CREDIBLE CHALLENGE AND THE SEARCH FOR EXCELLENCE

This article is excerpted from *A Director's Voyage through Risk Management*, a book by Dean Yoost that looks at how directors should approach cyber, strategic, third-party, and other risks. The book will be published by RMA later this year. Yoost, a member of RMA's Editorial Advisory Board, is a frequent contributor to *The RMA Journal.*

"Judge a man by his questions rather than by his answers." — Voltaire

Following the financial crisis, regulators and government officials responsible for ensuring the safety and stability of the capital markets launched a plethora of commissions and inquiries aimed at determining why risk management processes were ineffective.

The prevailing view is that the crisis can largely be traced to the failure of corporate governance and risk management systems. For some institutions, this suggests that boards and management did not sufficiently comprehend aggregate risk and that institutions lacked sufficiently robust risk frameworks.

As a result, the people, systems, and processes for monitoring the complex galaxy of risks failed. In some cases, compensation programs were structured to share upside benefits but not the downside risks. Meanwhile, inadequate and fragmented technology infrastructures hindered efforts to identify, measure, monitor, and control risk. And some institutions' risk cultures did not provide for effective challenge from independent risk management, audit, and control personnel.

While these problems existed to some extent at institutions of all sizes, the regulators embrace the view that it was the largest, most complex institutions where problems were most pronounced and which created the greatest potential threat to financial system stability.

In response to the crisis, the Office of the Comptroller of the Currency resolved to raise the standards for corporate governance and risk management systems. The OCC developed an informal set of heightened expectations, also referred to as "Getting to Strong," to enhance its supervision and strengthen governance and risk management practices at large institutions. Although most regulatory attention since the crisis has focused on mandating higher capital levels, the OCC's heightened exceptions were primarily directed at risk management processes.

Remarks by Comptroller Curry

In clarifying and raising the corporate governance bar for the largest and most complex institutions, the OCC significantly ratcheted up expectations for independent directors. Comptroller Thomas J. Curry has suggested that regulators expect directors to present a "credible challenge" to management and have thorough knowledge of the risks their institution is taking and how management is addressing them. The OCC is no longer willing to accept risk management systems that are simply satisfactory. It is seeking excellence. The expectation is that large institutions will meet high standards and that risk management functions and independent directors will take a strong hand in ensuring compliance.[1]

QUESTIONS DIRECTORS SHOULD ASK

- How do directors become comfortable that the proper "tone at the top" and culture of encouraging the right behavior exist across the institution? What is the process of accountability?
- What are the top risks threatening the institution's strategy, business model, and corporate existence? How does management identify and manage existing and emerging risks? What are the strategic objectives and risks associated with each line of business?
- What information is shared with the board? Is the information sufficiently detailed, yet not overwhelming, so that directors can understand and evaluate the critical risks?
- Are the proper resources in place to manage risks? Are the risk management capabilities improving regularly to ensure that risks are being properly managed in a dynamic environment?
- How are risk appetite and the risk management framework embedded into the business?
- Are the directors and management aligned with regard to the appetite for risk? How do directors evaluate the impact of the compensation program on management's risk taking?
- As new initiatives, products, and services are introduced, which processes are in place to evaluate the risks prior to approval? Do directors know the thresholds for when matters need to be brought to the board before a decision is finalized or risks are escalated?
- How is risk management used to add competitive advantage and value by addressing the gaps in the operations?
- What is the quality of the internal controls supporting the risk management framework?
- Which mechanisms are in place for the board to assess management's data against industry trends and other objective sources to ensure performance is measured accurately?
- In dealing with the regulators, are the institution's risk management initiatives and activities properly and comprehensively described? What is the level of the documentation indicating that directors are demonstrating credible challenge?
- Which gaps in experience and expertise of the directors need to be addressed for the board to provide the appropriate credible challenge to management?

THE FACT THAT THE HEIGHTENED STANDARDS WERE PRESCRIBED AS GUIDELINES RATHER THAN FORMAL REGULATIONS PROVIDES FOR FLEXIBILITY ON THE PART OF THE OCC.

