBOs will need to establish a board risk committee at the IHC level; however, the Guidelines establish requirements for independent directors at the bank level who in theory would not be representing the interests of the IHC shareholders.

This **Financial Services Regulatory Brief** analyzes the Guidelines' standards for risk governance and for the board of directors, assesses the current state of the industry against the standards, and suggests what banks should do next.

Standards for risk governance framework

The Guidelines' 13 proposed risk governance framework standards formalize many of the expectations that the largest global banks have been subject to since the financial crisis, and are detailed in this brief's **Appendix**. In particular, the standards formalize (a) the concept of the three lines of defense (business unit, risk management, and internal audit), (b) expectations regarding incorporating risk into strategic planning, and (c) requirements for defining and linking risk appetite, exposure limits, and limit management.

The Guidelines provide more clarity than previously existed around the roles and responsibilities of independent risk management across the three lines of defense. While each of the 19 banks in the Large Bank Program has made progress in meeting these expectations, most still have work to do around areas such as risk management function capabilities and responsibilities; audit capabilities and responsibilities; talent management; and risk data aggregation and reporting.

In particular, many large institutions still face challenges in building out the second line of defense, which is often reflected in matters requiring attention (MRAs) issued by the OCC in areas such as:

- Independence and stature of the independent risk management function
- Ability to influence and credibly challenge first line decisions
- Ability to be proactive and effective in mitigating problems

On the other hand, banks covered by the Guidelines that have been subject to the Federal Reserve's Comprehensive Capital Analysis and Review (CCAR) have made considerable progress in the areas of strategic planning, risk appetite, and risk governance, which in most cases will be aligned to the proposed standards.

The Guidelines formalize a requirement to align to the Basel Committee on Banking Supervision's *Principles for Effective Risk Data Aggregation and Risk Reporting* (January 2013), which require G-SIBs to make significant improvements to their risk infrastructure and data architecture by 2016. While the OCC does not plan to hold non-G-SIBs to these same standards, the introduction of a risk data aggregation and reporting standard will materially raise the bar with respect to data architecture and IT infrastructure, data quality, and overall data aggregation and reporting capabilities. In particular, US banks have struggled to meet expectations in three areas: quality of risk information, having an enterprise-wide view of risk across all entities and risk-types, and the ability to disaggregate and report risk data.

The challenges of the larger organizations will be amplified for the midsized banks, particularly for those previously supervised by the Office of Thrift Supervision. For these firms, the set of risk governance framework standards presents new expectations. Most of these institutions are still in the process of enhancing risk management capabilities, and are likely to find new challenges in the areas of risk appetite, strategic planning, risk data aggregation and reporting, talent management, and compensation.

Standards for boards of directors

The Guidelines introduce six standards for boards of directors. Four of these are related to board oversight and independence, and are largely in line with the principles or requirements captured in previous guidance by international regulatory bodies and other proposals, as depicted in the below table. One of these four – the requirement for a minimum number of independent directors – is also included in the FRB's proposed EPS (although the EPS does not specify a minimum of two independent directors as the Guidelines do).

The Guidelines also formally introduce two new standards, regarding board training and conducting an annual self-assessment of whether the board is meeting the Guidelines' standards. While these two requirements are in line with practices we have observed at some of the largest organizations, we expect some firms will need to enhance their practices.

Interestingly, two standards captured by the EPS and international regulatory guidance bodies are not included as part of the Guidelines. These relate to the board risk reporting and expertise of the board's risk committee, and are delineated at the bottom of the below table.

OCC's proposed standards for board of directors, as compared to others' guidance

	OCC	EPS[a]	SSG[b]	BCBS[c]	FSB[d]	IIF[e]	TCH[f]
Proposed OCC standards							
Oversight over implementation of risk governance framework	✓			✓	✓		✓
Active oversight of risk-taking activities, effective challenge	✓		✓				✓
Exercise of independent judgment	✓			✓	✓	✓	
Independent directors	✓	✓		✓	✓		✓
Ongoing training to independent directors	✓						
Annual self-assessment	✓					✓	
Other standards							
Appropriate expertise of board risk committee members		✓	✓	✓	✓	✓	✓
Formal board risk reporting		✓	✓	✓	✓	✓	✓

[a] Federal Reserve Board, *Enhanced Prudential Standards and Early Remediation Requirements for Covered Companies* (December 2012).

[b] Senior Supervisors Group, *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure* (December 2010).

[c] Basel Committee on Banking Supervision, *Principles for Enhancing Corporate Governance* (October 2010).

