Heightened Expectations for Some—a Message for All to Consider: The Evolution of the 3 Lines of Defense

By Thomas Grundy, CRCM, Senior Regulatory Consultant, Wolters Kluwer Financial Services
Mark Twain once said that, “Climate is what we expect, weather is what we get.” The words and wisdom of this great American author and humorist succinctly describe the mindset and experience leading up to and following the most recent global financial crisis we have endured. From what seemed endless sunny days of possibilities for an economy riding the real estate boom, the weather took a significant turn. For the financial services industry it came in the form of legislative response and tightening of supervisory control on the part of regulators. The Office of the Comptroller of the Currency (OCC) has, for its part, heightened expectations for the institutions under its supervision.

On September 11, 2014, the OCC established minimum standards that large national banks and federal savings associations must meet in designing, building and implementing their risk management frameworks. The minimum standards prescribed by the OCC have been issued in the form of Guidelines, as an appendix to 12 C.F.R. Part 30. The Guidelines establish minimum standards for Boards of Directors in their oversight of risk management activities. While the Guidelines do not apply to community banks, the OCC reserves the right to apply the Guidelines to any bank whose average total consolidated assets do not meet the $50 billion threshold but whose operations are “highly complex” or otherwise present a “heightened risk” based on complexity of products and services, risk profile, and scope of operations. With the rollout period spanning 18 months, the industry will observe the OCC’s application of the Guidelines with great interest.

Whether your institution falls under the direct coverage of this rule, risk management practices in all aspects are being scrutinized across the financial services industry. The concepts covered by the OCC’s Guidelines provide a good indication of what regulators might consider when reviewing your risk management practices.

Risk Governance Framework – The Components
The Guidelines provide that banks should establish and adhere to a formal risk governance framework. While not an entirely new concept, the Guidelines provide new impetus for Board members in how they oversee the decisions made by management. The Guidelines focus on risk governance frameworks as the core process by which banks manage and control risk-taking activities. The Appendix to 12 CFR 30 outlines the minimum standards for the design and implementation of a risk governance framework. The Guidelines allow covered banks to use a parent company’s risk governance framework, without modification. If the framework meets these minimum standards, the risk profiles of the parent company and the covered bank are substantially the same and the bank can demonstrate this through a documented assessment.

Risk governance frameworks should be developed with a view to addressing risks relating to the core “buckets” of risk—credit, interest rates, liquidity, pricing, operations, compliance, strategic planning, and the institution’s reputation. To support and fulfill the development of a conforming risk framework, well-defined roles and responsibilities for Front Line Units, Independent Risk Management, and Internal Audit are critical to the success of risk assessment and ongoing risk management at all levels of the enterprise. These three units must be independent from one another and must ensure that the Board of Directors is provided with sufficient information about the institution’s risk-taking activities to enable “credible challenges” to management’s decisions and recommendations.

Front Line Units
Comparing the proposed Guidelines to the final version, the definition of “Front Line Unit” has been modified to allow banks a degree of flexibility in identifying who and what should be included. This change was made in response to comments received stressing that organizational units such as Legal, Human Resources, Finance, and Information Technology do not create the types of risk that should be subject to the Guidelines.

Under the final Guidelines, a Front Line Unit, serving as the first line of defense, is any organizational unit or function thereof in a bank that is accountable for one of several enumerated risks and that:

- Engages in activities designed to generate revenue or reduce expenses for the parent company or bank;
- Provides operational support or servicing to any organizational unit or function within the bank in the delivery of products or services to customers; or
- Provides technology services to any organizational unit or function covered by these Guidelines.

The revised definition provides greater flexibility to identify and classify organizational units that are responsible for risks. The definition makes it possible for part of an organizational unit to qualify as a Front Line Unit without implicating the entire organizational unit. Additionally, if an organizational or functional unit is accountable for a risk, it is considered a Front Line Unit—whether or not it created the risk. The purpose of this change is to make clear that a Front Line Unit’s responsibility for, or ownership of, a risk may arise by engaging in the activity that originally created the risk within the bank, or when the organizational unit is assigned accountability for a risk that was created by another organizational unit.