More is also expected in terms of operations and financial profitability—and, by the way, of the regulators themselves. Curry says regulators must function in a way that keeps the banking system safe and sound and avoids anything like what was endured during the crisis.[2]

OCC Guidelines

In September 2014, the OCC issued "Guidelines Establishing Heightened Standards for Certain Large Insured Banks, Insured Savings Associations, and Insured Federal Branches." Frequently referred to as "heightened" or "minimum" standards, they apply to national banks, federal savings associations, and insured federal branches of foreign banks—as long as the institution has average total consolidated assets of $50 billion or more measured on the basis of average total consolidated assets for the previous four calendar years. Once the threshold is crossed there is no turning back, even if the institution has four quarters with less than $50 billion in total consolidated assets.

The guidelines also apply to institutions with less than $50 billion in assets that are determined by the OCC to be highly complex or that otherwise present heightened risk.

(The OCC recognizes that insured federal branches are not required to have statutory boards of directors and that their risk governance frameworks will vary owing to the variety of branch activities. The OCC intends to apply the guidelines to insured federal branches in a flexible manner.)

While the guidelines apply specifically to large institutions, directors need to be cognizant that the regulators are expecting strong industry commitment toward proper risk oversight. It is likely, and even probable, that the regulators will impose on virtually all banks elements of the OCC's guidelines. "All institutions irrespective of size need to take notice of these guidelines and calibrate and adjust board and management practices accordingly," noted Philip B. Flynn, president and CEO, Associated Bank.

The guidelines are intended to advance the heightened expectations program as memorialized by the OCC's informal set of heightened expectations. Examiners will now assess risk management practices and the effectiveness of board oversight using these guidelines to identify and communicate areas requiring improvement by the board and management.

The fact that the heightened standards were prescribed as guidelines rather than formal regulations provides for flexibility on the part of the OCC. "Guidelines give the OCC more flexibility in determining whether to require a noncompliant institution to submit a formal remediation plan or tailor a different remedy, taking into account the institution's circumstances and its self-corrective or remedial efforts," said Rodney R. Peck, partner, Pillsbury Winthrop Shaw Pittman and a board member of Bank of the West.

Under the guidelines, six minimum standards have been set for the board in overseeing the risk governance framework's design and implementation:

1. Require an effective framework. Directors should oversee compliance with safe and sound practices and require management to establish and implement an effective risk governance framework that meets the guidelines' standards.
2. Provide active oversight of management. The board should actively oversee risk-taking activities and hold management accountable for adhering to the framework.
3. Exercise independent judgment. Directors are expected to exercise sound, independent judgment when providing oversight.
4. Include at least two independent directors on the board.
5. Provide ongoing training to all directors. The board should establish and adhere to a formal, ongoing educational program for directors that considers the directors' knowledge and experience as well as the institution's risk profile.
6. Conduct an annual self-assessment. The board's self-assessment should include an evaluation of how well the institution is meeting the standards established for the board in the guidelines.

The guidelines indicate that directors should be knowledgeable about finance and committed to conducting diligent reviews of management, the financials, and business plans. The OCC will evaluate each director's knowledge and experience, as demonstrated in their written biographies and discussions with examiners.

Moreover, the guidelines reemphasize the OCC's expectations that the board provide a "credible challenge" to management. The OCC believes that directors will be able to exert this challenge if they have a comprehensive understanding of the risk-taking activities and actively engage in overseeing those activities.

As noted at the beginning of this article, the OCC believes that, during the financial crisis, directors at certain institutions had an incomplete understanding of risk exposures. To the OCC, this suggests a pre-crisis failure to exercise adequate oversight of management and to critically evaluate management's recommendations and decisions.

In issuing the guidelines, the OCC did not intend to impose managerial responsibilities on boards or to suggest that boards must guarantee results under the risk framework. The guidelines do indicate, however, that directors should require management to establish and implement an effective framework with the board's oversight.

The guidelines also provide that the board or its risk committee should approve significant, but not all, changes to the risk framework and monitor compliance. Directors are required to monitor framework compliance by overseeing management's implementation of the framework and holding management accountable.

