Review and Analysis

Introduction

The FDIC's compliance examination process assesses how well a financial institution manages compliance with federal consumer protection laws and regulations. The review and analysis phase of the compliance examination starts with a top-down, comprehensive evaluation of the compliance management system (CMS) used by the financial institution to identify, monitor, and manage its compliance responsibilities and risks. The procedures outlined below guide the examiner through an assessment of an institution's CMS, and assist the examiner in identifying specific areas of weakness for further analysis. Many procedures listed in this section can be performed at the field office or other location prior to the on-site portion of the examination, if materials are available.

Off-Site Review and Analysis

The Examiner-in-Charge (EIC) reviews and analyzes the material gathered from FDIC, third parties, and the institution in response to the Compliance Request Letter in order to develop the risk profile and scope memorandum and plan the on-site portion of the examination. This review and analysis should be broad enough to obtain an understanding of the organizational structure of the institution, its related activities, and compliance risks associated with each of its activities.

The review should be used to preliminarily determine whether the institution's management and Board of Directors identify, understand, and adequately control the elements of risks facing the financial institution. In general, management and Directors are expected to have a clearly defined system of risk management controls governing the institution's compliance operations, including those activities conducted by affiliates and third-party vendors. During this review the EIC should consider what types of questions should be asked while on-site to test whether the bank's written policies and procedures accurately reflect actual operations.

Risk Profile and Scope Memorandum

The goal of a risk-focused, process-oriented examination is to direct resources toward areas with higher degrees of risk. To accomplish this goal, 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. The result of this assessment is the Risk Profile, a matrix and narrative that summarizes the perceived risks, and provide the basis for preparing the Scope Memorandum. The Scope Memorandum describes the focus of the examination, including issues to be investigated and regulatory areas to be targeted during the examination.

A Risk Profile and Scope Memorandum template should be downloaded from SOURCE at the beginning of the examination process. SOURCE will automatically populate it with relevant information from other FDIC databases. After conducting the off-site review and analysis, the examiner should document the preliminary risk assessment and expected examination scope in the Risk Profile and Scope Memorandum, and obtain and document appropriate approval. During the examination the EIC should obtain approval for any material changes to the scope of the examination, in accordance with regional or field office requirements.

At the conclusion of the examination the EIC must review the preliminary Risk Profile and Scope Memorandum developed at the beginning of the examination and edit it as needed to reflect the actual scope of the examination. The final Risk Profile and Scope Memorandum should be posted to SOURCE, making it available to all staff and management during the exam review and for future internal use, especially for the start of the subsequent examination.

Additional information about crafting the Risk Profile and Scope Memorandum is provided in the following sections.

Developing a Risk Profile

In order to properly assess a financial institution's risk, the EIC or designee reviews the following primary areas:

Compliance Management System:

- Management and Director Oversight
- Compliance Program
  - Policies and Procedures
  - Training
  - Monitoring Procedures
  - Complaint Response
- Audit Procedures

Operational Areas:

- Lending
- Deposits
- Insurance Sales
- Investment Sales
- Other Products or Issues

The resulting risk profile compares the strength of the CMS to the risks attendant to particular operational areas.

While reviewing a bank's operations, the examiner should consider the impact of the following types of risk:

Performance Risk:

- Current & Past Enforcement Actions
- Reimbursement History
- History of Compliance with Fair Lending laws

- Current and Prior Regulator Ratings
- Audit Findings

Regulation Risk:

- Applicable Regulations
- New Regulations
- Changes to Regulations
- Recent Case Law

Product/Service Risk:

- Major Product Line
- New Products/Services
- Growth in Operations
- Complexity of Operations
- Third-Party Affiliations

Performance Risk: The financial institution's past compliance performance is an important consideration when developing its risk profile. Historic effectiveness of the compliance management system, including the results of previous examinations and management's record of taking corrective measures, will impact its risk profile and ultimately, the scope of the examination. The most recent compliance history should be given the most weight. The EIC will be able to locate performance risk information in various areas, including the FDIC's correspondence and enforcement records for the subject institution. The most recent Risk Management report and workpapers may contain additional information on the bank's performance risk (e.g. comments regarding institution management).

