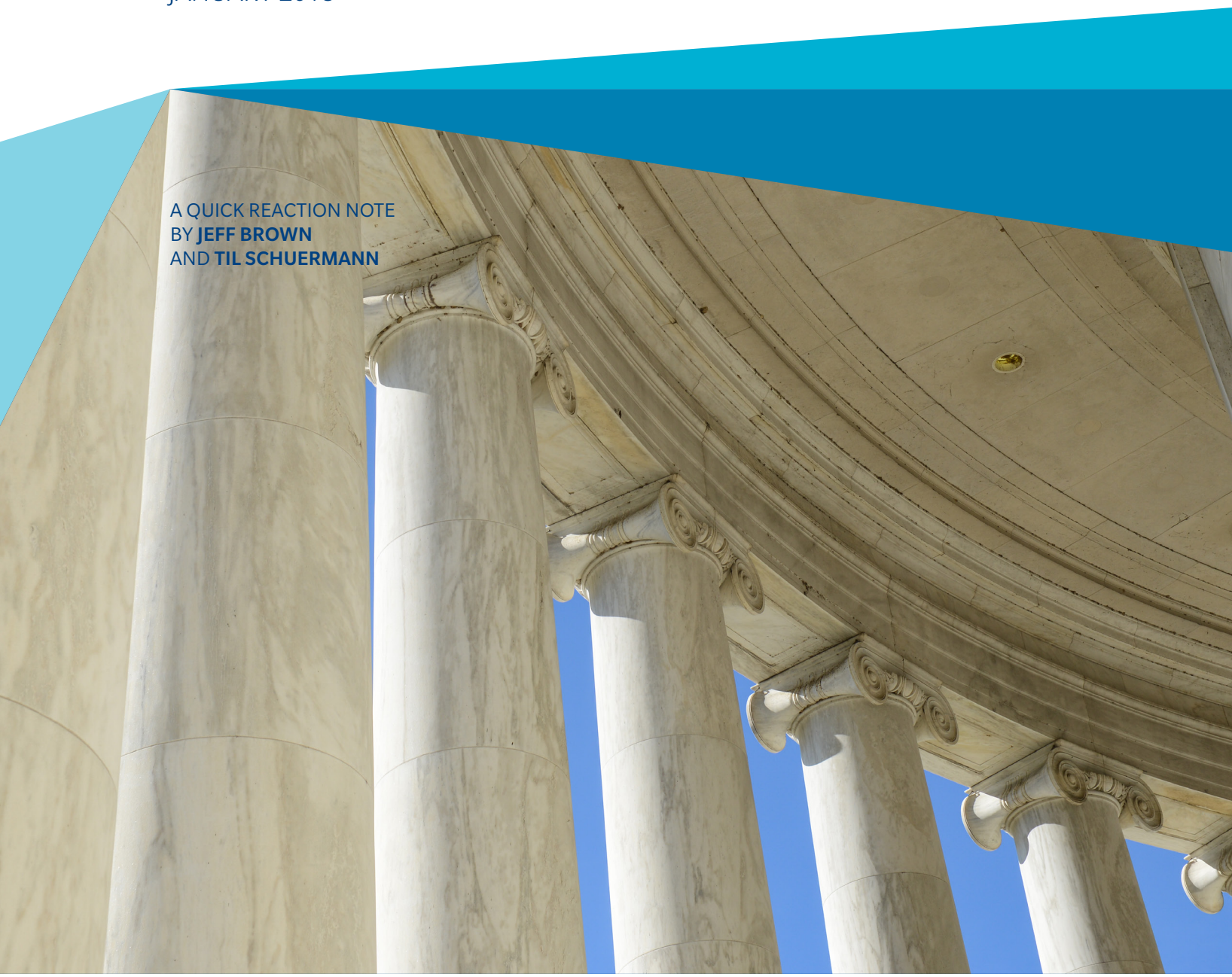
OLIVER WYMAN

Financial Services

PUTTING FLESH ON THE BONES OF THE "THREE LINES OF DEFENSE" SKELETON

PARSING NEW FEDERAL RESERVE GUIDANCE ON EFFECTIVE SENIOR MANAGEMENT

JANUARY 2018



A QUICK REACTION NOTE
BY **JEFF BROWN**
AND **TIL SCHUERMANN**

One question we hear a lot is: who really owns the risk management framework in a bank? Is it the Chief Risk Officer? Is it so fundamental that it is a shared responsibility among the whole executive or senior leadership team? And who owns the risk, and what does that mean?

