Overview of Compliance Examinations

Introduction

The Federal Deposit Insurance Corporation (FDIC) promotes compliance with federal consumer protection laws, fair lending statutes and regulations, and the Community Reinvestment Act through supervisory and outreach programs. The FDIC conducts three types of supervisory activities to review an institution's compliance management system; compliance examinations, visitations, and investigations.

Compliance examinations are the primary means the FDIC uses to determine whether a financial institution is meeting its responsibility to comply with the requirements and proscriptions of federal consumer protection laws and regulations. The FDIC conducts visitations for a variety of reasons: to review the compliance posture of newly-chartered institutions or those converting to state non-member status; to review progress on corrective actions or compliance with an enforcement action in the interval between examinations; or to investigate problems brought to the attention of the FDIC. Visitations are usually targeted events aimed at specific operational areas, or entire compliance management systems previously identified as significantly deficient. Compliance examinations and visitations may also be considered during the review of an application submitted to the FDIC (e.g., application for deposit insurance or establishing a branch). Finally, investigations are conducted primarily to follow-up on particular consumer inquiries or complaints, including fair lending complaints.

This section provides a general overview of the FDIC compliance examination. The purposes of compliance examinations are to:

- assess the quality of an FDIC-supervised institution's compliance management system (see "Compliance Management System") for implementing federal consumer protection statutes and regulations;
- review compliance with relevant laws and regulations; and
- initiate effective supervisory action when elements of an institution's compliance management system are deficient and/or when violations of law are found.

Examination Approach

FDIC compliance examinations blend risk-focused and process-oriented approaches. Risk-focusing involves using information gathered about a financial institution to direct FDIC examiner resources to those operational areas where compliance errors present the greatest potential risks of having a negative impact on bank customers, resulting in consumer harm (See the Evaluating Impact of Consumer Harm section of this manual at page II-2.1 for additional information.) Concentrating on the institution's internal control infrastructure and methods, or the "process" used to ensure compliance with federal consumer protection laws and regulations, both acknowledges that the ultimate responsibility for compliance rests with the institution and encourages examination efficiency.

Determining Risk

Risk-focusing involves:

- developing a compliance risk profile for an institution using various sources of information about its products, services, markets , organizational structure, operations, and past supervisory performance;
- assessing the quality of an institution's compliance management system in light of the inherent risks associated with the level and complexity of its business operations and product and service offerings; and
- testing selected transactions based on risk such as when an operational area is determined to have a high risk of consumer harm and institution's compliance management efforts appear weak.

Evaluating the Compliance Management System

Compliance examinations start with a top-down, risk-focused process to comprehensively analyze and review an institution's compliance management system. The compliance examiner considers:

Board and Management Oversight

- Commitment to and oversight of the institution's CMS.
- Level of resources dedicated toward compliance functions.
- Due diligence and oversight of third parties to ensure compliance with consumer protection laws and regulations, and appropriate oversight of third parties' compliance responsibilities.
- Anticipation and responsiveness to changes in applicable laws and regulations, market conditions, and products and services offered.
- Due diligence reviews performed in advance of product changes, considering the entire lifecyle of the product or service, and after implementation of changes.
- Comprehension and identification of compliance risks, including emerging risks, in the institution's financial products, services, and other activities.
- Management of identified risk, including self-assessments.

- Identification of and responsiveness to compliance risk management deficiencies and violations of law or regulations, including remediation.

Compliance Program

- Whether the institution's policies and procedures are appropriate to the risk in the products, services, and activities of the institution.
- Adequacy of third-party relationship program management.
- The degree to which compliance training is current and tailored to risk and staff responsibilities.
- The sufficiency of the monitoring and, if applicable, audit to encompass compliance risks throughout the institution
- The responsiveness and effectiveness of the consumer complaint resolution process.

Based on the results of this review, the examiner may conclude that weaknesses in the institution's compliance management system may result in current or future noncompliance with federal consumer protection laws, regulations, or policy statements, thereby resulting in potential consumer harm. The examiner must determine, based on this analysis, whether transaction testing is warranted to further study particular risk in an entire operational area or regulation, or only a limited aspect of an area or regulation.

