Compliance Management System

Introduction

Financial institutions operate in a dynamic environment influenced by industry consolidation, convergence of financial services, emerging technology, and market globalization. To remain profitable in such an environment, financial institutions continuously assess and modify their product and service offerings and operations in the context of a business strategy. At the same time, new legislation may be enacted to address developments in the marketplace.

All these forces combine to create inherent risk. To address this risk, a financial institution must develop and maintain a sound compliance management system (CMS) that is integrated into the overall risk management strategy of the institution. Ultimately, compliance should be part of the daily routine of management and employees of a financial institution.

This chapter discusses the elements of an effective compliance management system—Board of Directors (Board) and management oversight and the compliance program.

Compliance Management System

A CMS is how an institution:

- learns about its compliance responsibilities;
- ensures that employees understand these responsibilities;
- ensures that requirements are incorporated into business processes;
- reviews operations to ensure responsibilities are carried out and requirements are met; and
- takes corrective action and updates materials as necessary.

An effective CMS is commonly comprised of two interdependent elements:

- Board and management oversight; and
- Compliance program

When both elements are strong and working together, an institution will be successful at managing its compliance responsibilities and risks now and in the future.

Financial institutions are required to comply with federal consumer protection laws and regulations, and are ultimately responsible for such compliance including the use of third-party providers. Noncompliance can result in monetary penalties, litigation, and formal enforcement actions. The responsibility for ensuring that an institution and its third-party providers are in compliance appropriately rests with the Board and management of the institution. Therefore, every FDIC-supervised institution must have an effective CMS adapted to its unique business strategy.

Board and Management Oversight

The Board of a financial institution is ultimately responsible for developing and administering a CMS that ensures compliance with federal consumer protection laws and regulations. To a large degree, the success of an institution's CMS is founded on the actions taken by its Board and management. Key actions that Board and management may take to demonstrate their commitment to maintaining an effective CMS and to set a positive climate for compliance include:

- demonstrating clear and unequivocal expectations about compliance, not only within the institution, but also to third-party providers;
- adopting clear policy statements;
- appointing a compliance officer with authority and accountability;
- allocating resources to compliance functions commensurate with the level and complexity of the institution's operations;
- anticipating and evaluating changes in the institution's operating environment and implementing responses across impacted lines of business;
- identifying compliance risk in the institution's products, services, and other activities, and responding to deficiencies and violations;
- conducting periodic compliance audits; and
- providing for recurrent reports by the compliance officer to the Board.

Leadership on compliance by the Board and management sets the tone in an organization. The Board and management should discuss compliance topics during their meetings. They should include compliance matters in their communications to institution personnel and the general public. Institution management and staff should have a clear understanding that compliance is important to the Board and management, and that they are expected to incorporate compliance in their daily operations.

Policy statements on compliance topics provide a framework for the institution's procedures and provide clear communication to management and employees of the Board's intentions toward compliance.

Regardless of size or institution complexity, the first step Board and management should take in providing for the administration of the compliance program is the designation of

a compliance officer. In developing the organizational structure of the compliance program, Board and management must grant a compliance officer sufficient authority and independence to:

- cross departmental lines;
- have access to all areas of the institution's operations; and
- effect corrective action.

A compliance committee, as an alternative to or in addition to a full-time compliance officer, could be formed consisting of the compliance officer, representatives from various departments, and member(s) of management or the Board. However, the ultimate responsibility of overall compliance with all statutes and regulations resides with the Board.

A qualified compliance officer will have knowledge and understanding of all consumer protection laws and regulations that apply to the business operations of the financial institution. The compliance officer should also have general knowledge of the overall operations of the institution and interact with all of the departments and branches to keep abreast of changes (e.g., new products, services or business practices; personnel turnover) that may require action to manage perceived risk. In larger or more complex institutions the compliance officer may devote all of his or her time to compliance activities. In smaller or less complex institutions, where staffing is limited, a full-time compliance officer may not be necessary; instead, the compliance responsibilities may be divided between various individuals by type of regulation, such as loan-related or deposit-related regulations. In some instances, several banks may share a compliance officer.

A compliance officer's general responsibilities, regardless of the size or complexity of the institution's operations, include:

- developing compliance policies and procedures;
- training management and employees in consumer protection laws and regulations;
- reviewing policies and procedures for compliance with applicable laws and regulations and the institution's stated policies and procedures;
- assessing emerging issues or potential liabilities;
- coordinating responses to consumer complaints;
- reporting compliance activities and audit/review findings to the Board; and
- ensuring that corrective actions are implemented in a timely fashion and are effective at preventing recurrence.

