Office of Inspector General

September 2007
Report No. AUD-07-015

DSC's Examination Assessment of Financial Institutions' Compliance Management Systems

AUDIT REPORT

Office of Audits

OIG

Office of Audits

OIG

Report No. AUD-07-015
September 2007

DSC's Examination Assessment of Financial Institutions' Compliance Management Systems

Background and Purpose of Audit

Compliance examinations are the primary supervisory tool the FDIC uses to determine whether a financial institution is meeting its responsibility to comply with the requirements of federal consumer protection laws and associated regulations.

In the mid-1990s, the FDIC introduced risk-scoping in the compliance examination process. In June 2003, as part of the continued focus on risk-scoping, the FDIC revised the compliance examination process to increase attention on an institution's compliance management system (CMS). Although not required by law or regulation, the FDIC has stated it expects the institutions it supervises to have an effective CMS designed to aid compliance with consumer protection laws and regulations. Three interdependent elements comprise a CMS: a board of directors and management oversight; a compliance program (including policies and procedures, training, monitoring, and consumer complaint response); and periodic compliance audits.

The audit objective was to determine whether the FDIC's Division of Supervision and Consumer Protection (DSC) is adequately assessing institutions' CMSs during compliance examinations.

To view full report, go to www.fdicig.ov/2007reports.asp

Results of Audit

Our review of seven sampled institutions showed that the examiners had adequately assessed each financial institution's CMS as part of the related compliance examination. Specifically, the examiners (1) completed a preliminary risk assessment that addressed each institution's CMS to assist in risk-scoping the examination and (2) documented support for examination conclusions regarding the CMS. Additionally, the Reports of Examination (ROE) for the seven institutions addressed each CMS element, as shown in the table below, and included a summary statement and conclusion on the quality of each financial institution's compliance management practices for each element. Also, where significant violations were identified, the examiner tied the cause of the violation to one of the CMS elements in the ROE.

Examiner Assessment of CMS Elements

CMS Elements	The ROE Included a Conclusion on Each Element						
	1	2	3	4	5	6	7
Board and Management Oversight	✓	✓	✓	✓	✓	✓	✓
Compliance Program	✓	✓	✓	✓	✓	✓	✓
Compliance Audit	✓	✓	✓	✓	✓	✓	✓

Key
✓A conclusion was in the ROE, and there was documented evidence of examination work performed.

Source: OIG analysis of the ROEs.

Recommendations and Management Response

Based on the FDIC's establishment of examination guidance related to assessing an institution's CMS during a compliance examination and evidence of examiner implementation of the guidance, we concluded our audit. The report does not make any recommendations. DSC management commented that it was committed to assuring that financial institutions implement effective consumer protection safeguards by maintaining strong CMSs.

TABLE OF CONTENTS

ACRONYMS

CMS	**Compliance Management System**
DSC	**Division of Supervision and Consumer Protection**
FIL	**Financial Institution Letter**
RD	**Regional Director**
ROE	**Report of Examination**
RPSM	**Risk Profile and Scope Memorandum**

Federal Deposit Insurance Corporation
3501 Fairfax Drive, Arlington, VA 22226

Office of Audits
Office of Inspector General

DATE: September 26, 2007

MEMORANDUM TO: Sandra L. Thompson, Director
Division of Supervision and Consumer Protection

/Signed/
FROM: Russell A. Rau
Assistant Inspector General for Audits

SUBJECT: *DSC's Examination Assessment of Financial Institutions' Compliance Management Systems*
(Report No. AUD-07-015)

This report presents the results of our audit of the FDIC's Division of Supervision and Consumer Protection's (DSC) examination assessment of financial institutions' compliance management systems (CMS). Although not required by law or regulation, the FDIC has stated that it expects each FDIC-supervised financial institution to have an effective CMS adapted to its unique business strategy and designed to aid compliance with consumer protection laws and regulations. The objective of the audit was to determine whether DSC is adequately assessing financial institutions' CMSs during compliance examinations.

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.**

Source: The FDIC's *Compliance Examination Handbook.*

We conducted this performance audit in accordance with generally accepted government auditing standards. Appendix I of this report discusses our audit objective, scope, and methodology in detail. We concluded our fieldwork after a review of examination documentation[1] and discussions with examiners and field office supervisors for a limited sample of seven compliance examinations and the performance of related audit procedures.