As part of the heightened expectations, the OCC expects management to provide boards with enough information on the risk profile and management practices to ensure operation within the board-approved risk appetite, defined as the aggregate level and types of risk that the board and management are willing to accept to achieve strategic objectives and business plans. If variances arise, the OCC expects directors to challenge management.

In providing oversight, directors may rely on independent risk management and internal audit. While the guidelines are focused on those channels, they do not prohibit boards from periodically engaging third-party experts to help them understand risks and to make recommendations for strengthening board and institutional practices.

The OCC believes that the capacity to dedicate sufficient time and energy to reviewing information and developing an understanding of the key issues related to risk-taking activities is a critical prerequisite to effective oversight. Informed directors are well positioned to engage in substantive discussions with management wherein the board provides approval to management, requests guidance to clarify areas of uncertainty, and questions the propriety of strategic initiatives. The guidelines say that directors should question, challenge, and, when necessary, oppose recommendations and decisions that could cause the risk profile to exceed appetite or jeopardize safety and soundness.

The OCC expects that this provision, in addition to resulting in a more informed board, will enable directors to determine whether management is adhering to, and understands, the risk framework. For example, recurring breaches of risk limits or actions that cause the risk profile to materially exceed appetite may demonstrate that management does not understand or is not adhering to the framework. In these situations, the guidelines recommend that directors take action to hold the appropriate parties accountable.

The OCC does not intend the guidelines to become a compliance exercise or lead to scripted meetings between board and management. Instead, it will assess compliance primarily by what is gleaned from examiners' frequent conversations with directors. Likewise, the OCC does not expect directors to evidence opposition to management during every board meeting—only when necessary. The OCC believes that an environment in which examiners, directors, and management communicate openly will benefit the institution, so the guidance encourages such interactions.

The guidelines effectively hardwire the informal expectations program into the OCC examination process.

THE BOARD'S CREDIBLE CHALLENGE: AREAS OF REGULATORY FOCUS

	Areas of Focus
Corporate Strategy	Evaluation of capital, liquidity, funding, and risk management in creation of the annual strategy and funding plan.
Budgeting and Planning	Review and consideration of key financial and nonfinancial metrics informing the budget.
Institutional Performance	Understanding of the institution, the industry, emerging trends and risks, and management's assumptions to ensure performance objectives are met.
Significant Transactions	Evaluation of proposed transactions to ensure they align with strategic and risk objectives, are sufficiently planned and financed, and have the appropriate infrastructure in place.
Risk Management	Enforcement of a risk management framework that contemplates trends, is clearly communicated and consistently applied, and is incorporated into all aspects of business planning.
Compensation	Development of compensation practices that retain top talent and do not encourage irresponsible risk management behavior.
Succession Planning	Formulation of a succession plan in the event of a planned or unplanned change in leadership.
Culture and Ethics	Creation of an environment requiring adherence to a code of ethics that cascades through the institution, from management to all employees.
Capital Stress Testing (CCAR)	Evaluation of the institution's capital stress-testing program.
Resolution Planning	Development of resolution planning by requiring business management involvement and creating initiatives to enhance resolvability.

Source: "Board of Directors: Effective Challenge," PricewaterhouseCoopers, 2014.

Other Regulatory Initiatives

Although important, the OCC's guidelines represent only one of the latest trends in rule makings and pronouncements that focus on an institution's risk management framework and corporate governance structure as well as board responsibilities.

The regulators expect the whole to be greater than the sum of the parts when it

DIRECTORS SHOULD RECEIVE INFORMATION SUFFICIENT TO UNDERSTAND THE MATERIAL RISKS AND EXPOSURES IN ORDER TO INFORM AND SUPPORT DECISIONS ON CAPITAL PLANNING AND ADEQUACY.

comes to risk management. The Federal Reserve is focused on the enterprise-wide consolidated view of the institution, while the OCC expects the institution to evaluate and manage risk separate from its parent to protect the national bank charter. Both views are aligned and have the fundamental requirements of stronger risk management and governance.

