FOREWORD

The May 2008 change (Change 7) to the Corporate Examiner's Guide (CEG) consists of an update to Chapters 201, 201.1, 202, 203, 204, 205, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311 and 401. Change 7 includes revisions to the Investments (Chapter 201), Asset and Liability Management (Chapter 202), Capital (Chapter 204) Management (Chapter 301), Information Systems and Technology (Chapter 303), Item Processing Service Centers (Chapter 304), Funds Transfer (Chapter 305), ACH (Chapter 306), Contingency Planning (Chapter 307), Compliance (Chapter 308) and Supervisory Committee/Audit Function (Chapter 309) chapters resulting from technological and regulatory changes, as well as general updating of the other aforementioned chapters and certain associated appendices.

As a reminder to those utilizing this manual the CEG remains a guide, not a regulation. The guidance herein is dependable, but may not be the best or final approach in every situation. Examiner judgment and flexibility remain crucial to a successful examination program.

Kent D. Buckham
Director
Office of Corporate Credit Unions

NATIONAL CREDIT UNION ADMINISTRATION
CORPORATE EXAMINER'S GUIDE

The Corporate Examiner's Guide (CEG) provides guidance to National Credit Union Administration (NCUA) examiners for performing examinations and supervision of corporate credit unions. The primary goal is to ensure the overall safety and soundness of the corporate credit union system. While the CEG is intended to provide guidance to examiners, it also offers information corporate credit unions may find useful in understanding the examination and supervision process.

Both state and federal examination staff examine corporate credit unions, depending upon whether the individual corporate is state or federally chartered. Federal examiners normally consist of staff from NCUA's Office of Corporate Credit Unions (OCCU). The OCCU uses a risk-focused examination and supervision process, which emphasizes ensuring corporate credit union management identifies, measures, monitors, reports, and controls the current and projected risk of their operations.

Although the guidance provided in this CEG is dependable, it may not necessarily be the best or final approach in every situation. The risk-focused examination approach requires examiners to exercise their professional judgment to assess the risk inherent in a given corporate credit union operation and determine the scope of the examination taking into consideration the many variables presented by the individual corporate credit union. When examiners determine a safety and soundness concern and/or a regulatory violation exists, they communicate with corporate credit union officials and staff to develop action steps to eliminate the concern(s).

Please be advised it will take you approximately 20 minutes to download the CEG file using a 56k modem. (If your modem speed is less than or greater than 56k it will take you more or less time).

If you have questions that are not addressed in the CEG, please contact the OCCU at (703) 518-6640.

MISSION

OCCU MISSION

The Mission of the Office of Corporate Credit Unions (OCCU) is to ensure the safety and soundness of the corporate credit union system by:

1. Providing timely and effective advice to the National Credit Union Administration (NCUA) Board on legislative, regulatory, and operational issues concerning corporate credit unions.

2. Developing, implementing, and maintaining examination and supervisory policies and procedures that address in a timely manner corporate credit union issues in an evolving financial market.

3. Effectively managing OCCU's resources, the applicable risk to the National Credit Union Share Insurance Fund (NCUSIF) and the systemic risk to the credit union system.

TABLE OF CONTENTS

OTHER EXAMINATION AREAS 300

ASSESSMENT OF CORPORATE CREDIT UNIONS 400

WORKPAPERS

Chapter: 101

ADMINISTRATION

Introduction

The Corporate Examiner's Guide (Guide) is for use during the examination and supervision of Corporate Credit Unions (corporates) which are subject to regulation by the National Credit Union Administration (NCUA). It provides Office of Corporate Credit Union (OCCU) personnel with uniform standards for planning and conducting examinations and should be used as a reference tool, training aid, and a guide to NCUA policies and procedures.

Through the regulatory process, OCCU personnel assess the safety and soundness of each corporate. This process includes an:

1. Objective evaluation of a corporate's operational and financial soundness and its compliance with applicable laws and regulations;
2. Assessment of the quality of management and directors; and
3. Identification of areas where corrective action is required to strengthen operations, or improve the quality of performance, or enable compliance with applicable laws and regulations.

This Guide sets forth the framework for this process and is designed to encourage independent reasoning, objectivity, efficiency, and professionalism in the examination process. To promote consistent application among OCCU examination teams, the Guide sets forth minimum standards for examination objectives and procedures. While it promotes standardization of the examination process, field staff is encouraged to modify Guide programs to fit specific institution needs.

Examiners should supplement the Guide and its associated programs with education, experience, and sound judgment. Supplemental pages, updates, and revisions will periodically be published and distributed.

References within the text to specific regulations refer to regulations promulgated by NCUA, unless otherwise designated.

Guide Organization: Chapters

The Guide is divided into five major areas, with each area divided into chapters. Each area and chapter is designated by a divider tab.

400 Assessment of Corporate Credit Unions

500 Statutes and Regulations (To be developed)

Work papers

Index

Each chapter is divided into the following Sections and into further subsections, as applicable.

1. Introduction (Overview)
2. Examination Objectives
3. Examination Procedures
4. Examination Questionnaires
5. References
6. Appendices

Not every Chapter will include each Section.

Introduction

The Introduction describes the subject and explains the activity or operation. Introductions serve as an overview of the respective topics and reinforce knowledge the examiner has gained through NCUA's education programs and experience on the job. Introductions are designed to provide comprehensive information and guidance to examiners. They provide the reader with basic information such as NCUA policies and pertinent accounting issues. Introductions also focus on risks, rewards, and controls.

Examination Objectives

Examination objectives describe the goals that should be of primary interest to the examiner. Listed objectives are general and designed to help examiners tailor the examination to the specific corporate. Some examination objectives, such as evaluation of the corporate's system of internal controls, policies, practices, procedures, and the scope and adequacy of the audit function, help examiners determine the examination scope. Other objectives, such as assessing the corporate's compliance with laws and regulations and evaluating the need for corrective action, provide a framework to help examiners identify areas of risk and develop and implement a strategy for supervising the corporate.

Certain objectives are germane to the overall examination process and to virtually every examination section. These common objectives are presented below. Staff may wish to review this list during the course of an examination, as these objectives might not be specifically included in other Guide Sections.

<u>Common Objectives</u>

1. Document the effectiveness of the corporate's operations;
2. Determine compliance with laws and regulations;
3. Determine the adequacy of and adherence to corporate policies and procedures;
4. Assess management's expertise and ability to manage the corporate's affairs;
5. Assess the board of director's oversight and ensure that management and the board are receiving complete and accurate reports;
6. Verify that an acceptable system of records and internal controls is in place;
7. Verify management has assessed the effect of anticipated internal and external changes on the corporate;
8. Assess the corporate's ability to meet its future needs (e.g., fund growth, provide capital, absorb losses);
9. Identify any actual or potential undue risk to the corporate, the corporate system, or the National Credit Union Share Insurance Fund (NCUSIF); and

10. Report examination findings:
    a) Present analysis and conclusions regarding the corporate's overall condition, trends, and prospects for future viability; and
    b) Identify material concerns (i.e., through development of DORs, etc.) and seek management's agreement for timely resolution of such concerns.

Corporate Examination Procedures

Corporate examination procedures are steps an examiner may follow to accomplish objectives for an area. Examination procedures are a comprehensive collection of approaches from which the examiner-in-charge (EIC) selects only those necessary to adequately assess the area in the corporate under examination.

The materiality and significance of a given area of corporate operations are the EIC's primary considerations in deciding the scope of the examination and the procedures to be performed. Examiner flexibility results in examinations tailored to fit the operations of the corporate.

Examination procedures are divided into three groups: base, standard, and expanded. All examinations will be conducted under standard examination procedures (standard), unless otherwise justified by the examiner and approved by the EIC. However, even if the examiner chooses to divert from the standard procedures, at a minimum, base procedures will be performed for all examinations.

Base procedures are the minimum examination steps conducted when various factors do not warrant standard or expanded examination procedures. This determination may be made when developing a multi-year examination scope or as a result of events during an examination. For instance, the EIC and the Corporate Field Supervisor (CFS) may determine that the standard Automated Clearing House procedures should be conducted every other year to provide additional time to review the investment area. Likewise, the EIC may determine, after an examination has started, that a problem has arisen in an area that needs more attention, which requires less time in the Funds Transfer area. In each of these cases the standard procedures may be reduced, but never below base examination procedures.

Standard procedures are employed by examiners under normal circumstances. Normally, examinations are staffed for standard procedures; however, OCCU management expects EICs to use their discretion in adjusting the review level to either base or expanded, as individual circumstances warrant. Standard procedures may be reduced to base or increased to expanded procedures. The EIC must explain the decision to alter standard procedures in the Confidential Section work paper.

Expanded procedures are more discretionary. Examiners should follow these procedures only when they identify significant problems and it is necessary and expeditious to perform audit-like verification procedures. Ideally, these procedures can be performed by the corporate's staff, directors, and internal and/or external auditors. If the corporate's internal controls or external audit program are not adequate, the examiner should:

1. Require the corporate to immediately address the areas of concern; or
2. Broaden the examination scope to include expanded procedures.

Although examination subject areas differ greatly, certain procedures are applicable to any phase of an examination. A list of procedures that are common to the overall examination process and to virtually every examination section follows. The examiner may wish to review this list when completing an area of review, as the procedures might not be specifically incorporated in other Guide Sections.

<u>General Procedures</u>

Gather Data

1. Review previous Examination Report DORs and OEFs and work papers;
2. Review the current year's scope, supervisory correspondence, and interagency data;

3. Consider the regulatory policy associated with the areas of review; and
4. Obtain the corporate's risk management reports and written policies and procedures.

Set Scope

1. Establish a clear understanding of examination objectives;
2. Perform analytical review of financial data;
3. Identify new or unusual transactions requiring modified examination procedures;
4. Indicate areas of greatest concern;
5. Tailor the examination scope to meet the corporate's risk profile;
6. Consult with other examiners and take the nature of their initial findings into account in determining the examination scope and level of review;
7. Determine if expanded procedures are necessary;
8. Develop additional procedures not covered in the Guide, if necessary; and
9. Perform only those procedures necessary to achieve program objectives.

Evaluate Process

1. Interview corporate personnel;
2. Evaluate policies and procedures;
3. Spot check the reliability and accuracy of reports;
4. Test the corporate's procedures;
5. Identify material changes in operation or policy since the previous examination;
6. Evaluate trends;
7. Research significant variations from last year's examination to determine if there is cause for concern; and
8. Obtain explanations for any significant issues.

Assess Management

1. Review the adequacy of the risk management reports prepared for the board, ALCO, and operating management;
2. Determine the extent to which the directors are involved in monitoring performance and initiating corrective action;

3. Review the adequacy of management's strategic plans;
4. Interview management and staff to ascertain if personnel have adequate knowledge of policies and procedures;
5. Determine the sufficiency of the training and expertise of staff versus the scope and level or risk activities; and
6. Determine if policies and procedures are being communicated and regularly updated.

Formulate Conclusions

1. Keep the EIC informed of progress;
2. Discuss concerns with other examiners, if appropriate;
3. Identify, and determine significance of, regulatory violations and deficiencies;
4. Discuss findings with management;
5. Determine the adequacy of management's response to problem issues; and
6. Consider possible strategies for corrective action and develop a recommended course of action.

Conduct Post Review Activities

1. Review work to ensure objectives have been satisfied;
2. Summarize results and conclusions;
3. Draft comments, including scope, findings, and recommendations;
4. Assign ratings if applicable;
5. Ensure that there are properly cross-referenced work papers to document and support substantive findings and conclusions; and
6. Update the Field File.

Corporate Examination Questionnaires

Corporate Examination Questionnaires (Questionnaires) are checklists an examiner may utilize to gather and summarize information relative to an area. Questionnaires for each area of review are provided on a chapter-by-chapter basis under the guide tab entitled Work papers.

Questionnaires help to assess a corporate's control systems and improve the examiner's understanding of the corporate's internal controls, policies, practices, and procedures. Questionnaires ask about controls that ideally are in effect to provide the corporate with proper day-to-day protection. The examiner is primarily interested in controls that relate to compliance with managerial policies and procedures. The EIC decides when to complete or update the questionnaires related to a particular area of review as part of an examination. IT IS NOT NECESSARY TO COMPLETE ALL QUESTIONNAIRES DURING EACH EXAMINATION. The examiner should include only those questionnaires pertinent to the examination scope and objectives. In the event that the EIC determines completion of a questionnaire is unnecessary, the rationale for this decision should be supported and documented in the Confidential Section of the work papers.