Regulation Risk: Regulation risk measures the possible consequences to the bank and its customers of noncompliance with specific regulatory provisions. Regulation risk recognizes that the impact of noncompliance differs depending on the consumer law or regulation. For the public, it is the measurement of relative adverse financial impact or other harm that noncompliance may produce. For the bank, regulation risk is the measurement of legal, reputation, and financial harm that noncompliance may produce. For example, the financial harm both to the bank and to consumers associated with violations of the Truth in Lending Act (Regulation Z) requiring reimbursements far exceeds the consequences of an isolated undocumented check hold. The level of regulation risk is affected by such factors as:

- Potential financial and/or reputation harm to consumers;
- Potential legal, reputation, and financial harm to a bank;
- New laws, regulations or amendments thereof; and
- The amount of transaction activity subject to a specific regulation.

Product/Service Risk: The institution's products and services impact the bank's risk depending upon the financial institution's size, market share and portfolio concentration. The complexity of products offered and the associated likelihood of error should be considered. Third-party affiliations present heightened risk, particularly for product delivery, but also for any operation, product, service or activity provided or conducted by a third party on behalf of the institution. Finally, the institution's strategic plan for growth and for the introduction of new products and services should also be taken into account.

Taking into consideration the conclusions drawn in each of the preceding components, and any other pertinent information, the examiner should develop a risk profile of the institution by assigning and adequately supporting a category of Low, Moderate, or High compliance risk for each CMS element and operational area. An institution with a Low Risk Profile in a particular area will effectively manage compliance risks. The institution's Board and management actively participate in managing the CMS, the CMS is considered strong, and historic examinations support this assessment. Spot checks of transactions may be appropriate to verify continued strength. An institution with a Moderate Risk Profile is generally effective, but specific weaknesses are identified or suspected. Some particularized transaction testing should be planned. An institution with a High Risk Profile is ineffective in identifying, monitoring, or managing compliance risks in particular operational areas. Significant risk is readily apparent and may be supported by prior examination findings. Institutions in this category will require more extensive transaction testing in light of the risks of non-compliance. (Specific issues to be investigated and areas to be targeted with transaction testing should be addressed in the Scope Memorandum, which is discussed in the next Section.)

It is important to remember that one element of a financial institution's compliance efforts may influence another area. Be aware of relationships and their mutual impact. For example, if the initial review of bank practices identifies a lack of audit of loan denials, the examiner should look to see whether monitoring procedures are in place to mitigate the impact of the lack of audit procedures. The existence of monitoring procedures may lead the examiner to determine that the absence of an audit does not raise the institution's risk profile. Conversely, if the initial review of bank policies and procedures identifies well-organized written guidelines for deposit compliance management, the examiner should also consider the bank's record of oversight in this area. If deposit compliance has historically suffered from poor management oversight, then the existence of written procedures should be given less weight when determining the risk profile.

The following matrix should be completed as an illustration of the bank's overall Risk Profile. Each column/row intersection

should be labeled as presenting a (L)ow, (M)oderate, or (H)igh level of compliance risk for the institution. The narrative accompanying the matrix should summarize the perceived risks with sufficient information to support the risk ratings, including particular performance, regulation or product risks.

Risk Profile Matrix and Summary

Institution Name City, State	CMS Elements Oversight	Program	Audit
Operational Areas:			
Lending			
Deposits			
Insurance			
Investment Sales			
(Other)			
Other Issues:			
( )			
( )			

(L) = Low Risk; (M) = Moderate Risk; (H) = High Risk

Developing a Scope Memorandum

The EIC should prepare a Scope Memorandum using the information reflected in the preliminary Risk Profile. The Scope Memorandum must be in writing and should address the following:

- Scope of the examination;
- Issues to be investigated or areas to be targeted, and reasons why; and
- Areas not included in the examination scope, and reasons why.

The severity of CMS weakness and operational risk will dictate the intensity of transaction testing, as examination resources are focused in areas where risk is identified, either prior to or during the examination. If limited risk is identified or if the bank has mitigated the identified risk, then no Transaction Testing would be required even if the area was not reviewed at the last examination. The exception would be those areas that are always identified as high risk, specifically, Flood Insurance, HMDA, and Fair Lending, which should always be Transaction Tested.