Building on lessons learned from the crisis, the Federal Reserve has also taken a number of important steps to improve its supervisory program for large institutions. These initiatives have focused not just on the amount of capital an institution maintains, but also on the internal practices and policies an institution uses to determine the amount and composition of capital that would be adequate, given risk exposures and strategies as well as regulatory expectations and standards. Corporate governance, risk appetite, and risk management are viewed as important aspects of these initiatives.

In December 2012, the Fed issued SR 12-17, which established a framework for the consolidated supervision of large financial institutions. The framework has two primary objectives. First, each institution is expected to ensure that the consolidated institution and its core business lines can survive under a broad range of internal or external stresses. This requires financial resilience through the maintenance of sufficient capital and liquidity and operational resilience through the maintenance of effective corporate governance, risk management, and recovery planning. Second, each institution is expected to ensure the sustainability of its critical operations under a broad range of internal and external stresses. This requires, among other things, effective resolution planning that addresses the complexity and interconnectivity of the institution's operations.

In August 2013, the Fed also issued "Capital Planning at Large Bank Holding Companies: Supervisory Expectations and Range of Current Practice" (ROPE guidance). It describes Fed expectations for internal capital planning at the large, complex institutions subject to its capital plan rules, referred to as the Comprehensive Capital Analysis and Review (CCAR).

The ROPE guidance indicates that the board has ultimate oversight responsibility and accountability for capital planning and should be in a position to make informed decisions.

Directors should receive information sufficient to understand the material risks and exposures in order to inform and support decisions on capital planning and adequacy. The information must include a discussion of key limitations, assumptions, and uncertainties within the capital planning process so directors are fully informed of any weaknesses in the process and can effectively challenge reported results before making capital decisions. The ROPE guidance suggests that boards with stronger practices have sufficient expertise and level of engagement to understand and critically evaluate the information provided by management.

Fed Chair Janet Yellen has said that, while there is some evidence of improved risk management, internal controls, and governance at the biggest institutions, compliance breakdowns in recent years have continued to undermine confidence in risk management and controls. Given the size, complexity, and interconnectedness of the institutions, she said that this could have implications for financial stability.[3]

It is evident that the trend toward greater regulatory expectations of directors will continue in the foreseeable future as the following events unfold:

- The Federal Reserve implements the Dodd-Frank Act's enhanced risk management standards for large U.S. bank holding companies, large foreign banking organizations, and systemically important nonbank financial companies.
- Banking institutions design and implement comprehensive compliance and risk governance programs for the Volcker Rule, the Dodd-Frank liquidity risk management standards, capital planning and stress testing, the changing regulatory landscape for derivatives, and other important legal and regulatory developments.
- The Federal Reserve and FDIC apply similar risk governance principles to large state banks, and all U.S. banking agencies apply over time some or all of these principles to midsize banks.[4]

Given these pronouncements, the heightened expectations for risk governance are here to stay, and their criticality for the regulators will likely continue to increase. "The focus of regulators on such issues as capital adequacy, liquidity, operational risk, governance, and culture is driving change throughout the financial services industry," noted Eugene A. Ludwig, founder and CEO, Promontory Financial Group. "The heightened standards of the regulators place serious new responsibilities on both directors and management."

Siren Call to Directors

The financial services industry faces significant post-crisis challenges. The pace of change is unprecedented and, at times, bewildering. Many boards and management must contend with multiple jurisdictions and timetables for new regulations and expectations, while facing higher penalties for noncompliance.

The regulators seem determined to avoid putting taxpayers on the hook for another round of bailouts.

The primary driver of the OCC's guidelines is the presumed need for an entity or body, ultimately the institution's board, to establish the acceptable level of risk. The expectation is that directors will establish and monitor this level and push back on management and business lines that naturally want to increase risk as a trade-off for greater profitability.

RMA supports the notion of credible challenge and believes that the appropriate role of the board is to provide oversight to management by critically evaluating its recommendations and decisions. In this regard, directors need to understand the content of such recommendations and decisions, the desired outcomes, and the material risks, and then determine whether management has properly assessed the risks and either developed appropriate mitigation strategies or simply accepted the risks known at the time.[5]

The guidelines are intended to encourage and, in fact, compel the board's challenge to management, but they are not meant to promote confrontation between directors and management at board and committee meetings or even outside forums. However, directors are expected to expand their oversight of risk in meaningful ways. The idea is not for directors to question each and every decision of management. Rather, the guidelines require a board that is active and informed when it comes to risk matters. At the same time, the board does not operate at the front lines of the business. Directors rely on management and a network of reporting processes to remain informed.