Questionnaires reflect standards for safe and sound operating procedures and may be useful for evaluating a corporate's operations. They also assist in organization, act as memory joggers, and facilitate the review process.

References

Pertinent citations of law and regulation appear in the reference section. References to other relevant NCUA publications are identified where appropriate, including: various bulletins, agency instructions, industry sources, and accounting pronouncements.

An attempt has been made to ensure that the reference list is comprehensive, providing resources beyond those needed on a day-to-day basis. Therefore, the examiner should not be concerned if access to these references is not routinely available. If the corporate under examination is state chartered, the examiner should also refer to state regulations in accordance with OCCU policy.

Appendices

Following the main sections are appendices that might include various forms, checklists, statements, and guidelines. These provide the examiner with additional information regarding certain topics.

Corporate Examiner Conduct

Office of Corporate Credit Union Culture

OCCU has recruited and trained the highest caliber staff from within and outside NCUA. As such the expectations for performance and conduct are exceptionally high. OCCU staff are expected to be hard working, dedicated, efficient, effective, honest, independent, and professional.

OCCU staff expect to be treated in a professional and respectful manner by corporate officials, management, and employees. Likewise, those in the corporate expect the same treatment from OCCU staff. Discourteous treatment is not anticipated, nor will it be accepted, from either OCCU or corporate staffs.

Corporates are engaged in a dynamic industry where change is the "norm rather than the exception." Examiners must expect that corporate staff will go through the same learning curve which they have. Just as examiners learn through their experiences with other examiners and corporate staff, examiners should accept that corporate staff may look to them for their experience. Willingly sharing experiences builds mutual respect and understanding.

Examiners are expected to maintain open lines of communications with corporate staff. Those communication lines should enable corporate staff to discuss openly and frankly pertinent issues involving the corporate. Corporate staff should be encouraged to look to the district examiner (in most cases the EIC) to discuss examination and supervision related issues. Likewise, examiners should discuss issues first with appropriate corporate staff or the chief executive officers (CEO). If discussions are not fruitful, EICs are free to move up the chain of command in addressing those issues.

Corporate examiners should understand that while open communications with corporate officials are encouraged, they must maintain clear independence from the corporate and its staff. Thus, examiners are encouraged not to socialize with corporate employees. Any interaction which would give the perception to the reasonable person that the examiner may lose this independence is not appropriate.

Examples of questionable activities include, but are not limited to: corporates paying for meals, other than working meals, attending or participating in sporting events or other forms of entertainment, and other personal interactions.

Ethical Conduct

All OCCU employees are subject to the Principles of Ethical Conduct for Government Officers and Employees set forth in Executive Order 12674 of April 12, 1989, as modified by Executive Order 12731. All OCCU employees should have available to them a manual containing the Standards of Ethical Conduct for Employees of the Executive Branch issued by the United States Office of Government Ethics (OGE). The manual contains the principles and the regulations, 5 CFR Part 2635, issued by OGE. The Standards are available on OGE's website – usoge.gov/ in either TXT or PDF format.

OCCU employees should be familiar with the information contained in the manual since they are expected to comply with its requirements. NCUA's Ethics Officer offers some simple advice: "abide by the spirit as well as the letter of the standards." Should examiners have an ethical question which causes concern, they should contact the agency's Ethics Officer.

Administrative Issues in Corporate Credit Unions

The following policies governing professional conduct do not constitute an exhaustive or all-inclusive list; rather they are general guidelines addressing important issues that corporate examiners face in their day-to-day work environment.

<u>Duration of On-site Examinations and Supervision Contacts</u>

The scope of each examination and supervisory contact is determined by the EIC and the CFS, targeting problems and high-risk areas. These contacts should be conducted in the most efficient and least disruptive manner possible. Factors to consider in making these decisions are the number and availability of staff, travel costs, effect on the routine operations of the corporate, and the condition of the corporate. Appendix 102F, Reduced On-Site Examination procedures provide further details in this regard.

Working Hours

Examiners should manage their time in a responsible and professional manner. Due to the substantial travel involved with a national examination program, OCCU staff strives to be productive when traveling on airplanes, etc. OCCU staff work eight hour workdays, with travel authorized on Mondays and Fridays. On occasion in order to complete an examination in an effective manner, the EIC may request Sunday travel. Additionally, the distance and time to travel home on weekends may dictate that an over the weekend stay is necessary. Refer to the NCUA Personnel and Travel Manuals for more specific guidance on work hours and travel policy requirements.

EICs will provide each examiner with a work schedule. Examiners should obtain prior approval from the EIC for any deviation from the pre-determined work schedule. The EIC will ensure communication with the appropriate CFS regarding any deviations from the standard work day. Plans for each examination should be provided to the corporate being examined. As a courtesy, EICs should also inform corporate management of any material variances from the schedule if such situations arise.

Working Space

Normally corporates provide adequate working space for examiners. If space is inadequate, additional space may be requested, as long as it does not unnecessarily disrupt the corporate's operations.

Smoking

If a corporate has rules regarding smoking, they should be followed. Agency personnel who smoke should always be courteous and considerate of others. If a corporate allows smoking throughout the facility and it is perceived that it endangers the health of the examination participants, the EIC should work with the corporate to obtain smoke free space. If that is impossible, the EIC should work with the CFS on any other reasonable solution.

Access to Information

Examiners should carefully protect all information entrusted to them by the institution, securing it from unauthorized access. Confidential documents should not be left unattended.

Examiners should never divulge confidential information in any form to unauthorized persons. On the other hand, if the corporate refuses to provide information needed to complete the examination, the EIC should notify the CFS. If the CFS is not successful in obtaining the release of the information, the Director of OCCU should be notified to determine if appropriate administrative or other legal action is necessary.

Dress Code

Prior to conducting examinations and other contacts at corporates, the EIC is to determine the dress code that is acceptable at the corporate and inform all participants. In general, if less than business attire is acceptable in the corporate, business casual is acceptable for OCCU staff, even during staff and exit briefing meetings with officials. Traditional Business attire still is required for all joint conferences.

Examiners should use common sense in determining what business casual is. If, when corporate examiners look into the mirror, they have any questions as to the appropriateness of their dress, they should change into something they know is acceptable. Regardless of what examiners wear, it should be in good shape, fit properly, be clean, and appropriately pressed or ironed.

Acceptable business casual clothing includes: dress slacks, dress docker type pants, button down shirts, polo type shirts (such as high quality cotton shirts), loafer type leather shoes, dress shoes, socks, skirts (with hose), blouses, heeled shoes, and sweaters (with collared shirt).

Unacceptable casual dress includes: jeans or denim pants, sports type Khakis, un-collared shirts (men's), shirts with team or country club logos and characters (except agency issued shirts), deck shoes, tennis shoes, no socks, shorts or skorts, sleeveless shirts, open toed shoes including sandals, flannel shirts, and ski sweaters.

References

1. Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR Part 2635.

Chapter 102

CORPORATE CREDIT UNION SUPERVISION AND EXAMINATION PROCESS

Introduction

The Office of Corporate Credit Unions (OCCU) fulfills its mission by promoting and ensuring the safety and soundness of the Corporate Credit Union System (System) principally through a program of continual supervision. Supervision includes, but is not limited to, the on-site examination of corporate credit unions (corporates) resulting in an examination report. Supervision entails vigilance encompassing all regulatory efforts to formulate, implement, and maintain an ongoing process to ensure that:

1. Corporates report their condition in a timely and comprehensive manner;
2. OCCU evaluates and reports the condition of corporates;
3. Corporates correct deficiencies in a timely manner; and
4. The System remains safe and sound.

OCCU's Supervision Goal

OCCU's overall supervision goal is to ensure the safety and soundness of the System by (1) continuously evaluating and supervising the financial condition and performance of individual corporates and their service organizations, and (2) reporting those conditions to the NCUA Board in a timely manner. OCCU provides high-quality "targeted" supervision. The key element in accomplishing OCCU's goal is the timely identification and resolution of any problem or condition that may have a material impact on a corporate, the System, or the National Credit Union Share Insurance Fund (NCUSIF).

OCCU's efforts are focused on (1) identifying existing and/or emerging material problems in individual corporates and/or the System, and (2) ensuring such problems are corrected in a timely and appropriate manner. Since accepting risk is inherent to the business of the System, OCCU's philosophy is centered on evaluating risk.

OCCU applies this philosophy in all its supervisory activities. OCCU combines the structure of consistent supervision with reasoned flexibility to ensure its procedures are appropriate for both the corporate and the dynamic, evolving marketplace in which it operates. Flexibility allows examiners to adjust the supervisory effort to meet the risks posed by a particular corporate while ensuring risks are addressed throughout the System.

Elements of the Supervision Process

Regardless of the approach taken, effective supervision includes, at a minimum, the following elements:

1. Performing high quality annual examinations of all corporates that accept deposits from any federally insured credit union, whether federal or state chartered;
2. Conducting periodic or continuous on-site reviews of corporate activities based on the degree of existing or perceived risk they undertake;
3. Conducting monthly off-site reviews of corporate activities through review of financial and management reports including operating budgets and strategic plans; and
4. Conducting monthly reviews of corporate financial data (NCUA 5310 reports) to determine trends in individual corporates and the System.

In conjunction with its efforts to implement these four elements, OCCU communicates with State Supervisory Authorities (SSA) to coordinate an overall supervision plan. Agreements with SSAs are contained in Chapter 104 and may be supplemented by special agreements with individual SSAs. Examiners should familiarize themselves with any agreements prior to initiating a contact with the SSA to discuss supervision and examinations plans.

Targeted Risk Approach

OCCU employs targeted risk procedures to ensure the examination scope appropriately focuses resources toward areas of material risk. While all areas of risk are addressed, an appropriate examination plan may utilize one or more of the following techniques:

1. Allocate examination hours based on perceived risk the examination areas pose and the extent and results of prior years' review of the area;
2. Prioritize areas for a comprehensive review once every two or three years (depending on risk) unless there is a demonstrable need for more frequent or thorough review; and
3. Use examination procedures that test the quality of managerial supervision of the area, reliability of the area's internal controls, and the quality of oversight provided by the board of directors and its auditors.

Targeting risk requires examiners to determine how existing or emerging situations confronting a corporate, or the credit union industry, affect the nature and extent of risks in that institution. The examiner then structures supervisory plans and actions based on the corporate's risk profile. The Targeted Risk approach provides flexibility for the examiner to prioritize the use of resources toward the areas of greatest risk. It officially sanctions the ability and elevates the responsibility of the examiner-in-charge (EIC) to prioritize procedures for resource maximization.

OCCU recognizes corporates must take risks to earn a return. Risk levels, however, must be appropriately identified, measured, monitored, reported, and controlled. The significance of risks must be continually evaluated.

Corporate management is responsible for controlling risk. OCCU assesses how well a corporate manages risk over time, rather than at a single point in time. Targeted risk procedures focus on the oversight rather than an audit role. Targeted risk allows OCCU to concentrate on systemic risks and institutions that pose the greatest risk to the System and the NCUSIF.

OCCU's targeted risk approach identifies areas that, in the aggregate, pose the potential for presenting an unacceptable level of risk to the System and the NCUSIF. To address high-risk activities that can be influenced by market conditions, OCCU's goal is to communicate with, and influence, the System through direct supervision, policy, and NCUA regulation. In situations where corporates are not properly managing risks, OCCU uses appropriate means to influence management to adjust its practices to conform with sound business practices.

Inherent Risks

Some risks are inherent to the System. A wide body of knowledge exists within the System on how to identify, measure, monitor, report, and control these inherent risks. Targeted risk acknowledges these inherent risks and evaluates whether they are properly managed. Other risks in the System are more diverse and complex. These more sophisticated risks require enhanced controls and monitoring by both the corporate and OCCU. OCCU is committed to focusing its resources on these complex and evolving risks, especially when they present material actual or potential risks to the System.

Supervisory Response to Degree of Risk Exposure

Risks that large corporates assume are generally diverse and complex and warrant a targeted risk approach. Under this approach, examiners do not attempt to eliminate appropriate risk-taking, but rather ensure corporates understand and control the levels and types of risk they assume. In situations where risk is not properly managed, OCCU will direct management to take corrective action so the corporate is managed in a safe and sound manner. In all cases, OCCU's supervisory focus is to determine that management identifies, measures, monitors, reports, and controls risks to ensure sufficient capital is present in relation to the corporate's risk activities.