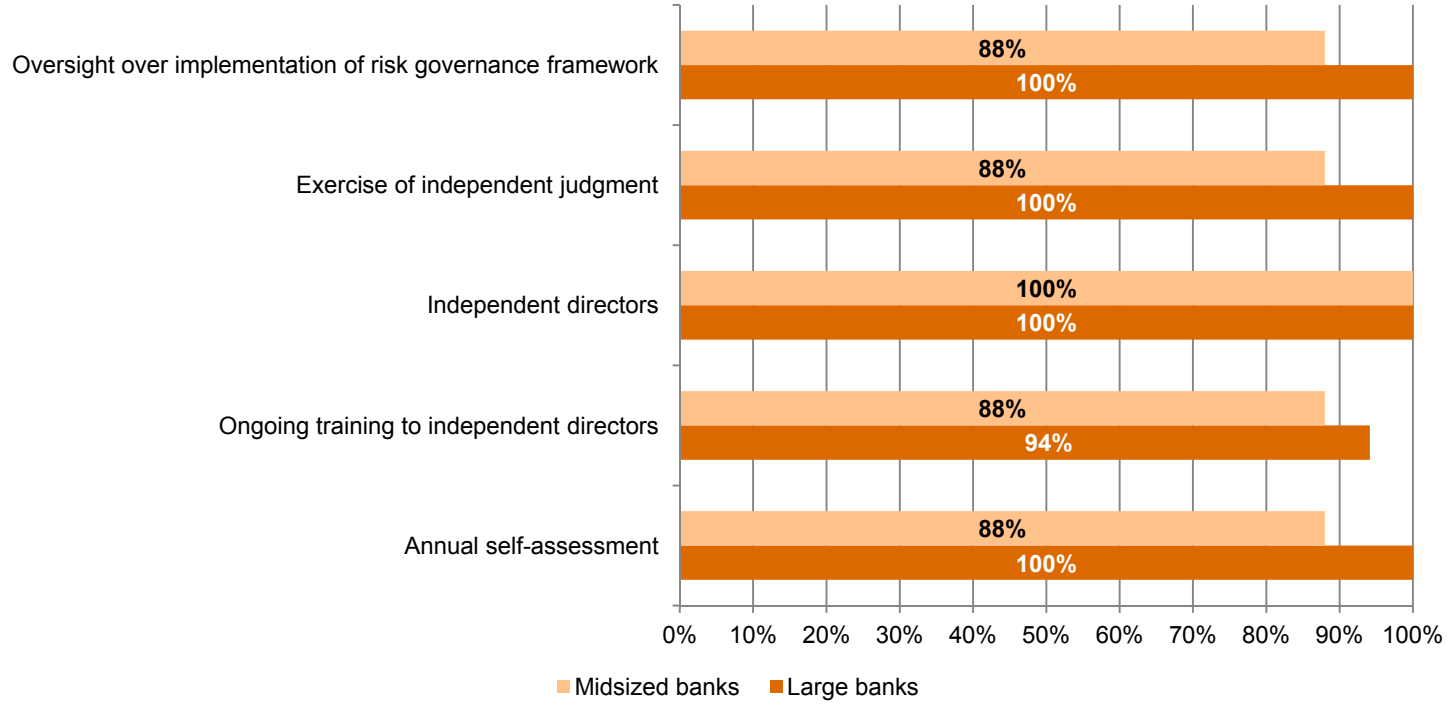
[d] Financial Stability Board, *Thematic Review of Risk Governance* (February 2013).

[e] Institute of International Finance, *Report on Governance for Strengthened Risk Management* (October 2012).

[f] The Clearing House Association, *Guiding Principles for Enhancing Banking Organization Corporate Governance* (March 2012).

The degree of alignment between boards' stated practices and the proposed Guidelines depends on the size of the bank. The following graph shows the percentage of midsized and large banks whose board charters conform to five of the Guidelines' standards. The banks in the Large Bank Program indicate near uniform alignment with the Guidelines, while one of the eight considered midsized banks falls short of a standard in four instances.

*OCC's proposed standards for board of directors, as compared to stated practices**



* Our analysis contrasts the Guidelines against board charters. For large banks, we use the 17 publicly available charters of the 19 banks in the OCC's Large Bank Program. For midsized banks, we use the 8 publicly available charters of the 8 midsized banks likely to in the proposal's scope.

What banks should be doing

While the impact of the proposed Guidelines on the largest institutions will be less than on midsized firms, all in-scope entities should take a closer look at their current practices to determine alignment with the standards, as well as assess themselves against peers. We anticipate that "horizontal" supervision will continue to be important, and while individual institutions may progress towards meeting expectations, evaluation criteria used by examiners will be influenced by peer practices.