BACKGROUND

Financial institutions are required to comply with federal consumer protection laws and regulations. Noncompliance can result in harm to consumers as well as monetary penalties, litigation, and formal enforcement actions against the institution. The

[1] The examination documentation included: (1) the Report of Examination (ROE), (2) the Risk Profile and Scope Memorandum (RPSM), (3) examiner work papers, and (4) DSC's System of Uniform Reporting of Compliance and Community Reinvestment Act Examinations (SOURCE).

responsibility for ensuring an institution is in compliance rests with the board of directors and management of the institution.

As the federal supervisor of more than 5,000 financial institutions, the FDIC conducts compliance examinations for each FDIC-supervised financial institution every 12 to 36 months, depending on the prior compliance examination rating and the asset size of the institution. These examinations are the primary tool the FDIC uses to determine whether a financial institution is meeting its responsibilities to comply with consumer protection requirements. The FDIC also promotes compliance with the requirements of federal consumer protection laws and regulations through outreach programs, which include attendance at bankers' forums and conferences, and various supervisory activities.

FDIC Institution and Examination Guidance for a CMS

In the mid-1990s, the FDIC introduced risk-scoping into the compliance examination process. The goal of risk-scoping was for examiners to focus attention on regulatory areas that posed the greatest risk to the institution and the greatest potential harm to customers. In 2003, the FDIC built upon that approach by initiating top-down, risk-focused compliance examinations that increased attention on a financial institution's CMS in order to emphasize a financial institution's responsibility to ensure it complies with consumer protection laws and regulations.

The FDIC notified the financial institutions it supervises of its revised compliance examination approach through Financial Institution Letter (FIL) 52-2003, *Revised Compliance Examination Process;* and FIL-10-2007, *Compliance Examination Handbook,* which replaced the compliance examination procedures. The FDIC also issued Regional Directors (RD) Memorandum 2005-035, *Revised Compliance Examination Procedures,* dated August 18, 2005; and RD Memorandum 2006-034, *Compliance Examination Handbook,* dated October 24, 2006, to transmit the revised compliance examination procedures to its examination staff. The *Compliance Examination Handbook* outlines procedures to guide the examiner through an assessment of an institution's CMS and assists the examiner in identifying specific areas of weakness for further analysis.

Elements of an Effective CMS

According to the FDIC's *Compliance Examination Handbook*, the three interdependent elements shown in Table 1 commonly comprise an effective CMS. The handbook states that when the three elements are strong and working together, an institution has an increased likelihood of being successful at managing its compliance responsibilities, including ensuring that it complies with federal consumer protection laws, regulations, and guidelines.

Table 1: Interdependent Elements of an Effective CMS

Element	Description
Board of Directors and Management Oversight	The board of directors 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 great degree, the success of an institution's CMS is founded on the actions taken by its board and senior management. Key actions that a 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, • 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, • conducting periodic compliance audits, and • providing for recurrent reports by the compliance officer to the board.
Compliance Program	A financial institution should generally establish a formal, written compliance program. A compliance program includes the following components: • policies and procedures, • training, • monitoring, and • consumer complaint response. A well-planned, implemented, and maintained compliance program will prevent or reduce regulatory violations and provide cost-efficiencies and is a sound business step. It is expected that no two compliance programs will be the same and that a program will be dictated by numerous considerations, including: • institution size, number of branches, and organizational structure; • business strategy of the institution (e.g., community bank versus regional; or retail versus wholesale bank); • types of products; • location of the institution—its main office and branches; and • other influences, such as whether the institution is involved in interstate or international banking.
Compliance Audit	A compliance audit is an independent review of an institution's compliance with consumer protection laws and regulations and adherence to internal policies and procedures. The audit (1) helps management ensure ongoing compliance and identify compliance risk conditions and (2) complements the institution's internal monitoring system. The board of directors 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: • organization and staffing of the compliance function, • complexity of products offered, and • outsourcing of functions to third-party service providers.

Source: *Compliance Examination Handbook*.

RESULTS OF AUDIT

Our review of compliance examinations for seven sampled institutions showed that the examiners had adequately assessed each financial institution's CMS. Specifically, the examiners completed a preliminary risk assessment that addressed each institution's CMS to assist in risk-scoping the examination and documented support for examination conclusions regarding the CMS. Additionally, the ROEs for the seven institutions addressed each CMS element and included a summary statement and conclusion on the quality of the financial institution's compliance management practices for each element as shown in Table 2 below. Also, where significant violations were identified, the examiner tied the cause of the violation to one of the CMS elements in the ROE.