"Pass-through" corporates (those which primarily rely on another corporate for investment placement and product offerings) are generally less diverse and complex than those which deal directly in the financial marketplace. Regardless of each corporate's complexity, the targeted risk approach still emphasizes that all risks be adequately managed.

Targeted Risk Approach

The Corporate Examiner's Guide stratifies targeted risk within base, standard, and expanded examination procedures as discussed in Chapter 101.

A crucial element of the targeted risk approach is the EIC's pre-examination risk assessment of the corporate. (The framework for this process is described in Appendix 102A entitled "Application of the Targeted Risk Approach in the Identification, Measurement, and Assessment of Risk.") During this assessment, the EIC determines and documents the level of supervisory concern for each risk category. Having prioritized the corporate's risk exposure, the EIC selects and documents a detailed examination scope. A determination not to use the standard examination scope will be documented. Advance Corporate Field Supervisor (CFS) approval is required for using anything other than the standard examination scope. While implementing the examination scope as part of the on-site field work, the EIC may determine expanded or base review procedures are more appropriate. These situations should be discussed with the CFS before the examination scope is adjusted.

Targeted Risk Summary

The Targeted Risk approach allocates greater resources to those areas with higher risks. OCCU accomplishes this by:

1. Identifying risks using common definitions. This set of risks forms the basis for supervisory assessments and actions;
2. Measuring risk based on common evaluation factors. Risk measurement is not always quantified in dollar terms; it is sometimes a relative assessment of exposure. For example, numerous internal control deficiencies may indicate a corporate has an excessive amount of transaction risk;

3. Evaluating risk management to determine if the corporate's systems adequately manage and control risk levels. System sophistication will vary based on the level of risk present and the size and/or complexity of the institution;
4. Assigning greater resources to areas of higher or increasing risk, both within an individual institution and among corporates in general; and
5. Performing examinations based on risks, reaching conclusions on risk profile and condition, and following up on areas of concern.

To accomplish these tasks, examiners will discuss preliminary conclusions with corporate management and adjust conclusions and strategies based on these discussions, as appropriate. OCCU can then target supervisory efforts on significant risks.

The targeted risk approach provides OCCU and the System with:

1. A high level of consistency in supervision by using minimum core procedures;
2. An allocation of resources based on risk;
3. Sufficient flexibility to allow examiners to tailor the supervisory effort to the risks present;
4. Less supervisory review of low risk areas; and
5. Help in determining the sufficiency of each corporate's capital level and risk management system.

Planning

Examination/supervision planning is the process of identifying and establishing supervisory goals and objectives for incorporation into OCCU's supervisory strategy for each corporate. On-site examinations, supplemented by on- and off-site supervision activities, are the means by which OCCU's supervisory strategies are implemented and its supervisory goals and objectives are achieved.

The targeted risk approach ensures that OCCU's resources are efficiently used by establishing appropriate examination procedures, and developing appropriate guidelines for OCCU personnel to follow when completing assignments.

Examination/Supervision Planning

OCCU's supervision policies require a specific supervisory strategy for each corporate. The strategy includes detailed, planned supervisory activities. Planning normally begins at the conclusion of a full-scope, on-site examination with the completion of the three-year plan (TYP). Reference should be made to Appendix 102C for OCCU's format and content requirements for TYPs and additional discussion in the section below (Developing and Examination/Supervision Plan).

On-going Modification of Examination/Supervision Plans

Examiners perform ongoing supervision and periodic follow-up activities throughout a supervision cycle to identify and assess risks and changing conditions. As supervisory strategy is dynamic, EICs and CFSs should review examination/supervision strategies and revise or update them to reflect the corporate's changing risk profiles, developments in the System, and regulatory changes. Examiners should discuss any approved changes to examination/supervision plans with corporate management.

Developing an Examination/Supervision Plan

Examination/supervision of individual corporates is tailored to conditions and needs according to OCCU policy. This approach balances consistency with flexibility. Annual examination/supervision plans for each corporate are developed as follows:

1. Budget - In conjunction with preparing OCCU's budget, each CFS will recommend to the OCCU Director (Director), the category Type of supervision (discussed below) planned for each corporate during the next examination cycle. The CFS consults with examiner staff before making a recommendation. The Director approves the type of supervision recommended (i.e., assuming agreement with the recommendation), subject to NCUA Board budget approval;
2. TYP - After each annual examination, the CFS and the EIC will develop the corporate's supervision and examination scope for the forthcoming year, and contingent plans for the subsequent two years (three years total). The TYP addresses what needs to be

accomplished and outlines the most efficient and effective method for achieving the goals established in the TYP. This includes use of base, standard, and expanded examination procedures (Chapter 101). The plan should also include any on-site visits to monitor operational changes (e.g., software, key staff, and conversions.) The TYP will be submitted to the Director for approval; and

3. The CFS and the EIC will monitor implementation of the plan on an ongoing basis, notifying the Director of any needed changes/revisions.

Supervision Types

Based on the criteria listed below, each corporate is assigned a supervision type category. The supervision type of each corporate is a key component of the target risk supervision approach and provides standard on- and off-site supervision strategies, based on each corporate's established supervision type. OCCU staff may vary the from the supervision strategies for each type if approved by their CFS and the Director.

A corporate's assigned supervision type is not a rigid function of asset size, expanded authority level, or Corporate Risk Information System (CRIS) rating. Rather, it represents a combination of factors that may include these elements in addition to perceived risk levels, quality of or changes in management, financial condition, trends, etc.

Type I

Type I corporates do not have expanded authorities above the Base Plus level.

Supervision of Type I corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 report data and trends, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision:

    a. Risk Management and Financial Risk rated either 1 or 2:

1) Annual Examination

b. Risk Management and/or Financial Risk rated no worse than a 3:

1) Annual Examination
2) Semiannual on-site follow-up contact

c. Risk Management or Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Quarterly on-site follow-up contact

d. Risk Management and Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Monthly on-site follow-up contact

Type II

To qualify for Type II supervision, corporates must generally exceed $1 billion in assets, and/or have expanded authorities above the Base Plus level and exercise its approved powers in a significant and assertive manner. Additionally, Type II corporate have complex and innovative operations, and/or have significant impact in the marketplace, and/or present unusual or unique examination and supervision problems that cannot be adequately addressed by Type I supervision.

Supervision of Type II corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 reports, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision:

a. Risk Management and Financial Risk rated either 1 or 2:

1) Annual Examination
2) Monthly one or two week on-site contact by EIC

b. Risk Management and/or Financial Condition rated no worse than 3:

1) Annual Examination
2) Semiannual follow-up Examination
3) Monthly one or two week on-site contact by EIC

c. Risk Management rated 4 and Financial Risk rated 3:

1) Annual Examination
2) Semiannual Examination
3) Monthly two week on-site contact by EIC

d. Risk Management rated 3 and Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Monthly two week on-site contact by EIC
4) Weekly review of financial deficiencies

e. Management and Financial Condition rated 4:

1) Annual Examination
2) Semiannual Examination
3) Full time, on-site presence

Type III

Corporates which qualify for Type III supervision, generally, have billions of dollars in assets, and/or have expanded powers in excess of Part I and exercise their approved powers in a significant and assertive manner. Additionally, Type III corporates have complex and innovative operations, and/or have a significant impact in the marketplace and on the corporate and/or credit union system, and/or present unusual or unique examination and supervision problems, which cannot be adequately addressed by Type I or Type II supervision.

Supervision of Type III corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 report data and trends, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision - regardless of Risk Management and Financial Risk ratings:

    a. Incremental annual examination, scoped with two separate contacts (i.e., typically investment and ALM phase and an operational risk phase)
    b. Full time presence by on-site examiner, not necessarily the EIC
    c. Monthly on-site EIC contact

For incremental examinations, the CRIS ratings are normally assigned after the operational examination phase. However, OCCU staff has the flexibility to adjust CRIS ratings after any examination phase. These situations should be discussed with the CFS, and if appropriate, the OCCU Director.

Examinations

Scheduling Examinations

Annual examinations are required and performed for all corporates. On-site follow-up examinations and supervisory contacts are performed consistent with the corporate's supervision category. Appendix 102B provides a timeline for completion of examination related activities.

Examination Teams

Examinations are performed by examination teams, composed of an EIC and one or more team members. The EIC and team members are assigned by the CFS based on a variety of factors such as corporate complexity, examiner experience, examiner proximity to the corporate, and scheduling considerations. Appendix 102F, Reduced On-Site Examinations (ROSE) also impacts examination team planning.

Examination Steps

An examination entails a number of steps in planning and execution. These steps generally include:

1. Off-site pre-examination planning;
2. On-site pre-examination preparation;
3. Examination field work;
4. Exit briefing;
5. Report writing;
6. Joint conference; and
7. Wrap-up.

Pre-Examination Planning

Prior to each examination, the EIC has responsibility to plan the on-site (field) examination work. This planning effort is accomplished during a period referred to as pre-examination. The pre-examination effort may be accomplished both on- and off-site, by the EIC.

By necessity, pre-examination planning is conducted approximately 45 - 60 days in advance of the examination, and generally requires from three days to one week to complete. Pre-examination planning is an opportunity for the EIC to:

1. Make team participant lodging arrangements;
2. Arrange for corporate management to complete and return to the EIC, the Pre-Examination Questionnaire (OCCU 102Q);
3. Develop the preliminary examination scope and time budget;
4. Prepare a memorandum to team participants regarding their participation on the examination; and
5. Prepare a letter to the corporate being examined to communicate the dates of the on-site examination, the exit and joint conference dates and times, to provide them with the information request list, and to request arrangement for review of the annual audit work papers.

Factors to consider in the pre-examination planning process:

1. Attain goals and objectives - The examination effort should be directed toward attaining the supervisory goals and objectives that were previously identified and established during the examination/supervision planning process. (e.g., TYP, pre-examination questionnaire, monthly management reports.)
2. Develop scope - Examination procedures contained in the individual programs are designed to be comprehensive and target risk areas. Therefore, it is important appropriate procedures are selected within each program.
3. Plan for optimum productivity - The EIC should plan opportunities for meetings with examination staff and corporate personnel, arrange adequate workspace for the examination team, and prioritize and schedule workflow.
4. Make assignments and monitor job - The EIC must determine the expertise necessary to perform certain aspects of the examination and make assignments accordingly. When assigning more than one individual to an area, it is recommended that a team leader be assigned who will be responsible for its completion. Training and development needs should also be considered when making examination assignments.
5. Budget and monitor overall time - The EIC must consider the time budget when assigning tasks. A useful tool for improved personnel planning is a time and planning summary organized according to sections of the examination. Such a summary specifies areas for which procedures are planned and provides a comparison of actual and budgeted hours. As the examination progresses, the time budget should be modified as deemed appropriate.
6. Assign priorities - The EIC assigns priorities to each area. Ordinarily this can be accomplished by assigning related areas to one team leader who subsequently coordinates the work of others.
7. Schedule examination - To minimize costs and disruption to the corporate, it is important that the examination be conducted as quickly as practical. It is the responsibility of the EIC to discuss any planning problems with the CFS. If corporate management is concerned about scheduling, this matter should also be discussed.

<u>Pre-Examination Questionnaire (OCCU 102Q)</u>

This questionnaire contains questions detailing the nature and complexity of the corporate's operations and internal controls. It is designed to assist the EIC in planning examination procedures and resources. It should be completed as one of the first steps of the Pre-Examination planning effort. Ideally, it should be prepared by corporate management or by the EIC during an interview with corporate management.

On-Site Pre-Examination Preparation

Examiners utilize on-site examination preparation time to accomplish several purposes:

1. Review the Pre-Examination Questionnaire which management has completed at the EIC's request and make any necessary changes in the preliminary scope;
2. Ensure management fills the items listed in the information request list so they will be available when the examination team arrives;
3. Ensure adequate work space is available for the team; and
4. Review the work papers supporting the annual audit.

On-site examination preparation efforts are generally performed during the first few days of the week preceding the on-site arrival of the examination team (first day of examination field work). This timing allows the EIC to review information provided by management pursuant to the pre-examination request, make any necessary changes in the preliminary scope, and follow-up on any requested information management has yet to make available.

Examination Field Work

Depending on the size and complexity of the corporate, an examination usually entails two to three weeks of on-site field work. The duration of a Type III incremental examination may vary.