The Federal Reserve has issued new guidance on governance regarding the responsibilities for risk management within large financial institutions. It puts flesh on the bones of the 'three lines of defense' skeleton, the bedrock of risk management. Together with guidance issued in August 2017 on Board Effectiveness, the January 4th release completes the picture of what the Federal Reserve views as effective governance of a large financial institution.

• • •

The Federal Reserve rang in the new year by issuing useful proposed guidance that consolidates and clarifies their expectations regarding the responsibilities for risk management within large financial institutions. It presents a comprehensive treatment across the three lines of defense, going beyond the well-trodden second and third lines (Independent Risk Management – IRM – and Independent Audit) and elucidating the risk management roles in the business lines where the first line of defense resides. In addition it clarifies the responsibility of the executive management team in managing the overall risk framework.[1]

US supervisory agencies, Federal Reserve and OCC alike, have spent considerable energy on pinning down expectations on the second and even third lines of defense while being lighter on specifics of the responsibilities of the first line, beyond the high level view that it should 'own the risk'. Similarly, while the Federal Reserve and OCC have articulated expectations for a risk management framework deployed across three lines of defense, prior statements have been unclear about who is responsible for that framework. This guidance puts flesh on the bones of the 'three lines of defense' skeleton. Since it is likely that the final version of this proposed guidance will be close to this version, now is the time for the covered banks to look closely at the roles and responsibilities in their risk management frameworks.

Together with the proposed guidance on Board Effectiveness issued last August, the January 4th release completes the picture of what the Federal Reserve views as effective governance of a large financial institution, the third of the three elements in the Federal Reserve's new rating system (the other two elements are capital and liquidity adequacy).[2] We see several themes in both the August and January proposed governance guidance, highlighted in this Quick Reaction Note.[3]

The proposed guidance applies to large financial institutions (LFIs, those with >$50 billion in assets), both domestic and foreign (effectively the CCAR banks), large Savings and Loan holding companies plus Financial Stability Oversight Council (FSOC) designated non-bank Systemically Important Financial Institutions (SIFIs; there are just two remaining). It is

1 https:/www.federalreserve.gov/newsevents/pressreleases/bcreg20180104a.htm

2 For Large Institution Supervision Coordinating Committee (LISCC) firms, effective recovery planning constitutes an additional factor in the Governance & Controls component of the new supervisory rating system. For more detail on LISCC and a list see https:/www.federalreserve.gov/supervisionreg/large-institution-supervision.htm

3 For a summary of the August 2017 proposed guidance and new rating system, see our Quick Reaction Note "Less is more" http:/www.oliverwyman.com/our-expertise/insights/2017/aug/less-is-more.html

notable that Foreign Banking Organizations (FBOs) are included in this (but excluded in the Board Effectiveness) guidance, consistent with expectations on risk management set out in Regulation YY, namely the establishment of a Chief Risk Officer (CRO) for the combined US operations (CUSO) encompassing both the Intermediate Holding Company (IHC) and the branch.

The proposed guidance is in the form of principles for effective governance and control by senior management, business line management, and IRM and control. While not enumerated, there are 16 principles, listed at the end of this note following the outline of the proposed guidance.