Table 2: Examiner Assessment of CMS Elements

CMS Elements	The ROE Included a Conclusion on Each Element						
	1	2	3	4	5	6	7
Board and Management Oversight	✓	✓	✓	✓	✓	✓	✓
Compliance Program	✓	✓	✓	✓	✓	✓	✓
Compliance Audit	✓	✓	✓	✓	✓	✓	✓
Key ✓A conclusion was in the ROE, and there was documented evidence of examination work performed.							

Source: OIG analysis of ROEs for the seven institutions.

Examiner Review of CMS Implementation

According to the *Compliance Examination Handbook*, the examiner must assess the financial institution's CMS as it applies to key operational areas and evaluate the risk of non-compliance with applicable laws and regulations. For each examination we reviewed, the examiner documented the preliminary risk assessment of the institution's CMS in the RPSM. In our review of documentation of examiner fieldwork, we saw varying levels of evidence documenting the examiner's assessment of a financial institution's CMS. For example, in reviewing the board and management oversight element, we saw examiner interview notes about board meetings or copies of meeting minutes in the examiner's documentation. In reviewing examiner documentation for the compliance program element, we saw, in some instances, copies of compliance policies and procedures annotated with the examiner's comments or a chart summarizing the examiner's review of a consumer complaint response. In reviewing examiner documentation for the compliance audit element, we found the examiners had documented the review of the audit committee meeting minutes. We also saw an instance where the examiner had documented audit memoranda, audit plans, and a summary status of audit exceptions. Although examination documentation varied, in each case, we were able to determine that work had been performed in support of the examiner's conclusions in the ROE.

The *Compliance Examination Handbook* states that the ROE must assess the strengths of the institution's CMS, clearly identify the most critical deficiencies and related causes, and aid the institution's board of directors and management in developing an action plan

to address the findings. The ROEs for the seven institutions discussed the overall quality of the financial institutions' CMSs and the examiners' conclusions for each CMS element, beginning with a summary statement about the quality of the financial institution's compliance management practices (strong, adequate, or weak) for each element.

Also, in accordance with the *Compliance Examination Handbook*, where significant violations were identified, the examiner tied the cause of the violation to an element of CMS in the ROE. For example, one institution had a Truth in Lending Act violation resulting from the failure to include the life-of-loan flood determination fees in the finance charge, resulting in an understated finance charge. The ROE attributed the violation to insufficient training and the bank staff's lack of awareness of the disclosure requirement and made recommendations to the board to improve the CMS in this area. The following excerpt from one of the ROEs we reviewed provides an example of how examiners concluded on each of the three CMS elements.

ROE Excerpt

COMPLIANCE MANAGEMENT SYSTEM

Board of Directors and Management Oversight

Board and management oversight is considered strong. Management at all levels is knowledgeable of consumer compliance laws and regulations and is committed to an effective compliance program. The Board provides sufficient resources and authority to management and compliance personnel. The Board has formally appointed … as the bank's compliance officer. Board members receive training quarterly from … to keep current with new laws and regulations. Audit and monitoring findings, as well as recommendations, are presented to the Board during the quarterly compliance meetings. In addition, policies, including compliance, are reviewed and approved by the Board annually.

Source: OIG review of examination documentation.

Conclusion

Based on the FDIC's establishment of examination guidance related to assessing an institution's CMS during a compliance examination and evidence of examiner implementation of the guidance, we concluded our audit. This report does not make any recommendations.

CORPORATION COMMENTS

On September 19, 2007, the Director, DSC, provided a written response to a draft of this report. DSC's response is presented in its entirety as Appendix III of this report. DSC stated that it is committed to assuring that financial institutions implement effective consumer protection safeguards by maintaining strong CMSs and will continue to emphasize this important area of risk through its supervisory programs.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The audit objective was to determine whether DSC is adequately assessing institutions' CMSs during compliance examinations. We conducted this performance audit from May through August 2007 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our observations.

Scope and Methodology

The scope of the audit focused on reviewing policies, procedures, and practices for the examiner's assessment of a financial institution's CMS during a compliance examination. We concluded our fieldwork after a review of the examination documentation for a limited sample of compliance examinations for seven financial institutions.