As the first line of defense, Front Line Units are responsible for, and accountable to, the Chief Executive Officer and the Board for appropriately assessing and effectively managing all risks associated with their business activities. Specifically, Front Line Units should:

- Regularly assess the material risks associated with normal activities establishing the basis for fulfilling responsibilities and to determine if action is required to strengthen risk management or reduce risk, given changes in the business’s risk profile;
- Establish and adhere to policies that provide guidance for ensuring that risks associated with the Front Line Unit’s activities are effectively identified, measured, monitored, and controlled, consistent with the bank’s risk appetite statement, concentration risk limits, and all policies established within the risk governance framework; and
- Adhere to all applicable policies, procedures, and processes established by Independent Risk Management.
Timeline for Compliance
The Guidelines establish initial compliance dates on which covered banks should comply. The compliance dates vary in accordance with average total consolidated assets:

- Covered banks greater than or equal to $750 billion as of November 10, 2014, must meet compliance with the Guidelines, as of the same date;
- Covered banks having at least $100 billion but less than $750 billion as of November 10, 2014, should comply with these Guidelines within six months from November 10, 2014;
- Covered banks having $50 billion but less than $100 billion as of November 10, 2014 should comply with these Guidelines within 18 months of November 10, 2014; and
- Banks with less than $50 billion that are banks because the parent company controls at least one other bank as of November 10, 2014, should comply with these Guidelines on the date that such other bank should comply.

In cases where a bank does not fall within the scope of the Guidelines on November 10, 2014, but subsequently becomes subject to the Guidelines because average total consolidated assets are equal to or greater than $50 billion after November 10, 2014, will be expected to comply with the Guidelines within 18 months from the as-of date of the most recent call report used in the calculation of the average asset.

Independent Risk Management
Independent Risk Management serves as the second line of defense, overseeing risk-taking activities and undertaking responsibility for assessing risks and issues independent of Front Line Units. Under the Guidelines, Independent Risk Management is primarily responsible for designing a comprehensive, written risk governance framework that is commensurate with the size, complexity, and risk profile of the bank. To meet this responsibility, Independent Risk Management must:

- Regularly identify and assess the bank’s material aggregate risks, leveraging this information as the basis for fulfilling its responsibilities;
- Establish and adhere to enterprise policies and processes to ensure compliance, with concentration risk limits stating how aggregate risks within the bank are effectively identified, measured, monitored, and controlled, consistent with the risk appetite statement and all policies and processes established within the risk governance framework;
- Identify and communicate to the CEO and the Board or the Board’s risk committee material risks and significant instances where Independent Risk Management’s assessment of risk differs from that of a Front Line Unit, and significant instances where a Front Line Unit is not adhering to the risk governance framework; and
- Identify and communicate to the Board or the Board’s risk committee material risks and significant instances where Independent Risk Management’s assessment of risk differs from that of the CEO, and significant instances where the CEO is not adhering to, or holding Front Line Units accountable for adhering to, the risk governance framework.

The Guidelines urge that the Independent Risk Management team reviews and updates the risk governance framework on at least an annual basis—and as often as needed—to address improvements driven by industry risk management practices and changes in the bank’s risk profile caused by emerging risks, corporate strategic planning, or any other relevant internal and external risk factors.

Internal Audit
Serving as the third line of defense, Internal Audit ultimately determines whether the risk governance framework complies with the Guidelines and is appropriate for the size, complexity, and risk profile of the bank. In carrying out its responsibilities, Internal Audit should:

- Maintain a complete and current inventory of the bank’s material processes, product lines, services, and functions, as well as assess the risks, including emerging risks, associated with each, which collectively provide a basis for the audit plan;
- Establish and adhere to an audit plan that is periodically reviewed and updated, taking into account the bank’s risk profile, identified issues and emerging risks and outline the frequency with which activities should be audited;
- Communicate significant changes in the audit plan to the Board’s audit committee;
- Evaluate the adequacy of and compliance with policies, procedures, and processes established by Front Line Units and Independent Risk Management under the risk governance framework;
- Report in writing, conclusions and material issues and recommendations from audit work carried out under the audit plan, identifying the root cause of any material issues;
- Determine the effectiveness of Front Line Units and Independent Risk Management in identifying and resolving issues in a timely manner;
- Establish and adhere to processes for independently assessing the design and ongoing effectiveness of the risk governance framework on at least an annual basis; and
- Identify and communicate to the Board’s audit committee significant instances where Front Line Units or Independent Risk Management are not adhering to the risk governance framework.
Internal Audit should establish a quality assurance program that ensures Internal Audit’s policies, procedures, and processes comply with applicable regulatory and industry guidance; are appropriate for the size, complexity, and risk profile of the bank; are updated to reflect changes to internal and external risk factors, emerging risks, and improvements in industry Internal Audit practices; and are consistently followed.