When more than one individual is responsible for compliance matters, responsibility and accountability must be clearly defined.

To be effective at overseeing compliance and maintaining a strong compliance posture, a compliance officer must be provided with ongoing training, as well as sufficient time and adequate resources to do the job. The compliance officer may utilize third-party service providers or consultants to help administer the compliance program or audit functions. However, the compliance officer should perform sufficient due diligence to verify that the provider is qualified, because ultimately the institution's Board and management are responsible for identifying and controlling compliance risks arising from third-party relationships, to the same extent as if the third-party activity was handled within the institution.

If an institution engages the services of a third party, the Board and management must ensure that the third-party operations, products, services, and activities are reviewed for compliance with consumer protection laws and regulations. An effective compliance risk management process will vary depending on the complexity and risk potential of the third-party relationship, but generally includes risk assessment, due diligence in selecting the third-party provider, appropriate contract structuring and review, and sufficient oversight of third-party activities, including adequate quality control over products or services provided.

Compliance Program

A sound compliance program is essential to the efficient and successful operation of the institution, much as a business plan. A compliance program includes the following components:

- Policies and procedures
- Training
- Monitoring and/or Audit
- Consumer complaint response

A financial institution should generally establish a formal, written compliance program. In addition to being a planned and organized effort to guide the institution's compliance activities, a written program represents an essential source document that will serve as a training and reference tool for all employees. A well planned, implemented, and maintained compliance program will prevent or reduce regulatory violations, provide cost efficiencies, and is a sound business step. However, a compliance program is not static. The compliance program must be dynamic and constantly amended on an ongoing basis to focus resources where they are needed most based upon risks to the institution.

It is expected that no two compliance programs will be the same, and that the formality of a program will be dictated by numerous considerations, including:

- institution's size, number of branches, and organizational structure;

- business strategy of the institution (e.g., community bank versus regional; or retail versus wholesale bank);
- complexity of products and services offered;
- staff experience and training;
- type and extent of third-party relationships;
- location of the institution—its main office and branches; and
- other influences, such as whether the institution is involved in interstate or international banking.

The formality of the compliance program is not as important as its effectiveness. This is especially true for small institutions where the program may not be in writing but an effective monitoring system has been established that ensures overall compliance. However, during periods of expansion or turnover of staff, a written compliance program becomes more important because individuals with the particular knowledge or experience may no longer be with the institution or available for contact.

Regardless of the degree of formality, all financial institutions are expected to manage their compliance programs proactively to ensure continuing compliance. Compliance efforts require an ongoing commitment from all levels of management and should be a part of an institution's daily business operations.

Policies and Procedures

Compliance policies and procedures generally should be described in a document and reviewed and updated as the financial institution's business and regulatory environment changes. Policies should be established that include goals and objectives and appropriate procedures for meeting those goals and objectives. Generally, the degree of detail or specificity of procedures will vary in accordance with the complexity of the issue or transactions addressed.

An institution's policies and procedures should provide personnel with all the information needed to perform a business transaction. This may include applicable regulation cites and definitions, sample forms with instructions, institution policy, and, where appropriate, directions for routing, reviewing, retaining, and destroying transaction documents. For example, loan application procedures should be established so that institution personnel consistently treat all applicants equitably and fairly. These procedures should incorporate and clearly convey to staff the regulatory requirements and the institution's lending policy, including the institution's nondiscriminatory lending criteria. Similarly, contracts with third parties should set clear expectations for adherence to relevant laws and regulations, as well as the applicability of regulatory guidance, and management should ensure that sufficient policies and procedures are in place to control the risks associated with a particular third party.

Compliance policies and procedures are the means to ensure consistent operating guidelines that support the institution in complying with applicable federal consumer protection laws and regulations, both directly and through the use of third-party providers. Also, these criteria will provide standards by which compliance officers and line managers may review business operations.

Training

Education of a financial institution's Board, management, and staff is essential to maintaining an effective compliance program. Line management and staff should receive timely, specific, comprehensive training in laws and regulations, and internal policies and procedures that directly affect their jobs.

The compliance officer should be responsible for compliance training and establish a regular training schedule for Directors, management, and staff, as well as for third-party service providers, where appropriate. Training can be conducted in-house or through external training programs or seminars. Once personnel have been trained on a particular subject, a compliance officer should periodically assess employees on their knowledge and comprehension of the subject matter.