We reviewed the FDIC's *Compliance Examination Handbook,* which includes guidance for the examiner's assessment of a financial institution's CMS, and performed the following:

- Obtained an understanding of:
  - the CMS expectations for financial institutions,
  - the CMS examination procedures,
  - the level of examiner assessment of the CMS,
  - how the CMS assessment results are used by the examiners to risk-scope the compliance examination and rate the financial institution, and
  - the impact of the CMS assessment on the overall results of the compliance examination process.

- Met with and interviewed DSC officials and staff in headquarters and in the three DSC field offices.

- Reviewed laws and regulations and other criteria pertaining to CMS, including:
  - FILs,
  - RD Memoranda, and
  - guidance on the Federal Financial Institutions Examination Council[2] Web site.

- Reviewed the *Formal and Informal Action Procedures Manual,* dated December 2005, covering administrative procedures affecting the processing and monitoring of

[2] The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, FDIC, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision and to make recommendations to promote uniformity in the supervision of financial institutions.

corrective actions against financial institutions, including addressing violations of laws and other weaknesses in financial institutions.

- Confirmed with OIG Counsel that there are no statutory or regulatory requirements for financial institutions to have a CMS.

- Selected a limited, non-statistical sample of compliance examinations for review.[3] As of March 20, 2007, there were 5,238 active banks identified in DSC's online resources. We pulled a random sample of 45 banks that had compliance examinations completed from January 1, 2006 through March 20, 2007. From that random sample, we selected seven examinations for review based on the size of the institutions, the compliance ratings, and location.

- Reviewed examiner documentation for the selected compliance examinations in DSC's Holyoke, South Boston, and Minneapolis field offices.

- Reviewed congressional correspondence relating to improving federal consumer protection efforts.

- Reviewed a Risk Analysis Center presentation, dated January 2007, on the *New Compliance Examination Handbook.*

- Identified and reviewed applicable DSC Internal Control and Review Section reports, including *Internal Control and Review-Field Territory Reviews: Potential Strong Practices,* dated January 2006.

- Reviewed the Office of Enterprise Risk Management *2006 Accountability Listing* for DSC compliance and consumer protection.

- Identified CMS examination procedures for the Office of Thrift Supervision, Office of the Comptroller of the Currency, and the Board of Governors of the Federal Reserve System.

- Reviewed FDIC *Supervisory Insights* journals from summer 2004 through winter 2006, for information on compliance examinations and CMS.

[3] The results of a non-statistical sample cannot be projected to the intended population by standard statistical methods.

- Reviewed and evaluated the following performance measurement planning documents:
  - *FDIC Strategic Plan* (2005-2010)
  - *FDIC Annual Performance Plan* for 2006 and 2007
  - *FDIC Corporate Performance Objectives* for both 2006 and 2007
  - *FDIC 2006 Annual Report*

Internal Controls

We gained an understanding of relevant internal controls by reviewing the: (1) DSC Internal Control and Review Section's internal review reports; (2) FDIC policies and procedures, such as FILs and RD Memoranda related to compliance examinations and the Relationship Manager Program;[4] (3) *Compliance Examination Handbook*; and (4) examination procedures for assessing institution performance related to a CMS. In addition, we interviewed DSC individuals to obtain an understanding of how examiners use examination guidance to assess institutions' CMSs during compliance examinations, including how compliance examiners and the field office supervisors coordinate the performance of work with risk management examiners.

Reliance on Computer-based Data

Our audit objective did not require that we assess the reliability of computer-based data. We obtained certain data from SOURCE to identify the universe of banks that had a compliance examination completed from January 1, 2006 through March 20, 2007. However, for purposes of our audit, we did not rely on computer-based data to support our observations or conclusions.

Compliance With Laws and Regulations

In conducting the audit, we confirmed with the FDIC's OIG Counsel that there were no federal statutory or regulatory requirements for financial institutions to have a CMS. We did identify various consumer protection laws and regulations applicable to financial institutions.

Government Performance and Results Act

The Government Performance and Results Act of 1993 directs federal agencies to develop a strategic plan and annual performance plan to help improve federal program effectiveness. We reviewed the FDIC's *Strategic Plan* for 2005-2010 and the *FDIC Annual Performance Plan* for 2006 and 2007. We determined that the FDIC has a strategic goal and objective related to ensuring consumers' rights are protected and that FDIC-supervised institutions comply with consumer protection and fair lending laws.