In the final Risk Profile and Scope Memorandum, the narrative in the Scope Memorandum describing changes should be in a different typeface for ease of reference. Do not delete the initial narrative. If a spot-check of a particular regulation revealed no problems, that should be noted in the Scope Memorandum chart; no Examiner Summary is required. If an Examiner Summary was prepared, it should be referenced in the Scope Memorandum chart.

The Scope Memorandum provides all members of the examination team with a central point of reference throughout the examination. A sample Risk Profile and Scope Memorandum can be found in Section III. Note that the format of the memorandum may be tailored to individual circumstances if appropriate.

On-Site Review and Analysis

Throughout the on-site review and analysis phase of the examination, the examiner should have discussions with senior management, the compliance officer, Directors, and other personnel to develop an understanding of how management approaches its compliance responsibilities. These discussions will enable the examiner to determine whether and to what extent the financial institution has a compliance management system that is integrated into its daily operations.

Entrance Meeting With Senior Management

During the pre-examination planning stage, the EIC should schedule a meeting with senior management (e.g., the president, chief executive officer, compliance officer, and if they wish, members of the Board of Directors). This meeting should take place as soon as possible after entering the financial institution to conduct the on-site portion of the examination and should facilitate the discussion of various administrative items and the scope of the examination. Matters to be discussed during the entrance meeting include:

- An overview of the examination process.
- The names of FDIC examiners involved.
- Anticipated length of the examination.
- The EIC's accessibility throughout the on-site examination to discuss any issues relating to the examination or FDIC policy and practices.
- The identity of the individual(s) who is/are the primary contact person(s) for examination related issues.
- Any issues identified during off-site review and analysis, particularly areas of significant risk that will be receiving close attention.
- The materials requested during PEP that were not provided by the financial institution prior to the on-site date.
- An explanation of the closing management meeting procedures.
- The date of the next Board of Directors/trustees meeting. (Management should be advised that depending upon the examination findings, the FDIC may need to attend the regularly scheduled meeting or call for a special Board meeting.)
- Any issues related to the CRA evaluation and fair lending review.

Examiners should use a written agenda to document the issues covered at the entrance meeting, and file a copy in the examination workpapers.

Ongoing Communication

Communication between financial institution management, Boards of Directors, bank staff, and FDIC examination staff is a major component of an effective examination or visitation. Open communication should be maintained with management during the course of the examination. To the extent possible, all issues of concern should be discussed with management as they arise. This allows management time to provide additional relevant information, or to begin correcting problems where appropriate.

The financial institution's directors/trustees are encouraged to participate in regularly scheduled meetings with examiners. However, examination findings should be discussed with senior management prior to discussing with Board members. Also, the EIC should notify the financial institution's management as early as possible of any plans to meet with the Board to present examination findings. This will provide directors/trustees with an opportunity to forego meetings during the examination, if that is their preference.

Review of the Compliance Management System

Based on information gleaned from the discussions with bank management and staff, along with the off-site review and analysis, the examiner should:

- Determine the quality of the institution's compliance management system, including the degree to which management has taken a proactive approach to compliance and whether management can demonstrate its ability to assure compliance with federal consumer laws and regulations.
- Assess whether the compliance management system is effective at facilitating compliance.
- Identify potential deficiencies in the compliance management system and areas of greatest risk and concern.
- Determine where transaction testing is necessary.

The following sections include question lists that are intended to serve only as general guidance for the matters to be addressed during the examiner's dialogue with bank personnel. The sections are organized by elements of the CMS, and should be considered in conjunction with each of the different operational areas of the bank to come to a conclusion about the strength of each element overall. The questions will not apply to every examination scenario and should be customized to each situation. Examiner judgment must be used to determine whether additional pertinent questions should be asked. Because all the facets of a compliance management system are interrelated, certain themes will be repeated in the question lists for multiple sections. Throughout the examination process, the examiner should refer to the FDIC Law, Regulations and Related Acts service set, and any pertinent outstanding FDIC guidance regarding the regulatory or policy requirements of each area under review.

