

## Financial Institution Compliance Update



June 11, 2013

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

### Deploy an Effective Compliance Management System Across Three "Lines-of-Defense"

The Consumer Financial Protection Bureau (CFPB), under its supervisory authority, has begun examinations of banks and other non-bank financial institutions in industries deemed to be high risk. These high-risk, non-bank organizations include debt collection, money transfer, and payday lending entities. In addition, community banks below the threshold for direct supervision by the CFPB should also anticipate similar expectations applied to their compliance efforts as the OCC and other regulators borrow ideas and concepts from the CFPB.

Feedback from our clients indicate that the initial CFPB examinations are proving to be onerous exercises as large teams of examiners are descending upon organizations for extended lengths of time. Banks and other non-bank financial institutions need to prepare for these reviews well in advance.

#### **Background**

Designing and implementing an effective Compliance Management System (CMS) is a key element of a successful CFPB exam. The CFPB outlines the key elements of a CMS in its supervision and exam manual. Included are four key control components: board and management oversight, compliance program, response to consumer complaints, and the independent internal audit of the compliance program. These elements form the basis for the CFPB's risk assessment at the outset of its review and aids CFPB staff in establishing the intensity of the review. In short, a strong CMS should equate to a less stressful and resource intensive effort.

Implied, but not explicitly stated, in the exam manual is the requirement that the CMS be

#### Update Your Subscription

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

[UPDATE HERE](#)



deployed across three "lines-of-defense." Compliance cannot be the role of a single function. Consumer compliance requirements need to be embedded into day-to-day business operations in order to be effective. Equally, the practical constraints on resources and proximity to the day-to-day flow of business transactions, means that the compliance function may not be in a position to undertake all the tasks needed to ensure effective compliance monitoring. Leading organizations have therefore developed a more robust and operationally comprehensive system of monitoring and control, based on three supporting lines of defense.

### **First Line of Defense – Line of Business**

Business teams form the first line of defense by implementing and monitoring the day-to-day execution of consumer compliance controls embedded in operational decision-making and activities. Ideally, compliance requirements end up fully embedded in the processes and procedures used by frontline staff, new hire and on-going training efforts, and incentive programs. Business teams also need to partner with the compliance team and provide critical input into the compliance risk assessment and design of key control. The business is also responsible for collecting, responding to and resolving consumer complaints and errors. Finally, operations should establish dashboards and metrics to monitor the execution of basic compliance functions such as dispute and complaint resolution cycle times, training completion and other monitoring activities.

The business is also intimately involved in developing new products and services and selecting third-party partners to support customer facing activities. This line of defense needs to include the application of consumer regulatory requirements to key changes in the structure of the organizations channels and delivery platforms, to establish programs that review the CMS of potential suppliers during their selection and to monitor the performance of key partners. Keep in mind that CFPB assumes that firms are monitoring their vendors' compliance activities as if they were directly managed by the firm.

### **Second Line of Defense – Compliance Function**

The second line of defense is responsible for defining the policies, processes and procedures for the CMS and monitoring for new risks and vulnerabilities that may arise. The oversight provided by the compliance team, supported where necessary by other control functions such as risk management, constitutes the second line of defense. It's important to note that the compliance function will also perform compliance monitoring. In banks and other financial services firms, this daily monitoring activity focuses on particularly risky areas, such as suspicious transactions, market abuse, personal account dealing, etc. For other risks, the compliance function provides surveillance over the effectiveness of the compliance controls embedded in the business. Additionally, this line must track the progress of and establish regular communications with upper management and the organization's board of directors to demonstrate that the GRC program continues to perform effectively and efficiently.

Management needs to establish an appropriate structure for the compliance function and ensure that it is properly resourced. A key aspect of this structure is the identification of a competent Chief Compliance Officer who reports directly into the Board of Directors or other compliance committee. The compliance function needs to have the ability to "cry foul" at the highest levels of the organization. Management also needs to review their budget and hiring processes for the compliance function to enable the hiring of sufficient staff and providing them with the tools and training to effectively carry out their responsibilities.

Finally, the compliance organization needs to be collecting and analyzing complaint-related data. The outcome of this analysis would typically yield changes to the CMS, operations, policies,

procedures and products that reduce the risk of harm to the consumers of the firm's services. Keep in mind that the CFPB will leverage complaints they've received by individual firms and in aggregate across industry sectors as part of their risk assessment used to determine the focus and intensity of their examination.

### **Third Line of Defense – Internal Audit**

The third line of defense is internal audit, which is required to be independent of both the business and compliance function. They should conduct regular ex-post reviews of the overall compliance risk management framework including the compliance function itself. The third line of defense operates as an independent entity and provides assurance to the board that the first two lines are conducting, managing and overseeing GRC (governance, risk and compliance) processes effectively.

The audit entity also needs to conduct its own assessment to validate that all appropriate regulatory requirements and risks have been addressed including an evaluation of compliance with Federal consumer compliance laws and regulations and the effectiveness of the CMS. Audit should also assess third-party monitoring programs. It may also validate compliance risk assessment approach, models, execution and conclusions. Finally, audit is ultimately responsible for communicating unacceptable exposures back to the business.

In the end, this appears to be very similar to the early days of Sarbanes-Oxley (SOX) as a more rigorous approach is applied to a set of risks and controls. The three lines of defense are reminiscent of how SOX was ultimately implemented with a dedicated SOX team working closely with the business to design, implement and monitor controls that were then verified by the internal audit function.

### **How Should My Institution Respond?**

Any compliance management system needs to be collaborative to be effective. It pulls together and leverages all the various control functions within the organization. The compliance and business units should partner to establish a basic policy and procedure framework that clearly aligns regulatory requirements with compliance policies and business processes and procedures. Identifying and integrating these three aspects will enable the organization to address all key regulatory requirements and lower the cost of maintaining these artifacts and implementing change when rules are modified or issues.

Once that is established, the business and compliance functions need to establish training and monitoring programs to evidence that key personnel are aware of the compliance requirements and executing on the appropriate policies and procedures. Once this has been put in place, the compliance team then needs to consider how to maintain and enhance its risk assessment, policies and monitoring program on an on-going basis. Sustaining the program is critical.

Once the building blocks of the CMS are in place, the focus should shift towards complaint capture and analysis as a mechanism for improving the CMS structure. Improving the infrastructure supporting the CMS – including the format of policies, procedures and processes, monitoring technology and risk assessment tools – will improve the efficiency and effectiveness of the CMS and enable the organization to quickly respond to changing requirements.

The CFPB is not going away. They have clearly staked out a focus on the CMS for supervised entities. Building an efficient and sustainable compliance program will enable organizations to manage their compliance risk and requirements in an effective manner while creating a sustainable and enduring structure that allows the institution to focus on running the business for

the long haul.

---

