Welcome to the C-Suite

by John Bugalla and James Kallman | September 1, 2013 at 6:00 am

A chief risk officer (CRO) is a relatively new addition to the corporate hierarchy. Originating within the broader financial industry sector in the late 1990s, the position expanded into the energy, insurance and utility sectors with a push from the credit rating agencies. Today the number of CROs has been steadily increasing in other industries as well. Thanks to Dodd-Frank and a proposal from the Board of Governors of the Federal Reserve, CROs in the banking and non-bank financial sector are going to receive a promotion. CROs, welcome to the C-suite, courtesy of Uncle Sam.

A Legislative Mandate

The Dodd-Frank legislation that was enacted in 2010 was aimed at reforming the financial sector. Section 165 of Dodd-Frank specifically addresses issues associated with the broader subject of risk management, especially in the area of corporate governance where the requirements called for a board-level risk

committee that included a “risk management expert.” The legislation also put forth a new framework that mandated an “enterprise-wide” approach to risk management.

More recently, the Board of Governors of the Federal Reserve System proposed “Enhanced Prudential Standards” that would implement the mandatory portions of Section 165. Most notably, every covered company and every publicly traded bank holding company with assets of $10 billion or more must establish a risk committee, have a board-level risk committee with one member being an independent “risk management expert,” and employ a chief risk officer who will report directly to the CEO and the risk committee. Rather than the usual general principals, the proposal sets out detailed rules about the responsibilities of the risk committee and the requirement for a CRO.

The Role of the CRO

The CRO’s proposed fundamental responsibilities are to implement and maintain enterprise-wide risk management practices. Additionally, the CRO should have direct responsibility for designating specific responsibilities and directing oversight for allocating delegated risk limits and monitoring compliance with such limits.

The standards also suggest that the CRO’s responsibilities should include establishing appropriate policies and procedures relating to risk management governance, practices and risk controls; developing appropriate processes and systems for identifying and reporting risks, including emerging risks; managing risk exposures and risk controls and monitoring and testing these controls; reporting on risk management issues and emerging risks; ensuring that risk management issues are effectively resolved in a timely manner; and making regular reports to the risk committee.

The question of expertise of the CRO has also been addressed by the proposed rules and this could present an interesting problem—namely, how to fill the position with a properly qualified person. This personnel issue is complicated because covered companies have to find two people: a CRO and an independent director who has risk management expertise to sit on the risk committee.

The risk management expertise of both the independent director and the CRO must be commensurate with the company’s systemic footprint. Even though most companies—including banks—are organized in functional silos, the Federal Reserve Board takes the strong position that an executive whose expertise and experience are in a focused area may not be suitable as a CRO in a global company with diverse businesses.

The specific proposed rules also go a long way toward addressing the structural risk management issues that are needed in financial institutions. The issue for consideration is that the larger firms that failed or required rescue actually had a CRO. But while the CROs of those firms reported to the CEO, they were largely ignored or removed altogether.

The personal interaction between the CEO and the newest member of the C-suite cannot be legislated or mandated, but because the proposed rule dictates that CROs must report directly to the board risk committee and the CEO, the thought might be that two risk management experts may be able to convince the CEO and/or the board to heed their warnings in time of crisis.

The CRO position has the potential to wield considerable power within an organization. While the proposed CRO mandate specifically applies to “covered compan[ies]” falling under the Federal Reserve umbrella, the functional responsibilities of the CRO stated in the proposed rules are sufficiently broad to serve as the benchmark or guide for other industries beyond the financial sector.

First Steps to Permanence

CROs will eventually become a permanent fixture within the broader spectrum of publicly traded companies. This change will occur for one of three reasons: 1) organizations start to recognize best practices in governance and risk management; 2) organizations are pushed either by crisis or by external forces such as activist shareholders and the credit rating agencies; or 3) government mandate.

The same reasoning applies to privately held businesses. However, in family-owned businesses the push will most likely come from second- and third-generation family members who, while not directly involved in management, want to protect their equity and dividend stream. Privately held businesses looking to sell would also be wise to strengthen their risk management programs as potential buyers take a more comprehensive approach to their due diligence process. In smaller companies, it is more likely that an existing senior executive officer will be assigned CRO responsibilities until a time when conditions warrant a dedicated position.

About the Author

 **John Bugalla** is a principal of ermINSIGHTS, an enterprise risk management consulting firm.