NOTE: The question lists are not to be given to institution management to complete.

Applicable Statutes and Regulations

The compliance management system must adequately address (through oversight, policies and procedures, training, monitoring, complaint response, and audit) all areas related to the following federal consumer laws, regulations, rules, and policy statements:

Lending

Truth in Lending
Real Estate Settlement Procedures
Homeowners Protection
Credit Practices Rule
Equal Credit Opportunity
Fair Housing
Home Mortgage Disclosure
Fair Credit Reporting
Flood Insurance
Preservation of Consumers' Claims and Defenses
Homeownership Counseling
Servicemembers Civil Relief Act
Consumer Leasing

Deposits

Truth in Savings
Electronic Fund Transfers
Expedited Funds Availability
Interest on Deposits
Overdraft Protection

Other Products

Non-Deposit Products

Privacy/Consumer Information/General Requirements

Advertisement of Membership
Electronic Banking
Privacy of Consumer Financial Information
Right to Financial Privacy
Fair Debt Collection Practices
Children's Online Privacy Protection
Unfair or Deceptive Acts or Practices
Telephone Consumer Protection
Controlling the Assault of Non-Solicited Pornography and Marketing
Health Insurance Portability and Accountability Act
Third Parties

Community Reinvestment Act

CRA Technical Requirements
Deposit Production Offices
Branch Closings
Interstate Banking and Branching

Evaluating Management Oversight

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to management oversight;
- Prior Reports of Examination, including Compliance, Safety and Soundness, and specialty examinations (with a focus on the management component of each);
- Minutes of the meetings of the Board of Directors (BOD), compliance committee, discount committee, etc.;
- New, modified or amended compliance-related policies, procedures, and other internal memoranda;
- All files related to the receipt and resolution of compliance-related consumer complaints archived by the institution or the FDIC, including information from the FDIC's automated complaint tracking system (Specialized Tracking and Reporting System [STARS]);
- Written management and Board response and follow-up to internal and external audits;
- Agreements with third parties to provide products or services such as with and outside vendor to provide compliance services and educational materials, or with a networking broker/dealer to provide brokerage services;
- Institution organizational chart and management résumés; and
- Examiner notes from discussions with the compliance officer, senior managers, etc.

Procedures

1. Review Board and committee minutes. Review of these documents should give the examiner an indication of the following:
   - Extent of Board oversight/involvement in assuring compliance with consumer protection and fair lending laws and regulations by the institution and, as applicable, by third-party providers.
   - Training of Directors and senior management regarding compliance and fair lending issues.
   - Rationale for implementing new policies or procedures or modifying existing ones.
   - Any negative comments on rejected loan applications during loan committee or any other meeting (such records must be traced to the specific loan file to assure that no unlawful disparate treatment or discrimination was involved in the denial).
   - Consideration of new loan or deposit products and strategies for their implementation.
   - Consideration of new software or software vendors.
   - Consideration of third parties for compliance audit.
   - Approval of, and rationale for, branch openings and closings.
   - Whether the Board documented a review of the prior Report that included, as applicable: a discussion of recommendations for policy changes, an adoption of those revisions, and a report regarding corrective action and subsequent testing for identified violations
2. Based on the material reviewed during PEP and on-site, and based on discussions with management, answer the following questions:
   - What is the bank's business strategy and what are the compliance implications of that strategy (for example, elevated risk due to rapidly growing subprime lending, cutting-edge e-banking activities, etc.)?
   - What particular compliance-related areas does management feel are weak or in need of review?
   - Have the Board and senior management worked to foster a positive climate for compliance?
   - Has management allocated the appropriate level of resources to compliance?
   - Does the institution have a designated compliance officer and/or compliance committee? If not, is the absence of an officer or committee significant in light of the institution's resources and risk profile?
   - Has management ensured that the compliance officer(s) and/or compliance committee has the appropriate level of authority and accountability to effectively administer the institution's compliance management system?
   - Has management responded appropriately and promptly to consumer complaints?
   - Has management responded appropriately to deficiencies noted and suggestions made at previous examinations and audits?
   - How does management stay abreast of changes in regulatory requirements and other compliance issues? Is this method appropriate in light of the institution's resources and risk profile?
   - How does management ensure that the institution's staff stays abreast of changes?
   - How does management ensure that compliance is considered as part of new product and service development, marketing, and advertising?
   - How does management ensure that due diligence is performed prior to changing third-party product or service providers, such as software vendors or third-party audit providers?
   - What is the level of management's knowledge of compliance issues?