As both large and midsized firms continue on the path to a "strong" assessment rating, they should consider whether the following actions are needed based on the current state of their risk management practices:

- Revise risk management policies and procedures to incorporate the proposed standards
- Review alignment of limit structures with the risk appetite statement
- Enhance the mandate of risk management committees at the board and management levels
- Formalize training and self-assessment requirements into board risk committee mandate
- Review risk data aggregation and reporting capabilities
- Clarify or establish explicit linkages between strategic plans, and risk appetite and limits
- Expand internal audit programs to consider the proposed standards
- Establish formal succession planning for the CEO

Appendix – OCC Guidelines' 13 Risk Governance Standards

Risk governance framework	• Establish and adhere to a formal risk governance framework • The framework should be designed by the independent risk management function and approved by the Board • The independent risk management function should review and update the governance framework at least annually
Scope of the risk governance framework	• The risk governance framework should cover the following risks: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputational
Roles and responsibilities	• The risk governance framework should include three distinct functions: front office, independent risk management, and internal audit
Strategic plan	• The CEO should develop a strategic plan with input from the three lines of defense • The Board should monitor, review, and approve the strategic plan at least annually • The plan should cover at least a three-year period and include: a comprehensive assessment of risks, strategic objectives for the bank, an explanation of how the risk governance framework will be updated, and a provision to review and update the strategic plan going forward
Risk appetite statement	• The risk appetite statement serves as the basis for the risk governance framework • The statement should include both qualitative (e.g., sound risk culture) and quantitative (e.g., limits) components • Limits should be set at levels that account for appropriate buffers and prompt management to reduce risk before the bank's capital adequacy is jeopardized
Concentration and front line unit risk limits	• The governance framework should include concentration risk limits for relevant risks
Risk appetite review, monitoring, and communication processes	• The risk governance framework should require: – Review and approval of the risk appetite statement at least annually – Initial communication and ongoing reinforcement of the risk appetite statement – Monitoring of risk limits by the independent risk management function, reporting to the Board at least quarterly – Monitoring by front line units of their risk limits, reporting to the board at least quarterly – Monitoring by independent risk management of front office's compliance with their risk limits, reporting to the Board at least quarterly
Processes governing risk limit breaches	• A process should be established that requires the front office and the independent risk management function to identify, escalate, resolve and be accountable for risk limit breaches
Concentration risk management	• The risk governance framework should include policies and processes for effectively identifying, measuring, monitoring, and controlling the bank's concentration of risk

Risk data aggregation and reporting	• The risk governance framework should include a set of processes designed to ensure the bank's risk data aggregation and reporting capabilities are appropriate – Design, implementation, and maintenance of data architecture to support data aggregation – Capturing and aggregating data to be reported in a timely manner to the board and OCC – Distribution of risk reports to all relevant parties at a frequency needed for decision making
Relationship of risk appetite statement, concentration risk limits, and front line unit risk limits to other processes	• The risk appetite statement, concentration risk limits, and front line unit risk limits should be incorporated in the following: – Strategic and annual operating plans – Capital stress testing and planning processes – Liquidity stress testing and planning processes – Product and service risk management processes – Decisions regarding acquisitions and divestitures – Compensation and performance management programs
Talent management processes	• The bank should establish process for talent development, recruitment, and succession planning to ensure employees responsible for risk management have the appropriate knowledge
Compensation and performance management programs	• The bank should establish a compensation program that meets the requirements of any applicable statute or regulation and is appropriate to: – Ensure employees adhere to an effective risk governance framework – Ensure front line unit decisions consider the level of risk identified by independent risk management and internal audit – Attract and retain the talent needed to maintain an effective risk governance framework – Prohibit incentive-based pay arrangements that encourage excessive risk taking

Additional information

For additional information about PwC's Financial Services Regulatory Practice and how we can help you, please contact:

Dan Ryan
Financial Services Regulatory Practice Chairman
646 471 8488
daniel.ryan@us.pwc.com

David Sapin
Financial Services Regulatory Practice Leader
646 471 8481
david.sapin@us.pwc.com

Armen Meyer
Director of Regulatory Strategy
646 531 4519
armen.meyer@us.pwc.com

Contributors: Dietmar Serbee, Alejandro Johnston, Douglas Roeder, Gary Welsh, Kevin Clarke, Audrey Galang, Jonathan Kahan, and Kenneth Peyer.

To learn more about financial services regulation from your iPad or iPhone, click here to download PwC's new Regulatory Navigator App from the Apple App Store.

Follow us on Twitter @PwC_US_FinSrvcs