In our view there are four main takeaways from this guidance:

- Explicitly states shared responsibility of senior management for implementing, within the board approved risk tolerance, the strategy of the firm in a safe and sound manner
- Defines collective responsibility of senior management for the implementation and maintenance of the risk management framework
- Articulates specific expectations of business line management on what it means to own the risk
- Presents more focused expectations of Independent Risk Management, both in the second and third lines of defense

SHARED RESPONSIBILITY FOR THE SAFE AND SOUND MANAGEMENT OF THE BANK – AND ALL THAT THAT ENTAILS – BY SENIOR MANAGEMENT

Supervisors, unsurprisingly, have paid considerable attention to financial institutions' risk and control environment. After all, supervisors are disproportionately focused on downside risk, and that focus has sharpened considerably since the financial crisis. The role of the CRO in particular has been singled out as requiring independence, expertise, stature and direct reporting to the Chief Executive Officer (CEO) with a direct line to the board. The CRO is expected to be head of an IRM function that occupies the second line of defense in the classic three lines of defense framework. The CRO and the Chief Audit Executive (CAE) are the two individual roles called out explicitly in both the board effectiveness guidance from August 2017 and this new proposed guidance. The second and third lines of defense have not been wanting for attention from supervisors, and expectations on their remit have gone up and up and up.

What, then, is expected of the first line of defense, the one that is supposed to 'own the risk'? Beyond that vague but important catch-phrase, supervisors have articulated precious little about what they expect of business line managers – note this also includes areas such as Treasury and IT. The January 4th proposed guidance lays out those expectations. Indeed this proposed guidance articulates an equal number of principles – five – that apply to business line management and to IRM.

EXPECTATIONS FOR THE FIRST LINE

The first of the principles that applies to business line management establishes the foundational responsibility: "Business line management should execute business line activities consistent with the firm's strategy and risk tolerance." It further calls for business line management to identify the risks that emanate from the strategic plan and how they expect those risks to be managed to stay within risk tolerances. The onus of risk identification and first-order risk management is clearly on the first line! Lest there be any doubt in the matter, the third principle makes it clear: "Business line management should identify, measure, and manage the risks associated with the business activities under a broad range of conditions, incorporating input from IRM."

The onus of risk ownership on the first line does not stop with risk identification, assessment and management. Clearly stated in principles four, five, and six, the Federal Reserve expects business line management to allocate sufficient resources and infrastructure to operate safely and soundly, that the internal control system is effective, and that business line managers are held accountable.

Do these higher expectations apply to all lines of business, even ones that are quite small? No. As with all supervisory guidance, the expectations expressed in this proposed guidance are modulated according to the risk and complexity of the situation. Only "core" business lines are expected to adhere to the principles laid out in the guidance – unless the bank is one of the LISCC institutions, in which case all business lines are considered "core". The guidance defines "core" somewhat vaguely: "any business line where a significant control disruption, failure, or loss event could result in a material loss of revenue, profit, or franchise value, or result in significant consumer harm." It is up to the bank to determine which business lines are "core" and how this decision was arrived at. Note, however, that the second and third lines are expected to cover the whole firm, whether LISCC or not.

Who then owns the risk management framework that spans the three lines of defense, with so many responsibilities falling to the business lines and business line management as well as to the IRM function? The proposed guidance establishes a collective responsibility on the part of senior management, defined as the "core group of individuals directly accountable to the board of directors for the sound and prudent day-to-day management of the firm." It imposes shared responsibility by senior management for "overseeing the activities of the firm's business lines (individually and collectively) and the firm's IRM and controls."

Specifically, "(s)enior management is responsible for implementing the firm's strategy and risk tolerance approved by the board." The duality of strategy and risk tolerance (appetite), inextricably linked, was the first of five principles of board effectiveness in the Federal Reserve's August 2017 proposed guidance, and it reappears in the January guidance in the first of 16 principles. Moreover, the identification of "senior management" as playing a critical role in the risk management framework is important because this creates a collective responsibility for the efficacy of risk management, as opposed to focusing that responsibility narrowly on the CRO and the CEO.

MORE FOCUSED EXPECTATIONS OF INDEPENDENT RISK MANAGEMENT

What, then, is expected of IRM? The proposed guidance describes expectations for a firm's IRM, which include

- Evaluating the firm's risk tolerance
- Establishing enterprise-wide risk limits and monitoring adherence to those limits
- Identifying, measuring, and aggregating risks
- Providing an independent assessment of the firm's risk profile, and
- Providing risk reports to the board and senior management.