During this period, the examination team gathers information and performs procedures as outlined in the examination scope.

<u>Managing An Examination</u>

Managing an examination is as important as planning it. The level and sophistication of management methods and procedures varies depending on the activities to be performed and the size and nature of the corporate. The EIC carries the responsibility for managing the examination.

Inherent in the EIC's responsibilities is ensuring supervisory objectives are met and activities are completed timely. To accomplish these goals, the EIC must continually monitor the progress of the examination and supervise, coordinate, and evaluate the work flow.

Key elements the EIC should consider during the course of the examination are:

1. Communicate examination objectives – The EIC must ensure that examiners understand the objectives of the examination and their assigned programs. Examiners should notify the EIC as questions occur regarding scope or depth of review. Examiners should not vary from standard examination procedures unless the EIC determines that such procedures are necessary to address potential risks. Ongoing communication between the EIC and team participants is critical to effective examination management;
2. Monitor staff performance - Examiners' performance must be monitored throughout the examination to ensure objectives are being met according to schedule and to prevent problems from developing. It is also important to avoid material deviations from the examination scope into unplanned activities. Early identification of work-related problems also allows examiners the opportunity to correct mistakes and to immediately improve skills;
3. Monitor the examination - Monitoring the examination's progress allows early adjustments to the scope, staffing, and completion date, as necessary. The EIC must notify the CFS if examination scope adjustments are necessary;
4. Training and evaluating examiners - Examiners may frequently need guidance, depending on their experience and ability. Questions should be encouraged and the EIC is responsible to ensure someone is available to provide guidance;
5. Communicate effectively - The EIC must maintain effective communications with the CFS, corporate management, the SSA, and examiners regarding the examination's progress;

6. Complete work papers - Prepare, file, index, and review work papers to facilitate efficient preparation of the examination report; and
7. Out-brief examiners - The out-briefing process is critical to the conclusion of the on-site examination effort. As the field work draws to a close, the EIC must have a complete understanding of the work performed and issues identified by each team member. Ideally, the EIC will monitor all team members' activities during the examination so the out-briefing is minimal. The out-briefing should provide an orderly transfer of examination materials, such as work papers, reference material, time sheets, etc., from the participant to the EIC or the EIC's designee. The EIC should also be informed of any additional items requested during the examination that should be added to the request list for the next examination.

Work Paper Documentation

Integral to the targeted risk approach is its system of work papers designed to assist the EIC in examination planning, coordinating, observing, understanding, critiquing, reporting, and follow-up. Overall, examination work papers provide efficient vehicles for the examiner to report both the understanding obtained and concerns identified.

Required work papers for each examination include:

1. A Corp110 form identifying the ratios, CRIS ratings, time spent, and problem areas;
2. National Credit Union Administration Examination Report, OCCU 102B and OCCU 102C - These forms are the standard report letter page for the distribution of an examination report. OCCU 102B is utilized for a report to a federally chartered corporate credit union and OCCU 102C is used for a state chartered corporate credit union. These forms list the procedures used during and objectives of the examination, cite the responsibility of the board of directors and management, and provide instructions on how to address the report's findings;
3. Executive Summary, OCCU 102D - The Executive Summary summarizes the examiner's review, analysis, and findings in major

areas of the corporate's operation, financial condition, management, and CRIS ratings;

4. Supplementary Facts, OCCU 102E - The Supplementary Facts is used to discuss material facts or situations not contained in other narrative sections of the examination report or to expand on Executive Summary discussions. This form is optional;
5. Document of Resolution (DOR), OCCU 102F - This form is designed to record and report the findings, issues, and actions needed to correct findings for issues of <u>major</u> importance. Matters presented on this form must represent violations of law, regulation, policy, and/or must constitute a material safety and soundness issue. As OCCU 102F issues are identified, examiners should:

   a) Confirm their understanding of the facts and circumstances surrounding the issue and the corresponding basis for the exception;
   b) Prepare the OCCU 102F; and
   c) Report the finding and provide a copy of the OCCU 102F to the team leader (if any) and the EIC.

   The EIC should seek management's agreement for action plans, responsible parties, and the time frame for resolving DOR issues. However, sometimes management's time frame may be inadequate to bring out regulatory compliance or adequate management of risks. Nevertheless, due dates should be reasonable and attainable and due dates not met will require additional correspondence between the OCCU/SSA and the corporate. OCCU/SSA must officially approve all due date changes after the final report is presented;
6. Other Examiner's Findings (OEF), OCCU 102G - The examiner has broad latitude regarding the documentation of issues, which do not merit inclusion on the OCCU 102F. The OCCU 102G has been devised to serve as a vehicle to report issues about which the examiner has a concern, but which are not material and are not appropriate for inclusion on the OCCU 102F.

   OCCU 102G issues should be discussed with departmental management as they are identified during the examination. This form will be provided to the corporate's directors no later than the conclusion of the joint conference. Normally, it will not be included in the official examination report. However, with the concurrence of the CFS, the examiner may include the form with the report if the number of non-material items, when considered as a whole, will have a material impact on the overall evaluation of any component of either the financial risk or risk management rating. When it is included as a part of the report, the examiner will explain the reasons to the corporate's board. The Executive Summary will detail to the officials whether this form is included in the examination report or handed out separately;

7. Trends on the Consolidated Balance Sheet Report (CBS, a product of the 5310 System) – The CBS is generated and analyzed during each examination and it, or a similar financial trend work paper is included in the examination report. The CBS provides monthly balance sheet, income, and ratio trends;
8. Procedures and Questionnaires - These forms are developed as part of the examiner's review responsibilities. The examiner should ensure that adequate comments are made as appropriate. The comment should be descriptive enough for a reviewer to draw a conclusion. Repetitive comments in the examination procedures, questionnaires, or Corporate Examiner Memorandums (CEM) should be avoided or at least minimized;
9. CEM, OCCU 102H - This form is developed as part of the examiner's Observation/Reviewing responsibilities. The examiner develops a thorough understanding of assigned processes as they are uniquely implemented in the corporate being examined.

   OCCU 102H should be a professionally written document that outlines the review area. The document should not contain non-verified information or hearsay. The document is presented to the corporate for accuracy and verification of the examiner's understanding of the policies, procedures, and practices. OCCU 102H is designed to be carried forward from year to year and updated/revised only as necessary to reflect any changes to the operation that have been made since the prior examination. Concluding each OCCU 102H is a brief narrative overview summarizing the examiner's conclusions regarding the operational status of the area reviewed. This should be a conclusions reached memorandum - not a listing of the review steps the examiner accomplished;

10. CRIS, OCCU 102I - This form is used to support the CRIS ratings (See Chapter 401) assigned by examiners during the examination. From this form, the EIC will derive the composite and component CRIS ratings which will be included in the Executive Summary, OCCU 102D. The SSA may have a separate rating or may use the CAMEL rating system for state chartered corporates;
11. Confidential Section, OCCU 102J - The Confidential Section is for NCUA's internal use only. However, situations exist when all or part of a report's Confidential Section may be released by court order or in compliance with a Freedom of Information Act request. The possibility of release should not dissuade examiners from presenting necessary information; however, examiners should maintain their professionalism and objectivity when writing the Confidential Section.

    Examiners are to report corrective and constructive work accomplished during the examination in the Confidential Section if not included in the open sections of the report. Examiners should comment briefly but completely enough to clearly reflect actions taken. Of particular importance is an explanation of what the examiner accomplished during discussions with officials and management. If not discussed elsewhere in the report, the Confidential Section should state what formal actions the board took and how the officials will handle major problems. At a minimum, this form should report:

    a. Advanced meetings with management;
    b. Joint conference;
    c. Deviations from scope and budget;
    d. Date of problem code assignment and elimination;
    e. Report distribution;
    f. Transmittal letter dissemination; and
    g. Recommended follow up.

    Examiners should include in the Confidential Section pertinent matters of a private or restricted nature, including professional opinions based on the examiner's observations. However, the examiner should not make statements based on gossip or hearsay;
12. Other examiner-designed work papers - Examiners are authorized and encouraged to use their professional judgment in devising

unique work papers to supplement core work papers for the assigned area of review. However, excessive documentation should be avoided and such work papers should only include information that is relevant and/or may require follow-up. Time spent recording extraneous information is better spent examining high-risk areas; and

13. Electronic database storage – The final examination report, CEMs, procedures, questionnaires, and custom work papers will be submitted to OCCU mail for electronic filing. All OCCU staff will ensure they abide by all policies and guidelines in maintaining and transmitting sensitive examination information (i.e., use NCUA computers, the VPN, etc.).

Exit Briefing

The exit briefing with corporate officials and management will be held at the conclusion of the examination fieldwork. The EIC must verify that all officials have been invited to attend the exit briefing. It is up to the board members (not operating management) to decide which officials will be in attendance. It is up to the discretion of the EIC what will be discussed during the exit briefing (e.g., DORs, OEFs). The EIC must have sufficient understanding of the issues to proficiently discuss them during the exit briefing.

Report Writing

Depending on the size and complexity of the corporate and/or deficiencies noted during the examination, the EIC is afforded one week to consolidate, review, and analyze the team's work papers and prepare and submit a draft report for supervisory review. It is expected that the draft report will be a professional product, void of grammatical, punctuation, and spelling errors. The draft report will be sent to the CFS and SSA (if applicable) for review and finalization.

While writing styles will vary, the EIC should ensure the examination report discusses facts, expresses OCCU's assessment of the various risks or issues, and provides closure for the issue at hand.

Joint Conference

The joint conference is usually scheduled as part of the pre-examination planning process. The joint conference should be set to accommodate the corporate, OCCU, and the SSA. Regularly scheduled board meetings usually work; however, special meetings may need to be called. A visual aide must be used for each joint conference. This could include power point, flip charts, handouts, etc. The joint conference must be a professional meeting held to summarize the financial condition of the corporate and examination findings. The ratings of the corporate will not be disclosed until the end of the joint conference.

OCCU attendees at the joint conferences are normally provided advance notification via an information memorandum developed by the EIC. A sample of this memorandum is shown in Appendix 102D.

Wrap-Up

After the joint conference the EIC will finalize the examination work papers and necessary forms. This includes:

1. Finalizing the confidential section;
2. Finalizing the transmittal letter to the corporate, region memorandum (see Appendix 102E), and SSA memorandum;
3. Preparing a TYP per this chapter, including establishing the scope for the next 12 months supervision;
4. Sending a zip copy of the database to OCCU;
5. Uploading the Corp110;
6. Sending work papers to OCCU, CFS, and SSA (if requested); and
7. Updating all other forms/logs required by OCCU (e.g., CUSO Logs, Privacy Checklist), if applicable.

Supervision

On-Site and Off-Site Supervision Process

Corporates are an integral part of the System and the credit union industry. Additionally, they have the ability to take risks in the management of their assets as they provide services to their members. Due to the complexity and inherent importance of corporates, on-going supervision is needed to ensure the safety and soundness of individual corporates and the System. Effective and continuous review of a corporate's operations is an essential part of the supervision process.

Files

EICs maintain field files for each corporate in their district. These files should include not only documents, analysis, and reports related to previous examinations and supervision contacts, but also current policies and procedures for all critical areas of operation. The files should be well organized to ensure their efficient use and, when necessary, their orderly transfer to other OCCU staff. It is imperative that hard and electronic examination information be formally and safely maintained and transferred. The following minimum information should be maintained:

1. Permanent file (containing a history of examination reports, regulatory information, critical correspondence, etc.);
2. The last one or two complete examination work papers;
3. Supervision contacts during the examination period;
4. Board and ALCO packages for the examination period;
5. Current budget and strategic plan;
6. Examination period correspondence; and
7. Monthly management reports, 5310s, and Corp110s.

Information Received

To supplement the files maintained, each EIC will receive monthly board and ALCO packages from corporates in their district. The packages, at a minimum, should include the following:

1. Monthly board and committee minutes with supplemental attachments (e.g., proposed policies, individual new product business plans, status of DOR and OEFs);
2. ALM reports (e.g., NEV, spread analyses, and book of business);
3. Financial statements, including a delinquent loan report;
4. Audit and internal control reviews completed;
5. Budget comparisons; and
6. Current lists of investments and new investments purchased during the month.

The examiner must verify DORs are completed within the agreed upon due dates. The examiner will initiate necessary correspondence, which includes correspondence from the Director and SSA (if state chartered), if due dates will not or have not been met.