[4] The Relationship Manager Program objectives include: improving communication, increasing flexibility for risk-focused supervision, and providing a comprehensive ROE that includes all supervisory ratings and addresses material findings in all areas.

The FDIC also has a 2007 performance goal to determine the need for changes in current FDIC practices for following up on significant violations of consumer protection laws and regulations identified during examinations of banks. We reviewed the FDIC's *Corporate Performance Objectives* for 2006 and 2007 and the *FDIC 2006 Annual Report*. We determined that there were no specific strategic objectives or goals directly related to DSC's examination assessment of a financial institution's CMS.

Fraud and Illegal Acts

We did not develop specific procedures to detect fraud and illegal acts because they were not considered material to the audit objective. However, throughout our review, we were sensitive to the potential for acts of fraud and illegal acts, and none came to our attention.

Prior Audit Coverage

The OIG has conducted two prior audits related to compliance examinations. We discussed the audits with the OIG Auditors-in-Charge and reviewed their work papers and the *Status of DSC Corrective Action* reports for the prior audits. Additionally, we performed a comparative analysis of the results of the prior audit reports, listed below, to our audit objective, scope, and methodology.

Audit Report No. 05-038*, Audit of DSC's Risk-Focused Compliance Examination Process*, issued September 2005. The objective of this audit was to determine whether DSC's risk-focused compliance examination program resulted in examinations that were adequately planned and effective in assessing financial institution compliance with consumer protection laws and regulations. We recommended that the Director, DSC, clarify and reinforce requirements that examiners adequately document the scope of work performed, including transaction testing and spot checks of the reliability of the institutions' compliance review functions, during the on-site portions of compliance examinations.

Audit Report No. 06-024*, Audit of DSC's Supervisory Actions Taken for Compliance Violations*, issued September 2006. The objective of this audit was to determine whether DSC adequately addressed the violations and deficiencies reported in compliance examinations to ensure that FDIC-supervised institutions took appropriate corrective action. We recommended that the Director, DSC, strengthen guidance related to the monitoring and follow-up processes for compliance violations by revising: (1) the *Compliance Examination Procedures* to require follow-up between examinations on repeat, significant compliance violations and program deficiencies; (2) the *Formal and Informal Action Procedures Manual* to require consideration of supervisory actions when any institution's corrective action on repeat, significant violations is not timely or when repeat, significant violations are a recurring examination finding; and (3) DSC's performance goals to focus more broadly on institutions with repeat, significant violations.

APPENDIX II

FINANCIAL INSTITUTION LETTERS AND RD MEMORANDA

Financial Institution Letters	Description/Summary
• FIL-10-2007, *Compliance Examination Handbook*, January 30, 2007	The *Compliance Examination Handbook* replaced the *Compliance Examination Manual* in June 2006 and includes guidance for examiner assessment of an institution's CMS.
• FIL-52-2003, *Revised Compliance Examination Process*, June 20, 2003	The FDIC's revisions to its process for examining FDIC-supervised depository institutions to determine their compliance with consumer protection laws and regulations. The revised process focuses increased attention on an institution's CMS.
DSC Regional Directors Memoranda	
• 2006-034, *Compliance Examination Handbook*, October 24, 2006	Transmitted the total revision and replacement of the *Compliance Examination Manual*. The handbook captures outstanding examination policies and procedures in effect as of June 30, 2006.
• 2005-035, *Revised Compliance Examination Procedures*, August 18, 2005	Transmitted revised compliance examination procedures for on-site reviews beginning on or after January 1, 2006.

APPENDIX III

CORPORATION COMMENTS

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990
Division of Supervision and Consumer Protection

DATE: September 19, 2007

TO: Russell A. Rau
Assistant Inspector General for Audits

FROM: Sandra L. Thompson [signed]
Director

SUBJECT: Response to Draft Report Entitled:
DSC's Examination Assessment of Financial Institutions' Compliance Management Systems (Assignment No. 2007-017)

The Division of Supervision and Consumer Protection appreciates that you found FDIC examiners effectively assessed financial institution's Compliance Management Systems (CMS) and appropriately presented findings in Reports of Examination.

We are committed to assuring that financial institutions implement effective consumer protection safeguards by maintaining strong CMS. We will continue to emphasize this important area of risk through our supervisory programs.