An effective compliance training program is frequently updated with current, complete, and accurate information on products and services and business operations of the institution, consumer protection laws and regulations, internal policies and procedures, and emerging issues in the public domain. For example, loan officers, as well as other front-line personnel regularly interacting with loan applicants, should be fully informed about the loan products and services offered by the institution and thoroughly knowledgeable about all aspects of the applicable consumer credit protection laws and regulations.

Monitoring and/or Audit

Monitoring is a proactive approach by the institution to identify procedural or training weaknesses in an effort to preclude regulatory violations.

An audit is an independent assessment and validation of an institution's system of internal controls, operations, and compliance risk management framework. It complements the institution's monitoring system. Audits can be performed internally or by an external entity, as long as the individuals that perform audit activities are independent of the areas being audited.

Every institution should have monitoring and/or audit functions that are appropriate for their size, complexity, and risk profile. Each function plays an important but different role in supporting a strong CMS. It should not be assumed that if an institution has a strong monitoring function in place, risks are appropriately mitigated. For many institutions, it is

necessary to have both.

Monitoring:

An effective monitoring system includes regularly scheduled reviews of:

- disclosures and calculations for various product offerings;
- document filing and retention procedures;
- posted notices, marketing literature, and advertising;
- various state usury and consumer protection laws and regulations;
- third-party service provider operations; and
- internal compliance communication systems that update and revise the applicable laws and regulations to management and staff.

Institutions that include a compliance officer in the planning, development, and implementation of business propositions increase the likelihood of success of its compliance monitoring function.

Changes to regulations or changes in business operations, products, or services should trigger a review of established compliance procedures. Modifications that are necessary should be made expeditiously to minimize compliance risk, and applicable personnel in all affected operating units should be advised of the changes.

Monitoring also includes reviews at the transaction level during the normal, daily activities of employees in every operating unit of the institution. This might include, for example, verification of an annual percentage rate, or a second review of a loan application, before the transaction is completed. Monitoring at this level helps establish management and staff accountability and identifies potential problems in a timely manner.

Compliance officers should monitor employee performance to ensure that they are following established internal compliance policies and procedures. The frequency and volume of employee turnover at an institution should be factored into the schedule for reviews. Such reviews are especially critical after problems have been noted during past audits or examinations, regulation changes, new products are introduced, mergers occur, or when additional branch locations are opened.

Audit:

The Board of the institution should determine the scope of an audit and the frequency with which audits are conducted. The scope and frequency of an audit should consider such factors as:

- expertise and experience of various institution personnel;
- organization and staffing of the compliance function;
- volume of transactions;
- complexity of products offered;
- number and type of consumer complaints received;
- number and type of branches;
- acquisition or opening of additional branch(es);
- size of the institution;
- organizational structure of the institution;
- outsourcing of functions to third-party service providers, including a review of agreements signed or made between the institution and vendors;
- degree to which policies and procedures are defined and detailed in writing; and
- magnitude/frequency of changes to any of the above.

An audit may be conducted once a year, or may be ongoing where all products and services, all applicable operations, and all departments and branches are addressed on a staggered basis. An audit may be performed “in-house” or may be contracted to an outside firm or individual, such as a consultant or accountant. A financial institution that outsources the audit should make certain that the auditor is well-versed in compliance, and that the audit program is based on current law and regulation, as well as comprehensive in scope. Generally, a strong compliance audit will incorporate vigorous transaction testing.

Regardless of whether audits are conducted by institution personnel or by a contractor, the audit findings should be reported directly to the Board or a committee of the Board. A written compliance audit report should include:

- scope of the audit (including departments, branches, product types and third-party relationships reviewed);
- deficiencies or modifications identified;
- number of transactions sampled by category of product type; and
- descriptions of, or suggestions for, corrective actions and time frames for correction.

Board and management response to the audit report should be prompt. The compliance officer should receive a copy of all compliance audit reports and act to address noted deficiencies and required changes to ensure full compliance with consumer protection laws and regulations. Management should also establish follow-up procedures to verify, at a later date, that the corrective actions were lasting and effective.

Consumer Complaint Response

An institution should be prepared to handle consumer complaints promptly. Procedures should be established for addressing complaints, and individuals or departments responsible for handling them should be designated and known to all institution personnel to expedite responses.

Examiners should also discuss with management how complaints are identified and defined, as consumer inquiries may also highlight areas with increased risk of consumer harm and/or regulatory compliance concerns.

Complaints may be indicative of a compliance weakness in a particular function or department. Therefore, a compliance officer should be aware of the complaints received and act to ensure a timely resolution. A compliance officer should determine the cause of the complaint and take action to improve the institution's business practices, as appropriate.

An institution should also monitor complaints to and/or about third parties that are providing services on behalf of the institution.