Analyses Performed

While conducting on-site and off-site supervision contacts, the EIC will perform, at a minimum, specific supervision functions. The following supervision tasks are key to determining whether an immediate on-site contact is required, the current on-site contact is expanded, and the scope of the next examination or supervision contact.

1. Analyze financial trends;
2. Ensure timely compliance with the previous examination report's DOR and OEF;
3. Assess management changes (e.g., board of directors, senior management, and other key employees);
4. Assess changes to MIS systems or major related systems (e.g., item processing);
5. Monitor and analyze changes in the investment portfolio and ALM strategies;
6. Review and verify for accuracy financial information submitted monthly by corporates, via the 5310 system; and
7. Review all material changes in policies, procedures, practices, and operations.

Other On-site Supervision Contacts

Other situations could warrant an on-site contact. This could be completed by the district examiner or with a team of examiners. The following situations could warrant an on-site contact:

1. CRIS rating - to follow-up on the status of completing DORs and correcting OEFs;
2. Expanded Authority Request (EAR) - to evaluate the EAR and prepare for the OCCU Director and/or NCUA board action and SSA concurrence, if required;

3. Request for NCUA board action - to evaluate the corporate's request and prepare for the board action;
4. Senior management change - a change in senior management could warrant a contact to verify accuracy of reports and overall condition of the corporate; and
5. Addition or deletion of a service - a purchase or sale of a service or a fixed asset that could have a material impact on the membership.

In all situations the examiner should prepare appropriate documents supporting the contact. This could include a contact memorandum documenting work performed, status reports for DORs and OEFs, and appropriate documents for requested actions.

If appropriate, CRIS ratings can be reevaluated during a supervision contact. Ratings will be changed, as deemed appropriate, based on favorable/deteriorating financial, managerial, and/or operational factors. OCCU reserves the right to change CRIS ratings, as warranted, with the concurrence of the OCCU Director.

Examination Objectives

Examination Planning and Control Objectives

1. Prepare for supervisory activities, including the on-site examination, in an efficient manner;
2. Select and structure examination programs that target the goals and objectives of the supervisory strategy;
3. Ensure the examination is conducted in a professional manner;
4. Establish controls and record keeping systems to communicate examination findings effectively; and
5. Maintain review processes to ensure prescribed work is completed and workpapers support conclusions.

Supervision Contact Objectives

Objectives of both on- and off-site supervision contacts

1. Obtain reasonable assurances each corporate will continue to be financially sound;
2. Determine NCUSIF risk;
3. Determine compliance with applicable laws and regulations; and
4. Determine that the corporate's activities and financial condition does not adversely affect the System.

Examination Procedures

See Corporate Examination Procedures - Examination Administration (OCCU 102P).

Examination Questionnaire

See Pre-Examination Questionnaire (OCCU 102Q).

Appendices

102A – Application of the Targeted Risk Approach in the Identification, Measurement and Assessment of Risk

102B - Examiner's Guideline for Completing an Examination

102C - Template for the Three-Year Supervision Plan

102D – Template of Joint Conference Information Memorandum

102E – Sample Transmittal Memo to the Region

102F – Reduced On-Site Examinations

Appendix 102A

COMPTROLLER'S - APPLICATION OF THE TARGETED RISK APPROACH IN THE IDENTIFICATION, MEASUREMENT, AND ASSESSMENT OF RISK

Supervision by Risk

Supervision by risk requires examiners to determine how certain existing or emerging issues facing a bank or the banking industry affect the nature and extent of risk in that institution. Based on that risk evaluation, examiners then structure regulatory supervisory plans and actions. Supervision by risk builds upon the risk-based supervisory philosophy historically used by the OCC. This enhancement provides consistent definitions of risk, a structure for assessing these risks, and a more integrated use of risk assessment in the supervisory process.

The OCC recognizes that banking is a business of taking risk in order to earn profits. Risk levels, however, must be appropriately managed and controlled. Banking risks also must be evaluated in terms of their significance. These assessments should be ongoing.

Supervision by risk leaves the responsibility for controlling risks with bank management. The OCC assesses how well a bank manages this risk over time, rather than only assessing the condition at a single point in time. With supervision by risk, the OCC functions in more of an oversight than an audit role. Supervision by risk allows the OCC to supervise by concentrating systemic risk and institutions or areas that pose the greatest risk to the system.

For the entire industry, the OCC's supervision by risk identifies areas that, in aggregate, pose the potential for presenting an unacceptable level of risk to the banking system and the federal deposit insurance fund. For those high-risk activities and/or activities that have become particularly risky because of market conditions, the OCC's goal is to communicate with, and influence, the industry through direct supervision, policy, and regulation. In situations where an individual bank is not properly managing its risks, the OCC's goal is to use appropriate means to influence bank management to adjust its practices to conform with sound fundamental banking principles.

Some risk are inherent to banking. A wide body of knowledge exists within the industry on how to identify, measure, control, and monitor these inherent risks. Supervision by risk acknowledges those inherent risks and performs limited testing in examinations directed at confirming whether adequate controls are in place. Other risks in the industry are more diverse and complex. These more sophisticated risks require enhanced controls and monitoring by both the bank and the OCC. The OCC is committed to directing its most significant resources to these complex and evolving risks, especially where they present material, actual, or potential risks to the banking system.

Risks that large banks assume are generally diverse and complex and warrant a risk-oriented supervisory approach. Under this approach, examiners do not attempt to prohibit appropriate risk-taking, but rather ensure that banks understand and control the levels and types of risk they assume. In situations where risk is not properly managed, the OCC tries to direct bank management to take corrective action so that the bank is managed in a safe and sound manner. In all cases, the OCC's supervisory focus is to ensure that bank management identifies, measures, controls, and monitors risks to ensure sufficient capital is present in light of the risks.

Risks that community banks assume are generally less diverse and complex than those of larger banks. Under this approach, examiners verify the existence of adequate controls and risk management systems by testing transactions. Examiners will focus attention on the risk management systems and the methods management uses to identify, measure, control, and monitor risk in those community banks or in areas that are more diverse and complex.

Supervision by risk allocates greater resources to those areas with higher risks. The OCC accomplishes this by:

- Identifying risks using common definitions. This set of risks forms the basics for supervisory assessments and actions.

- Measuring risk based on common evaluation factors. Risk measurement is not always quantified in dollar terms; it is sometimes a relative assessment of exposure. For example, numerous internal control deficiencies may indicate a bank has an excessive amount of transaction risk.

- Evaluating risk management to determine if bank systems adequately manage and control the identified risk levels. The sophistication of the systems will vary based on the level of risk present and the size and/or complexity of the institution.

- Assigning greater resources to areas of higher or increasing risk, both within an individual institution and among banks in general. This is done through the supervisory strategy.

- Performing examinations based on the risks, reaching conclusions on risk profile and condition, and following up on areas of concern.

To accomplish these tasks, examiners should discuss preliminary conclusions of this risk-based supervisory strategy with bank management and adjust conclusions and strategies based on these discussions, if appropriate. The OCC can then focus supervisory efforts on significant risks, i.e., the areas of highest risk within a bank and within the banking system.

Examiners must focus on the consolidated company risk profile to fully implement supervision by risk. This consolidated approach recognizes that risks at individual institutions may be mitigated or increased on a company-wide basis. Individual bank risk profiles, however, must be determined for the lead bank and significant national bank affiliates for the examiner to fully evaluate the consolidated risk profile.

In summary, the supervision by risk approach provides the OCC and the banking industry with:

- A high level of consistency in supervision because it sets and uses minimum core procedures.
- An allocation of resources based on risk.
- Sufficient flexibility to allow examiners to tailor the supervisory effort to the risk present.
- Less supervisory intervention in areas of low risk.
- Help in determining the sufficiency of each bank's capital and risk management systems.

Definition of Risk

For purpose of the OCC's discussion of risk, the OCC assesses banking risk by its impact to capital and earnings. From a supervisory perspective, risk is the potential that events, expected or unanticipated, may have an adverse impact on the bank's capital or earnings.

The simple existence of risk is not necessarily reason for concern. To put risks in perspective, examiners should decide if the risks a bank is undertaking are warranted. Generally, risks are warranted when they are understandable, measurable, controllable, and within the bank's capacity to readily withstand adverse performance. If examiners determine risks are unwarranted, they must communicate with management and the directorate to mitigate or eliminate the unwarranted risks. Appropriate actions for the bank to take may include reducing exposures, increasing capital, or strengthening risk management processes.

Risk Management

Because market conditions and company structure vary, no single risk management system works for all companies. Each institute should develop its own risk management program tailored to its needs and circumstances. The sophistication of the risk management system will increase with the size, complexity, and geographic diversity of each bank or company. All sound risk management systems, however, have several common fundamentals. For example, bank staff responsible for implementing sound risk management systems perform those duties independent of the bank's risk-taking activities. Regardless of the risk management program's design, each program should include:

- Risk identification. Proper risk identification focus on recognizing and understanding existing risks or risks that may arise from new business initiatives. Risk identification should be a continuous process, and should occur at both the transaction and portfolio level.

- Risk measurement. Accurate and timely measurement of risks is a critical component of effective risk management. A bank that does not have a risk measurement system has limited ability to control or monitor risk levels. Further, the sophistication of the risk measurement tools a bank uses should reflect the complexity and levels of risk it has assumed. The bank should periodically verify the integrity of the measurement tools it uses. Good risk measurement systems assess both individual transactions and portfolios.

- Risk control. The bank should establish and communicate limits through policies, standards, and/or procedures that define responsibility and authority. These control limits should be meaningful management tools that can be adjusted if conditions or risk tolerance change. The bank should have a process to authorize exceptions or changes to risk limits when they are warranted.

- Risk monitoring. Banks should monitor risk levels to ensure timely review of risk positions and exceptions. Monitoring reports should be frequent, timely, accurate, and informative; and should be distributed to appropriate individuals to ensure action when needed.

Effective risk management requires an informed board of directors. The board must guide the company's strategic direction. A key component of strategic direction is endorsing the organization's risk tolerance by approving policies that set standards, either orally or in writing. Well-designed monitoring systems allow the board to hold management accountable for operating within established tolerance levels.

Capable management and appropriate staffing also are critical to effective risk management. Bank management is responsible for the implementation, integrity, and maintenance of risk management systems. Management also must keep the directors adequately informed. Management must:

- Implement the company's strategic direction.
- Develop policies, formal or informal, that define the institution's risk tolerance that are compatible with the bank's strategic goals.
- Oversee the development and maintenance of management information systems to ensure they are timely, accurate, and informative.
- Ensure that strategic direction and risk tolerance are effectively communicated and adhered to throughout the organization.

When examiners assess risk management systems, they consider policies, processes, personnel, and control systems. A significant deficiency in one or more of these components constitutes a deficiency in risk management. All of those systems are important, but the sophistication of each will vary depending upon the complexity of the bank. Noncomplex community banks normally have less formalized policies, processes, and control systems in place than do large banks.

- **Policies** reflect the bank's intent and commitment to pursuing desired results. They set standards and courses of action to pursue, implement, or enforce specific objectives. Good policies link with, and reflect, a bank's underlying mission, values, and principles. They also clarify the bank's tolerance for risk. Mechanisms should be in place to trigger a review of policies in the event that activities or tolerances change. Policies may be written or unwritten depending upon the effectiveness of management and complexity of the area or bank. In any event, standards should be articulated and adhered to in practice.
- **Processes** are the procedures, programs, and practices that govern how a bank will pursue its objectives. Processes define how daily activities are carried out. Good processes are consistent with the underlying policies, are efficient, and include checks and balances.
- **Personnel** are the staff and managers that execute or oversee performance of the processes. Good staff and managers are qualified; competent, and perform as expected. They understand the bank's mission, values, policies, and processes. Compensation programs should be designed to attract, develop, and retain qualified personnel.

- **Control Systems** are tools and information systems that bank managers use to measure performance, make decisions, and assess effectiveness of existing processes. These feedback devices must be timely, accurate, and informative. They measure performance and assist in decision-making.

Categories of Risk

The OCC has defined nine categories of risk for bank supervision purposes. These risk are: **Credit, Interest Rate, Liquidity, Price, Foreign Exchange, Transaction, Compliance, Strategic, and Reputation**. These categories are not mutually exclusive, any product or service may expose the bank to multiple risks. For analysis and discussion purposes, however, the OCC identifies and assesses the risks separately.