- Does the review of the Board and/or Compliance Committee minutes indicate a reasonable level of Board involvement?
- Is the Board aware that it is ultimately responsible for the institution's compliance management system?

3. Develop and document a preliminary assessment of the institution's performance related to this area. Is management oversight generally strong, adequate, weak? On what is this assessment based?

Evaluating the Compliance Program

Policies and Procedures

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to policies and procedures, including the institution's business strategy, product offering, branches, third-party relationships, etc.;
- Compliance-related policies and other written compliance procedures;
- BOD minutes and compliance committee minutes; and
- Examiner notes from discussions with the compliance officer, senior managers, etc.

Policies and procedures, whether written or unwritten, should cover all of the areas listed below. A financial institution may have other policies or procedures related to compliance not listed here that should be included in the examiner's review, depending on the institution's activities and risk profile.

- Compliance Policy – This may be a single document or a compilation of various documents each relating to specific areas of institution activity. In addition to specific guidance on daily compliance activities, the policy should provide for an adequate level of responsibility and authority for the compliance officer, compliance committee, and individual employees.
- Lending – Often, institutions will have separate policies for various lending types such as consumer, real estate, commercial, agricultural, etc. All should be reviewed during PEP.
- Deposits – Institutions often have separate policies for Regulation DD, Regulation E, Regulation CC, and Part 329.
- Electronic Banking – The adequacy of e-banking policies should be assessed in light of the level of activity in which the institution is engaged.
- Privacy – Institution privacy policies and procedures vary widely, depending on the level of information sharing involved.
- Non Deposit Products – Policies and procedures must provide adequate guidance for the sale of investment and insurance products by bank employees (including loan officers who sell insurance during the loan process), dual employees, and on-site non-employee brokers.
- Branch Closing Policy – Section 42 of the Federal Deposit Insurance Act requires every financial institution to maintain a branch closing policy.

In order to ensure an accurate assessment of the institution's compliance management system, each policy and procedure must be reviewed during PEP or at the institution unless all the following are true: 1) the policy was reviewed at the prior FDIC compliance examination, 2) the review of the policy at the prior examination found no deficiencies, 3) no changes or amendments have been made since the policy was last reviewed, and 4) there have been no significant regulatory or operational changes pertinent to the area covered by the policy since the prior examination.

1. Conduct sufficient documentation reviews and management discussions to answer the following questions.
   - What areas of compliance do written policies or procedures cover?
   - Which policies or procedures are unwritten?
   - Is the use of unwritten policies/procedures adequate for the institution's needs?
   - Do the policies give effective guidance to institution employees?
   - Are policies and procedures structured and implemented in such a way as to ensure fair and equitable treatment of all consumers?
   - Do the policies assign compliance responsibility? Are the assignments logical and reasonable given the time and resources available to those employees?
   - Do the policies provide appropriate authority to employees responsible for identifying and correcting deficiencies?
   - Are the policies and procedures established in such a way as to ensure a smooth transition in the case of key personnel turnover?
   - Are policies, procedures, and standardized forms periodically reviewed and updated in response to regulatory changes and changes in the institutions risk profile? How frequent are the reviews?
   - Does the Board review and approve all changes to policies and procedures? If not, is the level of approval appropriate given the examiner-determined institution risk profile?
   - Are there any practices that have become policy by virtue of the frequency of their occurrence? If so, do these practices conflict with formal policies or procedures?

NOTE: Additional guidance for the review of loan and appraisal policies is located in the Fair Lending Examination Procedures.