The Clearing House believes board challenges should consist of informed and probing questions of management, inside or outside of the boardroom, rather than a formal record of disagreements with management or rejections of management recommendations. In particular, The Clearing House does not believe that the effectiveness of challenge can be evaluated based on the number of challenges recorded in the minutes or elsewhere.[6]

Some believe that the biggest handicap directors face in overseeing risk is self-inflicted. Many directors, for a variety of reasons—including the rationales that "This is how we have always done it" or "It would be impolite to ask"—have simply not asked management for the type, quality, and quantity of information necessary to meet increased oversight and governance expectations.[7]

Directors are compelled to pursue new approaches in effectively challenging management decisions. They must help management establish a "tone at the top" that fosters transparency in decision making and communication, as well as vigorous adherence to a code of ethics. Developing pointed questions that allow directors to consider broader institutional objectives, culture, and risk appetite when approving budgets, financial plans, and executive compensation is essential and very effective.[8]

The board must undertake a process that allows it to receive sufficient information about the business, risks, and performance in real time, including formal written opinions on the effectiveness of the risk management process from assurance providers. The board must then use this information to challenge assumptions, projections, and strategic initiatives of management. Directors must be confident that management has thought through the plans and is responding appropriately to questions and comments.

A dilemma for boards in obtaining more and better information is the risk of asymmetric data—in other words, the gap between the information known by management and the information presented to the board. The role of a director, by nature, is less than full-time. As such, directors rely heavily on management for the information they need to evaluate risks and performance.

Management cannot, and should not, provide every piece of data to the board. In selecting information to be shared with directors, it is possible for gaps to arise in what management knows versus what it presents to the board. Directors need to have confidence in management that the information reflects the facts and the realities of the business. The regulators are often helpful in identifying and remedying information gaps when they occur.

Creating and fostering a culture that actively supports credible challenge is extraordinarily difficult. Conflict, which generally is avoided at all cost, can be a key

EFFECTIVE OVERSIGHT OF RISKS

REGULATORY "EXPECTATIONS"

- The board should receive information from management sufficient to understand the material risks and exposures. The information should be received at least quarterly or whenever there are significant developments.
- Reports to the board should include a discussion of key limitations, assumptions, and uncertainties within the risk framework, so that directors are fully informed of any weaknesses in the process and can effectively challenge reported results.
- Reports to the board should include management's strategies to address identified key limitations in the risk management framework, so that directors can assess reported strategies and take appropriate action to address identified weaknesses.

INDUSTRY "BEST PRACTICES"

- Reports to the board should provide timely, concise, and accurate information, with key takeaways concerning current and expected market conditions, enterprise-wide risk issues and mitigating measures, and risk and performance profiles of each line of business.
- Reports to the board should include management's assessment of end-to-end risk management and reporting. This assessment outlines the strengths and limitations of the information provided to the board, including those related to data, models, and report production processes.
- Reports to the board need to include high-level summaries of efforts to improve the quality and accuracy of risk data, as well as assessments of controls' effectiveness in producing and aggregating risk information.

Source: "Board Governance: Higher Expectations, but Better Practice?" PricewaterhouseCoopers, January 2016.

ingredient in searching for facts, reaching the right conclusions, and making the best decisions. In all businesses and in many boardrooms, there is a fine line between being a "challenger" and being an "obstructionist." Success is predicated on a culture that truly values challenge and debate.[9]

According to the guidelines, active oversight does not mean that directors should assume management functions. Although Curry's commentaries and the OCC's guidelines are helpful in determining the director's role and responsibilities regarding risk oversight, it is likely that some directors' activities will occasionally come precariously close to management functions as they perform their own investigations and oversee management.