Credit Risk

Credit Risk is the risk to earning or capital arising from an obligor's failure to meet the terms of any contract with the bank or otherwise fail to perform as agreed. Credit risk is found in all activities where success depends on counter-party, issuer, or borrowed performance. It arises any time bank funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether reflected on or off the balance sheet.

Credit risk is the most recognizable risk associated with banking. This definition, however, encompasses more than the traditional definition associated with lending activities. Credit risk also arises in conjunction with a broad range of bank activities, including selecting investment portfolio products, derivatives trading partners, or foreign exchange counter-parties. Credit risk also arises due to country or sovereign exposure, as well as indirectly through guarantor performance.

Interest Rate Risk

Interest rate risk is the risk to earning or capital arising from movements in interest rates. The economic perspective focuses on the value of the bank in today's interest rate environment and sensitivity of that value to changes in interest rates. Interest rate risk arise from difference between the timing of rate changes and the timing of cash flows (re-pricing risk); from changing rate relationships among different yield curves affecting bank activities (basis risk); from changing rate relationship across the spectrum of maturities (yield curve risk); and from interest-related options embedded in bank products (options risk). The evaluation of interest rate risk must consider the impact of complex, illiquid hedging strategies or products, and also the potential impact on fee income which is sensitive to changes in interest rates. In those situations where trading is separately managed this refers to structural positions and not trading portfolios.

The assessment of interest rate risk should consider risk from both an accounting perspective (i.e., the effect on the bank's accrual earnings) and the economic perspective (i.e., the effect on the market value of the bank's portfolio equity). In some banks, interest rate risk is captured under a broader category of market risk. In contrast to price risk, which focuses on the market-to-market portfolios (e.g., trading accounts), interest rate risk focuses on the value implications for accrual portfolios (e.g., held-to-maturity and available-for-sale accounts).

Liquidity Risk

Liquidity risk is the risk to earnings or capital arising from a bank's inability to meet its obligations when they come due, without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned decreases or changes in funding sources. Liquidity risk also arises from the bank's failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value.

As with interest rate risk, many banks capture liquidity risk under a broader category-market risk. Liquidity risk, like credit risk, is a recognizable risk associated with banking. The nature of liquidity risk, however, has changed in recent years. Increased investment alternative for retail depositors, sophisticated off-balance sheet products with complicated cash-flow implications, and a general increase in the credit sensitivity of banking customers are all examples of factors that complicate liquidity risk.

Price Risk

Price risk is the risk to earnings or capital arising from changes in the value of portfolios of financial instruments. This risk arises from market-making, dealing and position-taking activities in interest rate, foreign exchange, equity, and commodities markets.

Many banks use the term price risk interchangeably with market risk. This is because price risk focuses on the changes in market factors (e.g., interest rates, markets liquidity, and volatilities) that affect the value of traded instruments. The primary accounts affect the value of traded instruments. The primary accounts affected by price risk are those which are re-valued for financial presentation (e.g., trading accounts for securities, derivatives, and foreign exchange products).

Foreign Exchange Risk

Foreign exchange risk is the risk to earning or capital arising from movement of foreign exchange rates. This risk is found in cross-border investing and operating activities. Market-making and position-taking in foreign currencies is price risk.

Foreign exchange risk is also known as translation risk and is sometimes captured as a component of market risk. Foreign exchange risk arises from accrual accounts denominated in foreign currency, including loans, deposits, and equity investments (i.e., cross-border investing). Accounting conventions require quarterly revaluation of these accounts at current rates. This revaluation translates the foreign denominated accounts into U.S. dollar terms.

Transaction Risk

Transaction risk is the risk to earnings or capital arising from problems with service or product delivery. This risk is a function of internal controls, information systems, employee integrity, and operating processes. Transaction risk exists in all products and services.

Transaction risk is also referred to as operating or operational risk. This risk arises on a daily basis in all banks as transactions are processed. It is a risk that transcends all divisions and products in a bank.

Compliance Risk

Compliance risk is the risk to earnings or capital arising from violations of, or nonconformance with laws, rules, regulations, prescribed practices, or ethical standards. Compliance risk also arises in situations where the laws or rules governing certain bank products or activities of the bank's clients may be ambiguous or untested. Compliance risk exposes the institution to fines, civil money penalties, payment of damages, and the voiding of contracts. Compliance risk can lead to a diminished reputation, reduced franchise value, limited business opportunities, lessened expansion potential, and lack of contract enforceability.

Compliance risk is often overlooked as it blends into operational risk and transaction processing. A portion of this risk is sometimes referred to as legal risk. This is not limited solely to risk from failure to comply with consumer protection laws; it encompasses all laws as well as prudent ethical standards and contractual obligations. It also includes the exposure to litigation from all aspects of banking, traditional and nontraditional.

Strategic Risk

Strategic risk is the risk to earning or capital arising from adverse business decisions or improper implementation of those decisions. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities.

Strategic risk focuses on more than an analysis of the written strategic plan. It focuses on how plans, systems, and implementation affect the bank's franchise value. It also incorporates how management analyzes external factors that impact the strategic direction of the company.

Reputation Risk

Reputation risk is the risk to earnings or capital arising from negative public opinion. This affects the institution's ability to establish new relationships or services, or to continue servicing existing relationships. This risk can expose the institution to litigation, financial loss, or damage to its reputation. Reputation risk exposure is present throughout the organization and is why banks have the responsibility to exercise an abundance of caution in dealing with its customers and community. This risk is present in activities such as asset management and agency transactions.

The assessment of reputation risk recognizes the potential impact of the public's opinion on a bank's franchise value. This risk is inherent in all bank activities. Banks which actively associate their name with products and services, such as with fiduciary services, are more likely to have higher reputation risk exposure. As the bank's vulnerability to public reaction increases, its ability to offer competitive products and services may be affected.

Measuring and Assessing risk

To ensure effective supervision by risk, the OCC requires a common framework to document decisions about risk. The risk assessment system (RAS) provides a concise method of communicating and documenting judgments regarding the quantity of risk, the quality of risk management, the level of supervisory concern (measured as aggregate or composite risk), and the direction of risk. The common definitions explained above are critical to identifying risk consistently. A list of evaluation factors that examiners should consider in making the assessments is also provided. These evaluation factors are not mandatory checklists, but rather provide an overview of issues that can assist the examiner in making decisions within the RAS.

Assessments of risk in the RAS must reflect both current and prospective view of the company's or bank's risk profile. This assessment drives supervisory strategies and activities. It also facilitates discussions with bank management and directors and helps to ensure more efficient examinations.

The RAS is used for all banks. The OCC has, however, developed two versions of the RAS, one for community banks and one for large banks. This allows for a common supervisory philosophy while recognizing the differing levels and complexities of risk present in each bank.

Examiners should discuss conclusions from the RAS with appropriate bank management and the board. Bank management's input may help clarify or modify the examiner's RAS conclusions. While the OCC does not require bankers to adopt a similar process, examiners must effectively communicate the rationale for their decisions in evaluating risk to ensure effective supervision. These discussions will help the OCC and bank management reach a common understanding of the risks, focus on the strengths and weaknesses of risk management, and ensure that future supervisory plans are achieved.

The Risk Assessment System for Large Banks

Once the risks in a company are identified using the common definitions explained above, examiners use the common framework provided by the RAS to assess the risk exposure for the nine types of risk. For seven of the risks (Credit, Interest Rate, Liquidity, Price, Foreign Exchange, Transaction and Compliance), the supervisory process includes an assessment of the:

- **Quantity of risk**, which is the level or volume of risk that exists and is assessed as high, moderate, or low.

- **Quality of risk management**, which includes how well risk are identified, measured, controlled, and monitored and is assessed as weak, acceptable, or strong.

- **Aggregate risk**, which is a summary judgment that reflects the level of supervisory concern considering both the quantity of risk and the quality of risk management, weighing the relative importance of each. The examiner's assessment of aggregate risk may be impacted by mitigating factors, not necessarily considered in the quantity of risk and quality of risk management decisions. An example of a mitigating factor is insurance. Aggregate risk is assessed as high, moderate, or low. Aggregate risk assessments direct the specific activities and resources outlined in supervisory strategies.

- **Direction of risk,** which indicates the likely changes to the risk profile over the next 12 months and is assessed as decreasing, stable, or increasing. Decreasing direction indicates the examiner anticipates that aggregate risk will decline over the next 12 months. Stable direction indicates the examiner anticipates that the aggregate will remain unchanged. Increasing direction indicates the examiner anticipates the aggregate risk will be higher 12 months in the future. When aggregate credit risk is moderate and direction is decreasing, the examiner can anticipate that aggregate credit risk will be low or lower in 12 months. The direction of risk often influences the supervisory strategy.

For the other two categories of risk, strategic risk and reputation risk, examiners' judgment of risk is less quantifiable. These risks affect the bank's franchise value but are not direct risks that examiners can precisely measure in an examination. These risks require examiners to consult with supervisory offices to ensure all elements are considered. Given the less explicit nature of these risks, the OCC's risk assessment and measuring process is modified. For strategic risk and reputation risk, the supervisory process includes an assessment of the:

- **Composite risk,** which is a summary judgment that reflects the level of risk of supervisory concern incorporating all elements that affect strategic risk and reputation risk. It is assessed as high, moderate or low. Composite risk assessments direct the specific activities and resources outlined in supervisory strategies.

- **Direction of risk**, which is the examiners' view of likely changes to the risk profile over the next 12 months, as explained above. It is assessed as decreasing, stable, or increasing.

The combined assessments of each significant national bank allow the examiner to assess the consolidated risk profile of the holding company. The relative importance of each risk, both for the individual bank and for the holding company, should influence the development of the strategy and the assignment of resources.

Examiners should complete a **consolidated** RAS quarterly. Examiners must also complete the RAS for each significant national bank affiliate every 12 months. The bank RAS should be updated more frequently if deemed appropriate based on the consolidated risk profile. The consolidated and individual bank RAS conclusions are recorded in SMS.

SUGGESTED TIME FRAMES FOR COMPLETING AN EXAMINATION

Action Needed	Discussion	Optimal Due Date	Actual Date Completed
Pre-planning on-site/off-site	Review previous examination report, correspondence, develop preliminary scope and budget, complete 102Q, and discuss scope with the CFS.	90 - 120 days prior to commencement of examination.	
Hotel arrangements	Make hotel arrangements for the examination team. Take into consideration the city and season when making advance reservations. In addition, make hotel arrangements for the joint conference (JC) when the date is known. (Hotel arrangements are made for NCUA participants only.)	As soon as the schedule is set.	
Communication with the SSA (if state chartered)	Work with the SSA throughout the entire examination process. Discuss the examination scope, exit briefing date, joint conference date, examiner responsibilities, etc.	Throughout the examination process.	
Pre-exam letter to the CFS	E-Mail the pre-exam letter to the CFS. The CFS will put it on letterhead and FedEx back. Be sure the exit and JC dates have been discussed with the CFS, corporate, and SSA (if applicable). (On occasion this is issued by the SSA.)	60 days prior to being on-site for pre-exam.	
Notify Region	E-Mail the ARD-P of the appropriate region inviting a regional representative once the JC date is finalized.	As soon as the J.C. date is set.	
Pre-exam letter to the corporate	Send pre-exam letter, labeled file folders, and questionnaires to the corporate. Be sure to send copies to cc's on letter (SSA (if applicable) and OCCU).	30 days prior to being on-site for the pre-exam.	
CFS approval of the budget	E-Mail the final time budget to the CFS and ask for approval or comments prior to sending it to the team participants.	Prior to sending out the team memo.	
Team memo and information to exam participants	Send the team memo and time budget to the examination participants. Rental car assignments can be made if flight schedules are known, otherwise notify separately when travel plans are communicated. Send out previous CEMs either in the database or separately, prior examination report, and status of DORs and OEFs.	2 - 4 weeks prior to being on-site.	
Examination files and supplies sent to the corporate	Send prior examination work papers and other pertinent information to the corporate. This includes all correspondence since the prior examination (board packages, 5310's, etc.) Also send supplies, such as paper, hole punch, Acco fasteners, etc.)	The week prior to the pre-exam week.	
Pre-exam week required work	1. Check files to verify that all requested items are available.	Pre-exam week	
	2. Verify space availability and/or assign rooms.		
	3. Review CPA work papers at their office.		
	4. Review Board and ALCO minutes since previous examination.		
	5. Make copies of time study, organization chart, financial statements, etc., for the team participants.		
	6. Call board and supervisory committee members as a courtesy letting them know you are on-site and invite questions and discussion.		
	7. Determine if the corporate has a power point projector. If not, send the CFS a message requesting OCCU's be sent to the JC location.		
Examination	Work with each examiner daily. As the EIC you will be answering questions, attending meetings, and reading examination related material on a flow basis. Establish good communications with participants to keep abreast of current findings, problems, and progress. Maintain ongoing communication with the SSA, EIC, and SSA participants (if applicable).	On-site examination	