2. Determine whether the institution's policies and procedures provide the appropriate level of guidance for all employees and include clearly defined goals and objectives.
3. Develop and document a preliminary assessment of the institution's performance related to this area. Are policies and procedures considered generally strong, adequate, or weak? On what is this assessment based?

Training

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to training;
- Compliance-related training documentation;
- Examiner notes from discussions with compliance officer, senior managers, etc.

1. Review the institution's training records and have sufficient discussions with management to answer the following questions:
   - Does every employee receive appropriate training given his or her compliance responsibilities?
   - Do third-party service providers receive appropriate training?
   - How often is training conducted? Is the frequency of training acceptable?
   - Is the training program continuously updated to incorporate accurate, complete information on new products and services, regulatory changes, emerging issues, etc.?
   - Is the effectiveness of the training evaluated by management through delayed testing, before-and-after work product reviews, or other means?
   - Regardless of whether staff training is conducted primarily in-house or is out-sourced, does management evaluate whether the institution's training needs are being met? As EIC, do you agree or disagree with management's conclusions?
2. Develop and document a preliminary assessment of the institution's performance related to this area. Is the institution's training considered generally strong, adequate, or weak? On what is this assessment based?

Monitoring

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to monitoring;
- Compliance-related policies and other written compliance procedures;
- Documentation of the results of monitoring activities;
- Formal and/or informal reports to management of the findings, corrective actions, and related follow-up from monitoring procedures; and
- Examiner notes from discussions with the compliance officer, senior manager, etc.

1. Conduct documentation review and have sufficient discussions with management to answer the following questions:
   - What monitoring systems are in place for loan transactions? Deposit transactions? Investment and insurance sales activities?
   - Is every transaction subject to monitoring? If not, what is the level of transactional review? Is the level of monitoring adequate?
   - Does monitoring include a review of the performance by third-party product or service providers?
   - Are the appropriate personnel conducting the monitoring (i.e. someone with daily involvement in the monitored area and who has received adequate training)?
   - How are errors that are identified during the monitoring process documented?
   - How are the errors corrected?
   - Is there appropriate follow-up when errors are identified (i.e. refresher training, disciplinary action)?
2. Determine whether the institution's monitoring efforts encompass all applicable regulations.
3. Develop and document a preliminary assessment of the institution's performance related to this area. Is the institution's monitoring effort generally strong, adequate, or weak? On what is this assessment based?

Consumer Complaint Response

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to consumer complaints;
- Consumer complaint policy or other written compliance procedures regarding complaints;

- All files related to the receipt and resolution of compliance-related consumer complaints archived by the institution or the FDIC, including information from the FDIC's automated complaint tracking system (STARS);
- BOD minutes and compliance committee minutes; and
- Examiner notes from discussions with the compliance officer, senior managers, etc.

1. Conduct documentation review and have sufficient discussions with management to answer the following questions:
   - Has the institution implemented policies and procedures to handle consumer complaints about the institution and, as applicable, third-party providers?
   - If policies and procedures are in place, do they comply with all regulatory requirements regarding complaints (maximum time limits for response, documentation requirements, etc.)?
   - If the institution has received consumer complaints, have all complaints been resolved satisfactorily?
   - Cross-referencing the complaints to all other areas of the compliance management system, does the type or quantity of complaints suggest any other areas in need of in-depth review?
   - Does the institution review complaints to determine whether improvements or changes to products or operations should be made?

2. Develop and document a preliminary assessment of the institution's performance related to this area. Are the institution's consumer complaint response processes generally strong, adequate, weak? On what is this assessment based?

Evaluating the Audit Function

Material to be reviewed during completion of this section will include, at a minimum:

- The examiner-determined risk profile of the financial institution as it relates to the audit function.
- Audit policy, external audit agreement, or other written audit guidelines;
- Compliance-related internal and external audit reports, responses, and follow-up;
- Internal and external audit workpapers;
- Institution organizational chart;
- BOD minutes and compliance committee minutes; and
- Examiner notes from discussions with audit staff, compliance officer, senior managers, etc.

Exception: Do not request fair lending self-testing reports (or results). If, however, a financial institution voluntarily provides documentation of its fair lending self-testing, review the findings as part of the fair lending examination.

