

Financial Institution Compliance Update



October 8, 2013

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

Three lines of Defense: Why two lines of defense are not enough and how work performed by one line can be leveraged by another.

Much attention has been paid by the Consumer Financial Protection Bureau (CFPB), the Federal Reserve Bank (FRB), the Office of the Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC) and state banking departments (collectively, the "regulatory supervisors") to the importance of the three lines of defense which support an effective Compliance Management System (CMS). Our regulatory update this past June focused on this topic as well because we observed anxiety from some smaller community bank clients with regard to expectations for establishing a "robust CMS." At that time, client concern was more of "how do I comply?" However, recently the concern has shifted to "do I really need all these lines of defense, and more, specifically, "can work performed by one defense line be leveraged by another?" This update serves to address this notion of redundancy among the lines of defense and to respond to the question of leveraging work.

Three Lines of Defense Defined

First, let us recap the lines of defense.

- **The First Line of Defense against Compliance Risk: Management Oversight.**
The front office businesses that engage directly with customers have the primary responsibility to understand and apply Managements' internal controls to avoid non-compliance with Board-approved policies and procedures and governing regulations. The chief operating officer (COO) is ultimately accountable for executing the organization's

Update Your Subscription

Take a moment to help us better understand your interests and how we can support your success.

[Update here](#)



If you have specific questions regarding the regulatory content and commentary of this message, please contact:

knowledge@experis.com.

strategy and Board's vision to execute the compliance program.

- **The Second Line of Defense: Compliance.**

The chief compliance officer (CCO) is ultimately accountable for creating, implementing, and executing the Compliance Department's overall CMS which includes a robust monitoring and testing function. This function assesses the firm's compliance risk and devises a risk-focused plan for conducting periodic reviews of internal controls to detect control weaknesses. This function is expected to assist management in devising proper corrective action to remediate and prevent such weaknesses from recurring. This assistance may include developing staff training, analyzing and collecting data and overseeing third-party providers.

- **The Third Line of Defense: Assurance Provided by Internal Audit.**

Assurance requires an independent audit of the compliance function to ensure the organization has effectively implemented compliance policies/procedures and to determine that controls are working as intended. Audits may be conducted by internal or external staff; Audit is tasked with assessing the control environment. Audits should be performed in accordance with a defined Audit Plan (or schedule) as led by the Chief Audit Executive under the direction of the Board.

Compliance Management System (CMS) and the Importance of Three Lines of Defense

The CFPB has identified four interdependent control components that they evaluate to determine the strength, robustness and effectiveness of an entity's CMS. They are:

- Board and Management Oversight
- Compliance Program
- Response to Consumer Complaints
- Compliance Audit

The financial regulators conduct periodic reviews to determine adequacy of a bank's CMS. Its summer 2013 review of bank (including thrifts, credit unions and non-bank depository institutions) programs disclosed that the CMS function for a majority of banks is considered adequate. However, for the banks with inadequate CMS units, the primary problem was that one of the three lines of defense was absent. They did not perform both periodic compliance monitoring reviews and independent compliance audits.¹

The CFPB survey of banks concludes that the periodic monitoring reviews are conducted by either the individual business lines or the compliance departments on a relatively frequent basis, generally monthly or quarterly, and allow the individual business lines or the compliance department to self-check their processes and ensure day-to-day compliance with Federal Consumer Financial laws.²

Internal audit then conducts independent compliance assessments on a less frequent basis, usually annually, to ensure that compliance with federal laws is ongoing, that the CMS as a whole is operating properly, and that the board is aware of compliance issues noted as part of these independent reviews.³

The CFPB warns that an institution that lacks periodic monitoring and relies on audit to identify violations and CMS deficiencies "increases its risk that violations and weaknesses will go undetected for a long period of time." Furthermore, the CFPB is concerned that deficiencies "may not be reported to the Board timely and that any unfair, abusive, discriminatory or otherwise unlawful practices performed by the businesses themselves may go undetected."⁴

Given this perspective, the reply to the question, "do I need all these lines of defense?" is a resounding "yes" unless your institution desires to be cited for an inadequate CMS function. The expectation is clear that compliance risk is to be managed on an ongoing basis. While compliance departments may be capable of performing three out of four attributes noted, compliance audit is of paramount importance to the process and should not be compromised.

¹ Source: CFPB website, <http://consumerfinance.gov/reports/supervisory-highlights-Summer-2013>.

² Ibid. Page 7.

³ Ibid. Page 7.

⁴ Ibid. Page 7.

The Question of Leverage: Can work performed by one defense line be used by another?

The question of "can work performed by one defense line be leveraged by another" is not as straight-forward as the question regarding the necessity for the lines of defense. In fact, there is ample evidence for arguments both for and against placing reliance on work performed by others. Certainly the cost savings is one argument for reliance, but the lack of independence is an argument against this. There is no simple answer, and our reply to this query is "it depends."

Audit can leverage the work of the Compliance function to the degree that compliance monitoring is working as intended. Audit needs to independently validate the effectiveness of the CMS and specific controls. Reliance on the Compliance function would be limited in each of the following cases:

- Compliance performs monitoring on an ad hoc rather than planned basis
- Compliance does not execute according to a developed plan
- Compliance identifies several or significant weaknesses
- Internal audit and compliance has limited coordination or lack protocols for accountability, reporting, and communication.

Each of the above scenarios suggests that limited or no leverage should be placed on the work performed by the Compliance Department. Instead, appropriate risk-based audit testing should commence, otherwise the risk for harm to consumers or other regulatory violations increases and expands the firm's exposure to fines, sanctions and high litigation costs.

Conversely, when compliance monitoring and testing is being executed in accordance with plan and no high risk, material or persistent findings surface, then this suggests that controls are operating as intended. In this scenario, the CFPB permits internal audit to leverage the work performed by Compliance, but not vice versa. The rationale is that the controls are working because the monitoring plan was effective in timely detecting weaknesses.

When the auditor leverages the testing performed by Compliance, the audit should reflect reduced scope and/or sample size which reduces the extent of audit effort. This approach should not only improve efficiency without compromising the CMS but should also partly alleviate the perception of "always being audited" expressed by some auditees and senior managers. When Chief Compliance Officers remain cognizant of their flexibility to assist with specific recommendations to correct deficiencies and provide training where necessary, then a partnership culture with the business lines should naturally develop. Compliance testing should be a partnership to be most effective.

In fact, Compliance departments should have direct access to business systems to generate their own reports and data for conducting periodic monitoring. End products are not required to be formal audit-like reports with ratings assigned. Instead, the company can provide less formal communication such as internal memos directed to stakeholders that contain a summary of controls tested, weaknesses detected and prudent, time-sensitive recommendations for corrective actions. Corrective actions should be closely monitored for completion with delays in meeting deadlines escalated to senior management or the Board. This practice would measurably enhance compliance risk management and provide for a robust CMS.

What your financial institution can do to ensure an adequate CMS function?

In summary, the three lines of defense are necessary for an effective and robust CMS program. Other recommendations are:

- While Compliance should not leverage work performed by others, audit may leverage work performed by Compliance to the extent that the compliance function is effective.
- Compliance testing should be done in partnership with the business to the largest extent possible. Simple changes to the testing methodology can set the tone for a partnership to develop where control weaknesses may be identified.
- Also, timely and corrective measures should be implemented swiftly to ensure that your institution complies with all applicable regulatory requirements.