Action Needed	Discussion	Optimal Due Date	Actual Date Completed
Exit briefing	Hold the exit briefing with corporate officials and management at the conclusion of the examination fieldwork. It is up to the discretion of the EIC what will be discussed during the exit meeting (e.g., DORs, OEFs). The EIC must verify that all officials have been invited to attend the exit briefing.	At the conclusion of the examination field work. Additional briefings may be necessary if staffing is staggered.	
Final day of examination	Make sure all necessary information from the participants (e.g., database, DORs, OEFs, time sheet) is received prior to staff release. Obtain a listing of any additional reports that should be requested at the next examination.	Last day of on-site examination work.	
Report writing	Write the Executive Summary, merge the DORs, and OEFs, finalize CRIS ratings, and write the Supplementary Facts. Work with the SSA examiner, if applicable, on the report preparation.	Wrap up week	
Draft report to CFS	Send draft report to CFS.	Friday of wrap up week	
Begin Power point, Confidential Section, and One-Year Plan	Begin working on Confidential Section, Power Point Presentation, and One-Year Plan.	Wrap up week.	
CFS will return report and set up briefing with OCCU Director, if necessary	CFS will make comments/corrections on the report and send back for updating. CFS will set up teleconference with Director and direct you to E-Mail the report to OCCU Mail and Director.	Week after wrap up week.	
Briefing	Brief the Director and finalize the report with the SSA, if applicable.	Minimum of 7 days prior to the JC.	
Report to the corporate	Send the final report (less CRIS rating) by E-mail or fax to the corporate requesting dissemination to the officials.	7 days prior to the JC.	
Report printing	Print and bind the final report. Bound copies should be kept to a minimum. The EIC must use discretion and each corporate may be different. The number of copies should be for: all corporate officials, Supervisory Committee members, official copy for the corporate, SSA (if applicable), OCCU, CFS, and Region. Be sure to sign, both OCCU and SSA, copies distributed to corporate officials. Copies for board members, committee members, and NCUA offices need not include color copies.	Prior to JC after OCCU briefing	
JC information memo	Send information memo to Director (through CFS) if they are attending the JC.	Prior to JC	
Joint Conference	Hold the joint conference beyond 21 days of the wrap up week unless approved by the CFS.	As previously determined.	
Transmittal letter, Region memo, SSA letter, One-Year Plan	Send via E-Mail to the CFS for processing the following: 1) Transmittal letter to the corporate; 2) Region Memo; 3) SSA Memo; and 4) One-Year Plan.	1 - 3 days after JC (30 days for the One-Year Plan)	
Corp110	Complete and upload Corp 110.	1 - 3 days after JC	
Final report	Send final report and workpapers (2 copies - OCCU and CFS). All core workpapers, any self-designed workpapers, examiner observations, etc. Include 2 bound reports to OCCU for processing with the SSA letter and Region Memo.	1 - 3 days after JC	
Electronic report	E-Mail zipped copy of the examination data base to _OCCU Mail.	1 - 3 business days after JC.	
Logs/forms	Update all other logs/forms required by OCCU (e.g., CUSO Logs, Privacy Checklist), if applicable.	1 - 3 business days after JC.	

APPENDIX 102C
Template for the One-Year Supervision Plan
NATIONAL CREDIT UNION ADMINISTRATION
Office of Corporate Credit Unions

OCCU/
CU #

TO: Director
Office of Corporate Credit Unions

FROM: Corporate Examiner
Corporate Field Supervisor

SUBJ: One-Year Supervision Plan (OYSP): Corporate Name, Charter/Insurance Number

DATE:

BACKGROUND
Discuss examination, financial information, areas of concern, etc.

CRIS RATINGS

Financial Risk	**Rating**	**Trend***	**Risk Management**	**Rating**	**Trend***
Empirical Capital			Capital Accumulation Planning		
Earnings			Profit Planning & Control		
Interest Rate Risk			Interest Rate Risk Management		
Liquidity Risk			Liquidity Risk Management		
Credit Risk			Credit Risk Management		
			Operations Risk		
			Board Oversight, Audit and Compliance		
Financial Risk Composite			**Risk Management Composite**		

***Use + for positive trend, – for negative trend, and = for stable.**

CHANGES IN OPERATIONS
Discuss any planned changes in management, systems, operations, etc. which affect future supervision plans and/or the focus of the next annual examination.

APPENDIX 102C
Template for the One-Year Supervision Plan

Discuss the factors affecting financial risk, the quality of risk management, the aggregate risk, and risk direction. Any material negative change in risk direction must be discussed.

SUPERVISION TYPE
Discuss supervision type and parameters as outlined in Chapter 102 of the Examiner's Guide.

SUPERVISION PLANS

Monthly/Ongoing	OnSite
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Discuss any foreseeable changes that could alter the supervision plans. It is not necessary to repeat the discussion of any issues previously covered in the operational changes section on page one.

ANNUAL EXAMINATION
Discuss the next year's annual examination, e.g., staffing, budget hours, additional expertise requested. Please note in the table below whether OCMP, CMS, ISS, or PSS participation is requested. Involvement of specialists must consider the risk profile, and directly relate to the resources necessary to accomplish the supervision and examination objective.

Ensure adequate documentation of any area that did receive a comprehensive review and explain when one is expected. Discuss whether base or expanded procedures were used on any focused area and what is anticipated for the next annual examination. The EIC needs to ensure a comprehensive review (at least standard procedures) of each area is completed every 3 years or more frequently, if necessary.

APPENDIX 102C
Template for the One-Year Supervision Plan

NEXT YEAR'S RESOURCES REQUESTED TABLE

RESOURCES	# HOURS REQUESTED BY EIC
CMS	
PSS	
ISS	
OCMP	
CEs	
Other	
Totals	

SPECIALIST PARTICIPATION

CMS Requested: *Please note specialist comments.*

PSS Requested: *Please note specialist comments.*

ISS Requested: *Please note specialist comments.*

Attached is a spreadsheet which will help the EIC to communicate to the specialist the need for participation. Note: There are three tabs inside the workbook one for each specialized area.

If the specialist is not onsite, the EIC will forward the attached specialist spreadsheet, CEM, questionnaire, and procedures for the respective area within three days after the joint conference. The spreadsheet was designed to assist the EIC with determining the need for specialist participation when the requisite specialist(s) is not on-site during the examination. When completed the spreadsheets must be submitted with the OYSP. If a specialist is onsite at the examination the EIC will discuss the future participation prior to the end of the examination. Specialists will document their recommendations in the conclusion section of their respective CEM(s). Also note: The timeframes listed above may conflict with other OCCU instructions for the submission of CEMs to specialists. These instructions do not supersede other OCCU instructions.

If the EIC is unsure which specialist to submit the information to they will contact the respective CFS for determination based on current work loads. The specialist will respond back to the EIC within 10 days of the joint conference. The EIC will submit the proposed plan to the CFS within 20 days of the joint conference. The final OYSP will be submitted to the Director within 30 days of the joint conference.

D:\My Documents\
amydata\OCCU\Planr

COMMENTS
Discuss competitive pressures, key issues going forward, future earnings, operational weaknesses, etc.

CUSOs
If applicable, address whether you recommend a separate CUSO review and provide support for your recommendation.

CONCURRENCE		**CONCURRENCE**	
☐ Yes		☐ Yes	
☐ No		☐ No	
____________________	____________	____________________	____________
Corporate Field Supervisor	Date	Kent Buckham Director	Date

Corporate Name:	Example	
Charter/Ins #:	12345	
	CMS Questions:	**YES/NO**
1	An OCCU or OCMP Capital Markets Specialist was ***NOT*** onsite for the current examination (or a supervision contact since the last examination.)	
2	There ***HAS*** been a key staffing change in senior management and/or investment, investment credit, or risk management staffing since the last examination.	
3	There ***HAS*** been a significant change in the structure, composition, complexity, and/or risk profile of the investment portfolio.	
4	The corporate ***HAS*** complex investment products.	
5	The corporate ***HAS*** Part I, Part II, Part III, or Part IV Expanded Authority.	
6	There ***ARE*** proposed changes in strategies forecasting future events that may have a material impact on balance sheet structure, composition, and risk profile.	
7	NEV and/or NEV volatility trends are ***NOT*** within regulatory or internal guidelines over the examination period.	
8	NEV and/or NEV volatility trends over the examination period ***ARE*** erratic.	
9	The Asset-Liability Risk Quantification Model is ***NOT*** in "maintenance" mode.	
10	Internal controls to ensure accuracy and reasonableness of risk assessment and quantification are ***NOT*** adequate.	
11	Risk Measurement Systems and Processes were ***NOT*** validated by a qualified third party over the past 3 years.	
12	Third Party risk measurement systems and Processes validation identified ***WEAKNESSES*** which remain ***UNRESOLVED*** .	
13	ALCO's knowledge, experience, oversight and/or reporting is ***NOT*** adequate.	
14	Liquidity controls, stress measurements, and/or external funding sources are ***NOT*** adequate.	
15	Investment Gains and/or Losses ***DO*** represent a material amount of Net Income.	

EIC NOTES:

Corporate Name:	Example	
Charter/Ins #:	12345	
	PSS Questions:	**YES/NO**
1	There ***HAS*** been a change in key management in any payment systems area (funds transfer, ACH, item processing)?	
2	There ***HAS*** been a significant change in operations?	
2a	Have any products, services, or systems been added, replaced, upgraded, or eliminated?	
2b	Has there been a significant expansion or contraction of member users?	
2c	Has there been a significant increase or decrease in processing volume?	
3	There ***HAS*** been an example of unacceptable management performance?	
3a	Are there unresolved internal or external audit findings?	
3b	Are there unresolved examination issues?	
3c	Are there Federal Reserve Bank account overdrafts resulting from cash management and/or procedural deficiencies?	
3d	Are there significant suspense items by aging, dollar amount, or number?	
3e	Have there been any reported regulatory violations?	
4	**DO** funds transfer or ACH activities include use of a proprietary payment system? Examples include PayPLUS, Fundtech Banker, Politzer & Haney, Goldleaf, etc. If you are unsure, consult your PSS.	
5	**DOES** ACH origination activity include non-financial institution members?	
6	There ***ARE*** unresolved business continuity issues?	
7	There **HAVE** been circumstances which prevented a PSS from being onsite during the last two examination cycles?	

EIC NOTES:

PSS COMMENTS:

Corporate Name:	Example	
Charter/Ins #:	12345	
	ISS Questions:	**YES/NO**
1	There ***HAS*** been a change in upper management, CEO or Chief Information Officer equivalent, since the last exam.	
2	Their written information security program, including their enterprise wide written risk assessment process, information protection strategy, and security policy has ***NOT*** been reviewed by an IT examiner.	
3	They ***HAVE*** an in-house core system.	
4	They ***DO*** in-house software development for any of their products.	
5	They ***HAVE*** (host) their own transactional web site.	
6	An IT examiner was ***NOT*** onsite the last examination (or a supervision contact since the last examination.)	
7	There ***HAS*** been a change in the core processing system.	
8	New technology services for members ***HAVE*** been added since the last exam.	

EIC NOTES:

APPENDIX 102D
Template of Joint Conference Memorandum

OCCU:

TO: Director
Office of Corporate Credit Unions

THRU:
Corporate Field Supervisor

FROM: CE

SUBJ: Corporate (Corp) Joint Conference

DATE:

Time , location, and address:

Hotel information, if applicable

( )

Information about the hotel amenities, rates, per-deim rates, etc.

Confirmation numbers.

<u>Directions from Airport to Hotel</u>

<u>Directions from Hotel to Corporate</u>

<u>Background Information</u>
Discuss number of directors, who attended the exit, and activity levels on the committees.

Discuss the characteristics of the board members e.g., name, position held, affiliated organization, assets size, number of years served, known information concerning the individual, any other pertinent information.