Three-Year Strategic Plan
In order to align the organization and establish a single vision for achieving strategic goals, the CEO should be responsible for the development of a formal strategic plan and is expected to coordinate input from Front Line Units, Independent Risk Management, and Internal Audit. The Board should evaluate and approve the strategic plan and monitor management’s efforts to implement it at least annually. The strategic plan should cover, at a minimum, a three-year period and:

- Provide a comprehensive assessment of risks that currently have an impact on the bank or that could have an impact on the bank during the period covered by the strategic plan;
- Articulate an overall mission statement and strategic objectives for the bank; and
- Explain how the bank will update, as necessary, the risk governance framework to account for changes in the bank’s risk profile.

The plan should be reviewed, updated, and approved, as necessary, due to changes in the bank’s risk profile or operating environment that were not contemplated when the strategic plan was developed.

Risk Appetite Statement
Under the Guidelines, banks are expected to have a comprehensive written statement outlining the risk appetite that, once approved and communicated, will serve as the basis for the bank’s risk governance framework. The risk appetite statement should include both qualitative components and quantitative limits. The qualitative components should emphasize a safe and sound risk culture, whereas quantitative limits should incorporate measurable outcomes.

Concentration and Front Line Unit Risk Limits
The risk governance framework should include concentration risk limits and, as applicable, Front Line Unit risk limits. Concentration and Front Line Unit risk limits should constrain excessive risk taking and, when aggregated across the Front Line Units, ensure that these risks do not exceed the boundaries established in the bank’s risk appetite statement.

The risk governance framework should include policies and supporting processes appropriate for the bank’s size, complexity, and risk profile for effectively identifying, measuring, monitoring, and controlling the bank’s concentrations of risk.

Risk Appetite Review, Monitoring, and Communication Processes
The risk appetite statement should be reviewed and approved by the Board or the Board’s risk committee at least annually or more frequently based on the size and volatility of risks and any material changes in the bank’s business model, strategy, risk profile, or market conditions. Communication and ongoing reinforcement of the bank’s risk appetite statement is essential to maintaining awareness among employees to align their risk-taking decisions accordingly. Independent Risk Management’s monitoring of the bank’s risk profile relative to its risk appetite—and compliance with concentration risk limits, including reporting its findings to the Board or the Board’s risk committee at least quarterly—is essential to understanding adherence to the limits and whether they are set appropriate to the bank’s risk profile. This reporting is further supported by Front Line Units’ monitoring compliance with their respective risk limits and reporting to Independent Risk Management at least quarterly. The frequency of monitoring and reporting should be performed more often, as necessary.

Risk Limit Breaches
Banks should establish and adhere to processes that require Front Line Units and Independent Risk Management to identify breaches of the risk appetite statement, concentration risk limits, and Front Line Unit risk limits. As breaches are detected, it will be important to understand the impact to the bank. Establish protocols for when and how to inform the Board, Front Line Unit management, Independent Risk Management, Internal Audit, and the OCC of a risk limit breach that takes into account the severity of the breach and its impact on the bank. Include in the protocols the requirement to provide a written description of how a breach will be, or has been, resolved. Finally, establish accountability for reporting and resolving breaches that include consequences for risk limit breaches and the magnitude, frequency, and recurrence of breaches.