This defines the role of IRM rather narrowly. With the overall risk appetite defined by the board, the CRO is the architect but not the owner of the enterprise risk management framework. That architect is also the policeman, monitoring compliance with risk limits/tolerances. The implication is that the CRO not only monitors compliance with limits/tolerances and reports on aggregate risks but also monitors the adequacy of the business line elements of the framework – basically the adequacy of the first line. By defining the role of IRM with more focus, this approach makes IRM's job manageable and assigns the responsibility to the executive committee (senior management).

Through the remaining principles, the Federal Reserve expects the CRO and CAE to have sufficient stature and independence (principles 7 and 8); asks IRM to evaluate the firm's risk tolerances and establish limits (principles 9 and 10); establishes independent risk identification, measurement, and assessment (principles 11 and 12); and ensures that risk reporting is accurate, concise, and timely (principle 13). Principles 14 and 15 speak to internal controls (controls should be effective given the size and complexity of the firm, and should be regularly evaluated and tested), and the last principle outlines expectations for internal audit to "examine, evaluate and perform independent assessments of the firm's risk management and internal control systems and report findings to senior management and the firm's audit committee." The emphasis on stature and independence of the second and third lines of defense is especially important in the risk framework implied by this proposed guidance, given the increased clarity and emphasis on the role of the business lines.

COMMUNICATE, COMMUNICATE, COMMUNICATE

We see repeated emphasis on communication in this proposed guidance, a theme carried over from the August guidance on board effectiveness (there it was the second of five principles). The basic idea being promulgated is that it is hard to be effective and make sound decisions without frequent, clear, and concise communication among and between the board of directors, senior management, business line management, and the control functions. "Senior management should base its decisions and actions, as well as its communications with the board, on a full understanding of the firm's risks and activities."

Risk reporting is a good case in point for demonstrating the spirit of this and earlier governance guidance: "Risk reporting should be comprehensive, useful, accurate, and timely." Yes, it should be comprehensive, but to be useful it has to be accurate and

timely. Implied is that it needs to be succinct to be useful; comprehensive does not mean overwhelming, a recognition that the post-crisis push for more and more documentation and reporting, especially to senior management and the board, likely crossed the line of usefulness (and definitely of user friendliness).

WHAT SHOULD BANKS DO NOW?

Although still in the proposed guidance stage, we do not expect the final guidance to change materially. Our main observations will almost certainly remain, namely

1. The collective responsibility for the safe and sound management of the bank – and all that that entails – by senior management
2. The elucidation of expectations of business line management (the first line of defense), and
3. The focusing of supervisory expectations on IRM.

Therefore it is not too soon to revisit the roles and responsibilities articulated by your bank's risk management framework and the relevant policies.

In our experience, the first of these observations (shared responsibility by senior management) is likely already the case. Different banks adopt different risk cultures. For example, in some banks there is an emphasis on clear ownership and accountability and a hesitance to assign shared responsibilities, whereas other banks simply lack clear articulation of their governance structures.

A casualty of the post-crisis regulatory push on improving and upgrading banks' risk and control structures has been, in our view, the overburden of the second line and insufficient emphasis and specificity on the first line really (really!) owning the risk. The complementarity of higher and more specific expectations on the first line, and more focus and specificity of the role of the second line, almost certainly merits careful examination at most banks and other financial institutions covered by the proposed guidance. And, at the risk of stating the obvious, any such evaluation, and conclusions drawn therefrom, should be shared with the board of directors. Finally we would encourage banks to submit such a review, together with any action plan that would emanate, to their supervisor to demonstrate a thoughtful and fulsome approach to effective governance at their firm.

APPENDIX

CORE PRINCIPLES OF EFFECTIVE SENIOR MANAGEMENT, MANAGEMENT OF BUSINESS LINES, AND INDEPENDENT RISK MANAGEMENT (IRM) AND CONTROLS[4]

I. Core Principles of Effective Senior Management

Principle: Senior management is responsible for managing the day-to-day operations of the firm and ensuring safety and soundness and compliance with internal policies and procedures, laws, and regulations, including those related to consumer protection.

II. Core Principles of the Management of Business Lines

A. Implementation and Execution of Strategy and Risk Tolerance

Principle: Business line management should execute business line activities consistent with the firm's strategy and risk tolerance.