NOTE: A financial institution's audit or review of loan files, internal policies, and training material may indicate difference in the treatment of applicants that could constitute a violation of the fair lending laws.

1. Conduct documentation review and have sufficient discussions with management to answer the following questions:
   - Are internal audits conducted? How often and by whom?
   - If internal audits are conducted, is the auditor independent of the transaction being audited? If not, is this considered acceptable considering the institution's resources and risk profile?
   - Are external audits conducted? How often and by whom?
   - Are internal/external audits comprehensive in scope? If audits are not comprehensive, do they cover all areas of significant risk? Do they include reviews at every branch location and of significant third-party relationships?
   - Are audit findings compiled in writing? Do they identify the nature and circumstances (i.e., cause, time period, etc.) of the identified exceptions? Do they provide management enough information to (1) determine cause and (2) formulate an appropriate corrective action?
   - Are internal/external audits of sufficient quality?
   - Are the audit findings communicated to the Board either directly or through the compliance committee?
   - Have audit report findings been appropriately addressed by the Board and senior management in a timely manner and include corrective actions and follow-up efforts?
   - Are written audit reports readily available for examiner review?

2. Develop and document a preliminary assessment of the institution's performance related to this area. Is the audit function generally strong, adequate, or weak? On what is this assessment based?

Transaction Sampling and Testing

After analyzing the CMS elements in relationship to a bank's operational risks, the EIC must decide what transaction sampling and testing is necessary. The number of transactions and the particular regulatory requirements to be reviewed should be carefully tailored to weaknesses identified in the CMS as it relates to specific operational areas. For example, if there is a weakness in monitoring the calculation of Annual Percentage Rates (APRs) in open-end credit transactions,

then a sample of those calculations should be tested; it would not be necessary to test all Truth in Lending Act (TILA) requirements.

The severity of CMS weakness and operational risk will dictate the intensity of transaction testing; greater weakness and higher risk will generally lead to the review of more transactions. If the examiner finds a moderate degree of risk, then sufficient testing should be done to support a conclusion. Depending on the importance of an element, the examiner may find it appropriate to spot-check a couple of transactions to support a favorable conclusion. If no transaction testing in a particular regulatory area was done in the previous examination, then at least a spot-check should be done at the current examination, even if there are no risk indicators. In certain cases, however, management's admission that a violation occurred is sufficient to warrant the citation without transaction testing. This also negates the need to list specific transactions in the Report of Examination (ROE).

When transaction sampling and testing is conducted, the examiner should tailor the actual sample and test to the identified weakness. If testing is not considered necessary to support conclusions about an element of the CMS or with respect to a particular operational area, appropriate documentation should be retained in the workpapers and comments should be included in the Risk Profile and/or ROE to support this conclusion.

Consultation Policy

Consultations and communication between Field, Regional and Washington staff members help maintain the quality and consistency of compliance, fair lending and CRA examinations and supervision. Information communicated informally or through consultations alerts senior DCP officials to significant, unusual or emerging supervisory issues, which ensures that these issues receive appropriate and timely consideration. Current information from examiners in the field also helps the FDIC and interagency groups develop more realistic policies and regulations.

Examination staff should consult with regional or field office management or staff if they find an unusual issue or problem. In turn, regional or field office management and staff are encouraged to consult with Washington subject matter experts, particularly with respect to findings, issues or potential violations requiring guidance with respect to new regulations, or involving emerging/sensitive policy concerns.

Certain situations, because of their sensitivity or potential impact, mandate that the Regional and/or Washington office(s) be consulted. Actions that require either approval or concurrence under delegated authority or DCP policy also require formal documentation.

If a consultation results in an outcome inconsistent with the examiner's recommendation, then the examiner and the review examiner should ensure that the language of the ROE or CRA PE is consistent with the final outcome.

References

DSC RD Memo 08-042: Consultation Policy and Procedures for Consumer Compliance and Community Reinvestment Act Issues

DSC RD Memo 08-020: Guidance for Managing Third Party Risk

DCP RD Memo 2011-026: Consultation Process for Compliance and CRA Examinations

(This page intentionally left blank.)