The FDIC examination approach appropriately recognizes that the Board of Directors and management of a financial institution are responsible for complying with all federal consumer protection laws and regulations. While the formality and complexity of compliance management systems will vary greatly among institutions, the FDIC expects the Board of Directors and management of each institution to have a system in place to effectively manage its compliance risk, consistent with the size and complexity of its products, services, and markets.

Managing the examination based on risk maximizes examiner efficiency and may reduce the on-site examination presence, while emphasizing areas requiring elevated supervisory attention. By focusing on compliance management systems, examiners will be able to identify the root causes of deficiencies and suggest appropriate corrective actions designed to address the problem and prevent recurrence.

Applicability and Adaptability to Large and Small Institutions

In order to provide as much relevant and useful guidance as possible, the procedures detailed in this Manual include instructions for reviewing the various elements of a compliance management system (CMS), such as written policies and procedures, monitoring and/or audit, and training. When these elements are in place at an institution being examined, the examiner will use the guidance to evaluate their effectiveness. However, the fact that certain elements of a CMS are described in these examination procedures is not intended to suggest that all institutions *must* maintain a CMS that includes all of these elements. Many institutions do not. There is no reason for them to, if their operations do not warrant it. Conclusions about the adequacy of a bank's CMS must be based on the effectiveness of those elements that are in place, taken as a whole, for that bank's particular operations.

For example, assume two institutions – a large, complex bank and a small, non-complex bank – each has a record of strong compliance with all regulations that apply to the products and services it offers. Because of the complex nature of its operations, the large bank's CMS includes comprehensive external audits and formalized training from third-party vendors. The smaller bank's CMS includes no internal or external audits and no formalized training except for the compliance officer, who trains bank staff individually when needed. After reviewing all relevant material available, the examiner finds no significant deficiencies in the small bank's CMS and no reason to believe that the adoption of an audit function or formalized training is necessary to ensure ongoing compliance. The examiner would not criticize the small bank for the absence of audit (or formal training.) Nor should the examiner feel obliged to assign a higher rating to the larger bank simply because its CMS has more elements than the smaller bank. This is because each bank has a CMS that is adequate for the compliance responsibilities that are incumbent upon it due to its operating environment.

The descriptions of CMS elements provided in the Manual will assist the examiner in evaluating the element if one exists and in suggesting content if he or she determines that management should consider adopting an element.

Role of the Compliance Examiner

Compliance examiners play a crucial role in the supervisory process. The compliance examination, and follow-up supervisory attention to an institution's compliance program deficiencies and violations, helps to ensure that consumers and businesses obtain the benefits and protections afforded them under federal law. To this end, an examiner's efforts should help the financial institution improve its compliance posture and prevent future violations.

Primarily, examiners must:

- establish an examination scope focused on areas of highest consumer harm risk;
- evaluate an institution's compliance management system;

- conduct transaction testing where risks intersect with weaknesses in the compliance management system or uncertainties about aspects of that system; and
- report findings to the Board of Directors and management of the institution.

As part of the examination process, examiners are expected to:

- take a reasoned, common sense approach to examining and use sound judgment when making decisions;
- maintain ongoing communication with financial institution management throughout an examination;
- assist an institution to help itself improve performance by providing management with sound recommendations for enhancing its compliance management system;
- share experiences and knowledge of successful compliance management systems; and
- provide guidance regarding the various consumer protection and fair lending laws and regulations.

Overview of the Examination Process

Compliance examinations primarily involve three stages: pre- examination planning; review and analysis, both off-site and on-site; and communicating findings to institution management via meetings and a report of examination.

Pre-examination Planning

Pre-examination planning involves gathering information available in FDIC records and databases, contacting the financial institution to review and narrow the draft request for information and documents, and delivering a letter to the institution requesting specific information and documents for detailed analysis by the examination team (*see* Section III). Proper examination preparation and planning maximizes an examination team's time and resources.