B. Risk Identification and Risk Management

Principle: Business line management should identify, measure, and manage the risks associated with the business activities under a broad range of conditions, incorporating input from IRM.

C. Resources and Infrastructure

Principle: Business line management should provide a business line with the resources and infrastructure sufficient to manage the business line's activities in a safe and sound manner, and in compliance with applicable laws and regulations, including those related to consumer protection, as well as policies, procedures, and limits.

D. Business Controls

Principle: Business line management should ensure that the internal control system is effective for the business line operations.

E. Accountability

Principle: Business line management and staff are accountable for operating within established policies and guidelines, and acting in accordance with applicable laws, regulations, and supervisory guidance, including those related to consumer protection.

III. Core Principles of Independent Risk Management and Controls

A. Governance, Independence, and Stature

1. Chief Risk Officer

Principle: The CRO should establish and maintain IRM that is appropriate for the size, complexity, and risk profile of the firm.

2. Chief Audit Executive

Principle: The CAE should have clear roles and responsibilities to establish and

4 https:/www.federalreserve.gov/newsevents/pressreleases/bcreg20180104a.htm

maintain an internal audit function that is appropriate for the size, complexity and risk profile of the firm.

B. Independent Risk Management

1. Risk Tolerance and Limits

   Principle: IRM should evaluate whether the firm's risk tolerance appropriately captures the firm's material risks and confirm that the risk tolerance is consistent with the capacity of the risk management framework.

   Principle: IRM should establish enterprise-wide risk limits consistent with the firm's risk tolerance and monitor adherence to such limits.

2. Risk Identification, Measurement, and Assessment

   Principle: IRM should identify and measure the firm's risks.

   Principle: IRM should aggregate risks and provide an independent assessment of the firm's risk profile.

3. Risk Reporting

   Principle: IRM should provide the board and senior management with risk reports that accurately and concisely convey relevant, material risk data and assessments in a timely manner.

C. Internal Controls

Principle: A firm should identify its system of internal control and demonstrate that it is commensurate with the firm's size, scope of operations, activities, risk profile, strategy, and risk tolerance, and consistent with all applicable laws and regulations, including those related to consumer protection.

Principle: A firm should regularly evaluate and test the effectiveness of internal controls, and monitor functioning of controls so that deficiencies are identified and communicated in a timely manner.

D. Internal Audit

Principle: The internal audit function should examine, evaluate, and perform independent assessments of the firm's risk management and internal control systems and report findings to senior management and the firm's audit committee.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

AMERICAS
+1 212 541 8100

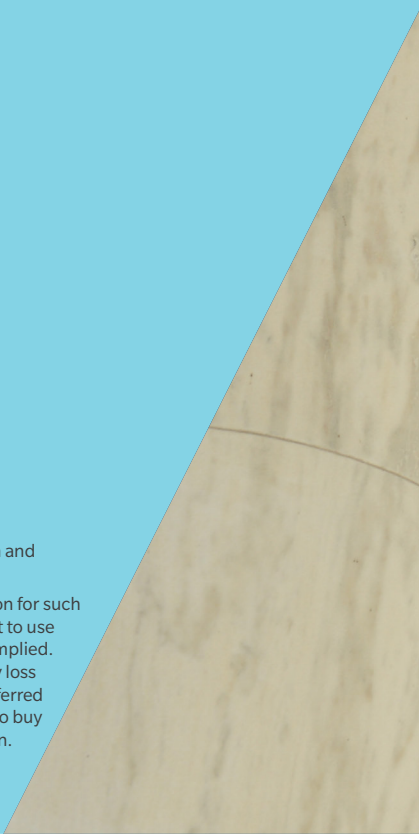
EMEA
+44 20 7333 8333

ASIA PACIFIC
+65 6510 9700

JEFFREY BROWN
Partner, Finance & Risk and Organizational Effectiveness Practices
jeffrey.brown@oliverwyman.com

TIL SCHUERMANN
Partner, Finance & Risk and Public Policy Practices
til.schuermann@oliverwyman.com

www.oliverwyman.com



OLIVER WYMAN