Risk Data Aggregation and Reporting
The risk governance framework should include a set of policies, supported by appropriate procedures and processes, that are designed to provide risk data aggregation and reporting capabilities appropriate for the size, complexity, and risk profile of the bank, and support supervisory reporting requirements. These policies, procedures, and processes should provide for:

- The design, implementation, and maintenance of a data architecture and information technology infrastructure that supports the bank’s risk aggregation and reporting needs during normal times and during times of stress;
- The capturing and aggregating of risk data and reporting of material risks, concentrations, and emerging risks in a timely manner to the Board and the OCC; and
- The distribution of risk reports to all relevant parties at a frequency that meets their needs for decision-making purposes.
Talent Management, Compensation, and Incentives
Banks are expected to establish processes for talent recruitment, development, and succession planning to ensure that management and employees who are responsible for or influence material risk decisions have the knowledge, skills, and abilities to effectively identify, measure, monitor, and control relevant risks. The Board or an appropriate committee of the Board should appoint the CEO and appoint or approve the appointment of a chief audit executive and one or more chief risk executives with the skills and abilities to carry out their roles and responsibilities within the risk governance framework. Compensation and performance management programs are sufficient to attract and retain the talent needed to support and sustain an effective risk governance framework. Furthermore, banks must avoid any incentive-based payment arrangement that encourages inappropriate risks or that could lead to material financial loss.

Standards for Boards of Directors
Each member of the Board should oversee the bank’s compliance with safe and sound banking practices. This is achieved through active oversight of risk-taking activities and holding management accountable for adhering to the risk governance framework. In providing active oversight, the Board may rely on risk assessments and reports prepared by independent risk management and internal audit to support their ability to question, challenge, and, when necessary, oppose recommendations and decisions made by management that could cause the bank’s risk profile to exceed its risk appetite or jeopardize the safety and soundness of the bank. The Guidelines set the standard by stating that the Board should exercise sound, independent judgment.

The membership of the Board should include at least two independent directors who are not officers or employees of the parent company or bank and who have not been an officer or employee of the parent company or bank during the previous three years. Furthermore, independent directors cannot be members of the immediate family of a person who is, or has been within the last three years, an executive officer of the parent company or bank, and they must qualify as independent directors under the listing standards of a national securities exchange.

Boards of Directors should establish and adhere to a formal, ongoing training program that builds on Directors’ knowledge and experience and the bank’s risk profile. Director training should include information with respect to complex products, services, lines of business, and risks that have a significant impact on the bank; as well as laws, regulations, and supervisory requirements applicable to the bank.

Annually, bank Boards should conduct a self-assessment that includes an evaluation of their effectiveness in meeting the standards established by the Guidelines.

Conclusion
Whether you are a large national bank or federal savings association under the direct supervision of the OCC, or not, the message is clear for all that risk management practices are critical to the sound operation of financial institutions. Every business decision must be made in accordance to the risk appetite established by the Board and executive leadership and those making critical decisions will be held accountable. Above all else, you can expect that your system of checks and balances along the three lines of defense will be reviewed by your regulator like never before.
About Wolters Kluwer Financial Services

Whether complying with regulatory requirements or managing financial transactions, addressing a single key risk, or working toward a holistic enterprise risk management strategy, Wolters Kluwer Financial Services works with customers worldwide to help them successfully navigate regulatory complexity, optimize risk and financial performance, and manage data to support critical decisions. Wolters Kluwer Financial Services provides risk management, compliance, finance and audit solutions that help financial organizations improve efficiency and effectiveness across their enterprise. With more than 30 offices in 20 countries, the company's prominent brands include: AppOne®, AuthenticWeb®, Bankers Systems®, Capital Changes, CASH Suite®, GainsKeeper®, NILS®, OneSumX®, TeamMate®, Uniform Forms®, VMP® Mortgage Solutions and Wiz®. Wolters Kluwer Financial Services is part of Wolters Kluwer, which had 2014 annual revenues of €3.7 billion ($4.9 billion), employs 19,000 employees worldwide, and maintains operations in over 40 countries across Europe, North America, Asia Pacific, and Latin America. Wolters Kluwer is headquartered in Alphen aan den Rijn, the Netherlands. Its shares are quoted on Euronext Amsterdam (WKL) and are included in the AEX and Euronext 100 indices.

© 2015 Wolters Kluwer Financial Services, Inc. All Rights Reserved.

Please visit WoltersKluwerFS.com for more information.