Review and Analysis

During the review and analysis phase of an examination, an examiner thoroughly evaluates an institution's compliance management system to assess its quality and effectiveness, and documents system weaknesses and violations of federal consumer protection laws and regulations, if any. The EIC starts by analyzing information about the type, level, and complexity of the institution's operations, and begins to develop the scope of the examination and plan for resource deployment to areas of highest risk. The EIC also preliminarily assesses the potential risk of consumer harm based upon the information available at the time of pre-examination planning.

The scope of an examination will be preliminarily established prior to entering the financial institution, and should be refined through the results of examiner discussions with management, the compliance officer (or staff assigned), and the internal auditor. Consistent with the FDIC's approach, examination resources are focused on addressing the areas of highest consumer harm risk. Additionally, there may be some cases where the EIC may include additional areas in the examination scope even though consumer harm risk is not exhibited. While on-site at an institution, an examiner may limit the scope of the compliance review based on reliable procedures and controls in place. Similarly, the examiner may expand the review based on, for example, management's view about compliance, a lack of necessary procedures or controls, the presence of violations, the identification of potential or actual consumer harm, or the presence of new or significantly amended regulations. The compliance review continues with an evaluation of the:

- commitment of the Board of Directors, management, and staff to compliance;
- qualifications of the compliance officer or designated staff;
- scope and effectiveness of compliance policies and procedures;
- effectiveness of training;
- thoroughness of monitoring and any internal/external reviews or audits; and
- responsiveness of the Board and management to the findings of internal/external reviews and to the findings of the previous examination.

An examiner must consider the size, level, and complexity of an institution's operations when evaluating the adequacy of an institution's compliance management system.

The examination procedures outlined in this Manual are designed to enable an examiner to identify and measure compliance risk; make an assessment of an institution's compliance infrastructure and methods for identifying, monitoring, and controlling compliance risk and potential consumer harm; and determine the transaction testing needed to assess the integrity of the compliance management system. The number of transactions selected and the type of sampling used should be relative to the perceived risk of consumer harm and the need to assess the level of compliance in an activity or function.

At the conclusion of the review and analysis phase, an examiner:

- summarizes all findings regarding the strengths and weaknesses of an institution's compliance management system;

- determines the cause(s) of programmatic deficiencies or Level 3 or Level 2 violations and relates them to the underlying root causes as well as specific weakness(es) in the institution's compliance management system; and

- identifies actions necessary to address deficiencies or violations.

Determining the cause(s) of a program deficiency or violation is critical to recommending solutions that will successfully address problem areas and strengthen an institution's compliance posture for the future.

Communicating Findings

Examiners must discuss findings and recommendations with management and obtain a commitment for corrective action. These discussions will be held during the course of the examination and at an exit meeting with management and/or the Board of Directors.

The results of the examination will also be communicated to the Board of Directors and management of the institution in a Report of Examination. The Report of Examination provides an account of the strengths and weaknesses of a compliance management system. It is more than an exception-based document and should add value to the institution's compliance efforts.

Distinguishing Between Laws, Regulations, and Supervisory Guidance

Supervisory communications should distinguish clearly and accurately between the requirements of laws and regulations, which are legally binding and enforceable, and supervisory guidance, which is not itself enforceable but sets forth information including the factors the FDIC considers when exercising its supervisory authority.

As articulated in the *Interagency Statement Clarifying the Role of Supervisory Guidance dated September 17, 2018 (FIL-49-2018)*, unlike a law or regulation, supervisory guidance does not have the force and effect of law, and the agencies do not take enforcement actions based on supervisory guidance. Rather, supervisory guidance outlines the agencies' supervisory expectations or priorities and articulates the agencies' general views regarding appropriate practices for a given subject area.

Examiners will not criticize a supervised financial institution for a "violation" of supervisory guidance. Rather, any citations will be for violations of law, regulation, or non-compliance with enforcement orders or other enforceable conditions. During examinations and other supervisory activities, examiners may identify deficiencies in compliance risk management, or other areas that do not constitute violations of law or regulation. In some situations, examiners may reference (including in writing) supervisory guidance to provide examples of appropriate consumer protection practices, and other actions for addressing compliance with laws or regulations.

References

FIL-49-2018: *Statement Clarifying the Role of Supervisory Guidance*