Considerable management support is required to oversee risk and exercise credible challenge. Directors will need more documentation to support management's assertions about risks and how they are being managed. Directors should be receiving high-level information and current and emerging risk data and actionable reports. Management reporting must be able to highlight the current state of risk and emerging themes in ways that allow directors to assess information in greater depth. Best practices are focused on quality data supported by analysis and synthesis sufficient to make information relevant and transparent. As a result, enhanced oversight likely requires more board and committee meetings, better analytics, a commitment to board education, and an overall much greater command of risk details.[10]

As the guidelines bring a new level of detail to board-level issues, a gap analysis of the institution and the board to ensure compliance and meet the expectations of regulators may be necessary in some cases. Both the board and management need to be committed to appropriately addressing gaps or deficiencies.

Importantly, levels of litigation and regulatory risk have become elevated as boards and management implement more transparent and demonstrable risk management systems. Better and more formal risk management processes and improved information, far beyond the details of what would be normally expected as a matter of good corporate governance, could burden directors with documented knowledge of the risk acceptance and risk tolerance decisions that have the potential for controversy. These new risks of greater scrutiny and the possibility for more litigation must be fully understood by directors, and mitigation strategies need to be thoughtfully developed.[11]

Care must be exercised in what is documented and in the level of detail supporting the board's credible challenge. The regulators will focus on the number of risk committee meetings and their duration, the quality of information provided, and the active engagement of the directors. All of these factors demonstrate the level of interaction, the presence of effective challenge, and the importance of risk. It is also important to document in the minutes and with board materials that management is working through the insights that result from directors' challenges.[12]

Final Comments

The standards for board oversight are evolving rapidly, and many directors face significant challenges in meeting new expectations. The notion of the board's credible challenge presents a serious next step for directors in search of excellence.

Directors need to digest regulatory requirements and understand regulators' expectations. Each board member is expected to have knowledge and meaningful experience that adds value to the discussion of risks and the risk framework. Directors also need to dedicate ample time and energy to understanding the business and the institution's inherent and emerging risks. That is accomplished by not only studying and absorbing board materials and presentations but also, in many cases, walking the halls to become acquainted with people, programs, and processes.

In closing, credible challenge is effectively presented by directors who apply their knowledge and invest the requisite time and effort—and who also have both the confidence to ask difficult questions of management and the patience to tenaciously pursue acceptable responses. ®

Dean A. Yoost is a member of the board of directors of MUFG Union Bank and Pacific Life Insurance Company, as well as an advisory board member of American Honda Finance Corporation. He is a retired partner of PricewaterhouseCoopers (PwC), where he spent 33 years and served as a member of PwC's Global Oversight Board. He can be reached at deanyoost@cox.net.

Notes

1. Remarks by Thomas J. Curry at the 49th Annual Conference on Bank Structure and Competition, Chicago, Illinois, May 9, 2013.
2. Remarks by Thomas J. Curry at the ABA Risk Management Forum, Orlando, Florida, April 10, 2014.
3. Remarks by Janet L. Yellen at the Committee on Financial Services, U.S. House of Representatives, Washington, D.C., November 4, 2015.
4. "Introduction to Risk Governance and the OCC's Guidelines," Davis Polk, 2014.
5. Letter from The Risk Management Association to the Office of the Comptroller of the Currency, March 25, 2014.
6. "Guiding Principles for Enhancing U.S. Banking Organization Corporate Governance," The Clearing House, 2015.
7. Parveen P. Gupta and Tim J. Leech, "Risk Oversight: Evolving Expectations for Boards," The Conference Board Governance Center, January 2014.
8. "Board of Directors: Effective Challenge," PricewaterhouseCoopers, December 2015.
9. Robert A. Prentice and Yousef A. Valine, "Barriers to Achieving Credible Challenge," *The RMA Journal*, July-August 2015.
10. "Stronger: OCC's Heightened Expectations – Enhancing Risk Management and Driving Growth," Deloitte, 2014.
11. Parveen P. Gupta and Tim J. Leech, "Risk Oversight: Evolving Expectations for Boards."
12. "OCC Final Guidelines Establishing Heightened Standards for Certain Large Insured Banking Institutions," KPMG, September 2014.