Financial Services Regulatory Update

November 8, 2016

This communication is designed to provide you with quick snapshots and timely perspectives on recent regulatory developments.

Auditing Corporate Culture and Managing Ethics Risk

Background

In September, 2016, the Consumer Financial Protection Bureau imposed a multi-million dollar fine against a U.S. financial institution for sales practices that led to the creation of thousands of fictitious accounts. The actual financial impact of these accounts to consumers is estimated to reach millions of dollars. While the bank's executive leadership has indicated controls were in place to prevent, detect and report such a breach in ethics, the U.S. Senate has called for stronger penalties against the bank and its executive management team, and has asked the question: how many more banks are engaging in the same practice? As a result of these developments, banks of all sizes are beginning to assess their systems of internal controls to determine whether an event like this could land them in hot water with regulators, legislators, and consumers. Their primary question: where do we start?

Managing Risk across the Organization

Operational and compliance risk management programs have been a regulatory expectation since the Committee of Sponsoring Organizations (COSO) published a framework for improving the quality of financial reporting through business ethics, internal controls and corporate governance in 1992. Since the original guidance was issued, updates and clarifications have been published as well, including the committee's *Internal Control - Integrated Framework* issued in 2013 and *Leveraging COSO Across the Three Lines of Defense* published in July 2015. The framework considers risks specific to business lines, compliance and monitoring functions, and internal audit.

According to the COSO model, an organization's board of directors is primarily responsible for establishing objectives for the organization, articulated through policies and carried out within the organization under the supervision of the senior leadership team. The board and executive officers set the tone for carrying out those objectives as well, and through example and directives to the senior leadership team, establish expectations for ethical, fair and responsible business activities to meet established objectives.

The framework is intended to address risk at every level of the organization:

1. **Management Controls and Internal Control Measures**

    - Business objectives established by the board and executive leadership must balance risk and strategy, consider the potential for realistically meeting objectives while maintaining integrity, and investing in business processes and controls that present unacceptably heightened risk
    - Senior management oversee the conduct of business activities and processes designed to meet established objectives, including responding to situations or circumstances that present heightened risk of failing to meet goals in a manner consistent with the board's objectives and expectations
    - Business line management design and implement processes that are designed to achieve the organization's objectives in a manner consistent with board expectations

- Primary drivers of business activities, such as sales quotas, are designed in view of inherent risks
- Controls and processes are developed to effectively manage inherent risks related to all stakeholder groups (i.e., financial and operational expectations of shareholders, the board, executive management; compliance and safety/soundness expectations of regulators; fairness and ethics expectations of customers and communities, etc.)

2. **Financial, Security, Risk Management, Quality, Inspection and Compliance Controls**
    - Internal check-points and controls are sensitive to residual risks within business processes
    - The organization's financial performance, safety and soundness, and compliance with regulatory requirements are facets of monitoring programs to ensure business activities are conducted in a manner consistent with board and executive management expectations
    - Dialogue between the first and second lines of the defense, as well as between business activities and the board, encourages fluidity in the risk management program and greater agility to respond to changes, challenges, and failures
3. **Internal Audit**
    - Through objective, independent assessment and testing, the internal audit function provides assurance to the organization's stakeholders that business objectives are being met in a manner consistent with their expectations
    - Internal audit determines whether business processes and controls are designed effectively, whether risk is adequately identified and mitigated, and whether failure to meet objectives is likely

Boards, Executive Leaders, and the *Tone at the Top*

The *Tone at the Top* is a concept addressed at length in the COSO framework. No longer are financial organizations at liberty to ignore the potential for loss, fraud, or non-compliance in pursuit of strategic objectives. Stakeholder groups demand fair, responsible and ethical business activities conducted according to the organization's stated objectives, with safeguards in place (the three lines of defense) to prevent, detect and remediate failures in the conduct of those activities.

An organization's Ethics Policy and Program, the document declaring its *Tone at the Top*, is itself a framework directing the business of the entire organization. Typically, this framework is comprised of multiple components:

- Policy outlining expectations for the conduct of business according to applicable laws and regulations, following both the letter and spirit of those requirements
- Internal communication channels encouraging employees across the organization to report actual misconduct or increased risk of misconduct (e.g., Whistleblower hotlines, Ethics hotlines, etc.)
- Performance management strategies integrating ethics, compliance and professional responsibility
- Assessment or evaluation of strategic objectives and their impact on the organization's compliance and ethics risk profile, creating risk awareness at the board and executive level

Internal Audit and Knowing the Organization's Culture

By developing and implementing an effective internal audit of the organization's culture, the third line of defense can facilitate effective governance across the first and second lines by providing insights into control gaps or weaknesses, and resulting risk elevation resulting from unrealistic or overly ambitious strategic objectives. Internal audit typically report directly to the board, providing objective assurance of governance, risk and control effectiveness, or lack thereof. In evaluating an organization's culture, internal audit can:

- Demonstrate an understanding of the organization's commitment to integrity and ethical values, and accountability for meeting stakeholder expectations
- Assess the state of the organization's ethical climate and the effectiveness of its strategies, tactics, communications and other processes in achieving the desired level of legal and ethical compliance
- Evaluate the suitability and sustainability of objectives in view of the operating environment and risks associated with the organization's business
- Analyze the policies, procedures, controls and processes intended to mitigate business risks
- Assess the capability of the first and second lines of defense to meet expectations for their risk management responsibilities
- Evaluate the effectiveness of the organization's risk management program processes and controls
- Communicate concerns, heightened risks, or ineffectiveness of controls to the board and monitor remediation
- Provide guidance to the board, management and the first and second lines of defense to facilitate a robust and effective ethics program

How Experis can help

Experis Finance offers industry experience in all aspects of Financial Services, including:

- Performing objective assessments of corporate culture and Tone at the Top
- Assessing the adequacy of your organization's compliance control environment
- Developing internal corporate culture and ethics training programs to address unique risks
- Assisting in the development and/or enhancement of monitoring programs to detect compliance violations
- Developing and maintaining first, second, and third line controls and testing

Our Risk Advisory Services practice can evaluate your current loan compliance program, provide comprehensive recommendations for improvement and help address those recommendations.

Our team of professionals is experienced in working with clients to address these issues in order to help them avoid costly fines and penalties. If you have any questions about or concerns around your implementation of these steps, contact an Experis representative at financialservicesindustry@experis.com or visit our website Experis Finance.