APPENDIX 102D
Template of Joint Conference Memorandum

Supervisory Committee
Discuss the characteristics of the committee members e.g., name, position held, affiliated organization, assets size, number of years served, known information concerning the individual, any other pertinent information.

Other
Discuss any other information deemed appropriate for meeting.

APPENDIX 102E
Sample Transmittal Memorandum to the Region

OCCU/

TO: Regional Director

FROM: Director
Office of Corporate Credit Unions

SUBJ: Corporate Credit Union

DATE:

Attached is a copy of the July 31, 2001, examination report for the subject. This confidential report is being provided for your review and information. Please ensure that access to this report is provided on a need-to-know basis.

If you have any questions, please do not hesitate to contact me.

Attachment

cc: CFS
CE

Appendix 102F

REDUCED ON-SITE EXAMINATIONS – ROSE PROCEDURES

Purpose

The purpose of Reduced On-Site Examinations (ROSE) is to provide OCCU staff flexibility to conduct corporate credit union (CCU) examinations in the most efficient and effective manner. OCCU's objective is to optimize resources by allowing its staff to perform greater portions of CCU examinations from staff duty stations without sacrificing the quality of the examination process.

Other benefits derived through ROSE are as follows:

1. Reduced travel expenses;
2. Increased productive time; and
3. Improved quality of life.

ROSE Exams

OCCU management expects corporate examiners to use their professional judgment to determine which examination areas should be performed off-site. When EICs prepare the examination scope and team assignments, they should use professional judgment to determine the best approach to accomplish the examination's objectives. Professional judgment should take into account the financial stability of the corporate, CRIS ratings, operating authority/complexity, OCCU training needs, and other relevant factors.

The EIC (including the SSA EIC, if applicable) finalizes the proposed examination scope, team assignments, and budget; then submits it to their Corporate Field Supervisor (CFS). The CFS will communicate with the EIC if any questions or concerns arise from the review of the proposed examination scope. However, if examination scope changes occur, the EIC must be comfortable that the examination's objectives will be met, regardless of where portions of the examination are performed.

Pre-Examination Planning

It is imperative for the EIC to provide the CCU with a clear and comprehensive examination request list outlining the information needed and its format (i.e., electronic and/or hard copies, etc.). In addition, the examination questionnaires will need to be completed by the CCU well ahead of the anticipated examination commencement date so that this information will be readily available to the examination team. Each EIC must verify that the examination request list only contains information which has not previously been provided to the EIC and/or the District Examiner.

During the pre-exam week the EIC electronically and/or by hard copy, sends examination materials to the examination team. The EIC may consider having a team participant(s) work on-site during the pre-exam week or other examination weeks to facilitate dissemination of the records request information to the examination team. The EIC should ensure all corporate policies and procedures are submitted electronically so they can be transmitted to team members via E-Mail. If a document is only available hard copy, the EIC can have the documents scanned and faxed through Rightfax for further distribution electronically. If the files cannot be distributed electronically the EIC will FedEx the files to each team member during the pre-week so they have the hard copies during the off-site week of the exam. As with any examination process, the EIC and the examination team must utilize a secure process (i.e., encryption, etc.) when transmitting CCU information electronically or in hard copy.

The EIC will also need to have a telephone contact established for each team member so that questions can be answered. In addition, E-Mail will be more critical and the EIC will need to establish a list of E-Mails and chain of command protocol for the corporate and team members. The EIC is responsible for some of the administrative duties (e.g., retrieving data files, making copies for all examination binders, etc.) for off-site exam team members, since performing some of these activities from a remote duty station is not feasible.

Administrative time demands on the EIC are increased under ROSE due to the changes to the data accumulation and distribution process (i.e., examination questionnaires, etc.). Therefore, it is critical the EIC handle the dissemination of examination data in an efficient and effective manner.

The EIC is responsible for ensuring all on- and off-site examination team members receive sufficient information (i.e., electronically, or otherwise) to perform their analysis.

Chapter 103

ON-SITE PRESENCE SUPERVISION

Introduction

Corporates qualifying for Type II supervision will generally be assigned a capital markets specialist (CMS) to perform on-site supervision one to two weeks each month. However, if a Type II corporate is assigned CRIS ratings of 4 in both Financial Risk and Risk Management, the CMS will maintain a full-time on-site presence.

Corporates qualifying for Type III supervision (as defined in Chapter 102) will be assigned a CMS on a full-time basis. Additionally, the assigned examiner-in-charge will generally be on-site monthly.

Objectives of On-site Supervision Presence

The goal of the on-site supervision presence is to develop and maintain a thorough understanding of the operations and risk profiles of large complex corporates. Maintaining an on-site presence promotes interaction with the corporate's staff and allows the CMS to maintain a working knowledge of the corporate's operations, especially in the capital markets areas (investments, asset and liability management, risk monitoring, etc.). The knowledge gained through on-site supervision allows the CMS to more effectively monitor and evaluate financial changes. The EIC's monthly on-site presence promotes a higher level of understanding of operational issues and changes. Early understanding of changes in financial strategies as well as early review of new products, services, and operational changes provides OCCU and the SSA, if state chartered, the opportunity to promptly dialogue with corporate officials and management to address issues and/or concerns.

Operational understanding and changes will be the primary responsibility of the EIC. Operational risk is significant throughout the corporate system. Ongoing supervision of these activities (e.g. item processing, payment systems, network security) is crucial for the continued understanding of the evolving technology utilized in all these areas.

<u>New Investment Strategies</u>
The CMS will monitor the corporate's investment portfolio to identify changes in and/or variances from investment strategies and to assess impact of changing economic conditions. New or changing investment strategies will be analyzed and discussed with the corporate's investment and risk management staff to determine the rationale for the change and the impact on the corporate's risk

position. Economic factors affecting the investment portfolio will also be discussed.

New Member Deposit Products/Services

The CMS will monitor new deposit products and services offered to the corporate's members. New member deposit products will be analyzed in relation to the corporate's strategic business plan and ALM/balance sheet structure strategies. Safety and soundness issues, if any, will be addressed with management.

Organizational/Infrastructure (Key Personnel Changes)

Changes in key staff or reporting structures may affect the corporate's ability to adequately address risks.

The CMS will evaluate individuals filling key risk management positions in relation to the level of the corporate's expanded authorities. The benefit derived from the on-site supervision presence is the timeliness in obtaining such information. However, the CMS must not be involved in the employee selection process or any other personnel matters.

Certain expanded authorities require adequate separation of duties as well as expertise and experience to adequately control risk. Any changes to the corporate's operational structure will be evaluated to ensure the new structure meets the requirements defined in the Guidelines for Submission of Requests for Expanded Authorities and Part 704 Guidance Letter No. 2, and those approved by the NCUA Board and SSA, if applicable.

ALM Modeling, Assumptions, and Results

Effective asset/liability management is the cornerstone of a safe and sound financial institution. ALM modeling results are affected by the methodology applied and the assumptions used. The CMS will review any changes to:

1. model(s) used by the corporate;
2. assumptions used in the model(s);
3. management reports generated by the models; and
4. management's review process and documentation of model results.

The CMS will determine whether such changes are appropriate and consistent with the corporate's complexity and approved level of expanded authorities. In general, new models and/or assumption changes should be run parallel with the old model(s) and/or assumptions to determine the effect of these changes versus changes in the corporate's portfolio and the market environment. The analysis resulting in the changes should be maintained by the corporate for review during the annual examination period.

Corporates with expanded authorities are expected to have their ALM modeling methods validated periodically. A qualified third party should conduct such validations and the results reported to the Asset-Liability Committee.

Monitoring Strategic Plans and Initiatives
The CMS will review the corporate's strategic and marketing plans and periodic product/business line evaluations to ensure management is adequately evaluating current and potential competitors. The corporate's board and management should have plans in place to effectively address competition through either product development, improved efficiencies, and/or exit strategies, if necessary. The CMS will evaluate the effectiveness and timeliness of the corporate's response to competitive market pressures. The CMS will report any concerns to OCCU management and SSA (if state chartered) after discussing them with corporate management.

The CMS will discuss changes in strategic plans, goals, and significant budget variances with senior management to ensure the monitoring and planning process is adequate.

Cultivate Effective Communications
The CMS will foster open communications with corporate management through regular meetings with key managers and staff. Meetings may be formal or informal but in all cases, the CMS should document the topics of discussion for inclusion in the monthly management report.

The CMS will function as a liaison between the corporate, OCCU, and where applicable, the SSA. The CMS on-site presence allows them to coordinate prompt feedback to all parties and to facilitate meetings between respective staff.

As necessary, the CMS will formalize communications by submitting draft correspondence for the OCCU Director's signature. Correspondence involving state chartered corporates will be coordinated with the appropriate SSA.

Corporates applying for expanded authorities must submit detailed documentation supporting their request. Additionally, corporates sometimes require waivers from provisions of Part 704. The CMS will coordinate these efforts with the corporate and provide appropriate guidance in order to expedite the application process. However, the CMS should not construct the documentation for the corporate.

Monitor Effects of Capital Markets Trends

Corporates are affected by changes in the capital markets. Changes in interest rates, credit spreads, and liquidity all affect a corporate's risk position. The CMS will stay abreast of market trends and provide timely feedback to OCCU, and the SSA, if applicable, regarding any material effects of changes to their assigned corporate(s).

The CMS will regularly evaluate the following and discuss any significant changes or concerns with corporate credit union management:

1) The effect of changes in interest rates on:
    a. the duration and weighted average life of the corporate's investment portfolio;
    b. the corporate's NEV; and
    c. the corporate's net income.

2) The effect of changes in market sector credit spreads on:
    a. the corporate's NEV; and
    b. the corporate's liquidity.

3) The effect of changes in market liquidity levels on:
    a. the corporate's ability to fund member demands; and
    b. the corporate's ability to raise liquidity from available sources.

Corporates with Part III expanded authorities are exposed to sovereign risk. The CMS will stay informed of the countries to which the corporate has exposure. Any potential changes to a country's risk rating should be evaluated and discussed with corporate management. Where appropriate, the CMS will utilize Bloomberg to monitor investment values, as well as, market activities, which will impact the corporate's balance sheet or risk profile. Additionally, for institutions with Part III expanded authorities, the CMS will monitor the sovereign ratings and news items for countries and financial institutions the corporate has approved for investments.

Monitor Changes in Balance Sheet Structure

A corporate's role as a liquidity center may require management to restructure the balance sheet in response to changing member needs and market conditions. The CMS will evaluate trends at least monthly by reviewing the Corporate 5310 Call Reports. Key information will be verified to internal financial statements, General Ledger balances, and/or subsidiary reports. The CMS should utilize the Consolidated Balance Sheet (CBS) to evaluate monthly trends and to identify and monitor fluctuations.

Corporate management utilizes numerous internal management reports. These reports may be generated daily, weekly, monthly, or quarterly. If corporate management utilizes a daily balance sheet report, the CMS should obtain them to identify changes in the corporates balance sheet structure. Such reports are especially useful during times of low liquidity when corporates may have to liquidate assets or borrow to meet member liquidity demands.

Review Material Risk Areas for Compliance

The CMS will utilize the Corporate'*s* 5310, CBS, ALM reports, and management reports to monitor compliance with Part 704 and corporate policies. At a minimum, the CMS will verify compliance with key regulatory risk limits including, but not limited to:

1. the NEV ratio;
2. the maximum allowable change in NEV in +/- 300 basis point interest rate shock tests;
3. the change in net interest income in +/- 300 basis point shock tests;
4. the capital ratio;
5. credit concentration limits;
6. reserve transfers;
7. lending limits;
8. borrowing limits; and
9. credit ratings.

In addition to the above listed regulatory limits, the CMS should also review the corporate's investment and credit watch lists to monitor securities facing possible downgrades. The CMS will monitor all watch list securities on Bloomberg for press releases, downgrades, and any other information that may be available.

Lending and borrowing trends should be monitored as increased activity in these areas may reflect decreasing liquidity in the credit union system. This monitoring may occur through the review of the corporate's lending activities to members as well as its borrowing activity on both and overnight and term basis.

Any regulatory violations or negative trends should be promptly reported to OCCU and the SSA, if applicable.

Planning Focused Supervision Activity

Chapter 102 of this guide outlines normal examination/supervision planning. In addition to normal planning, the CMS must plan regular on-site supervision activity. This supervision activity is determined using the targeted risk approach.

Supervision of federally chartered corporate credit unions should be developed jointly with the appropriate corporate field supervisor. Supervision of state chartered corporates must also be coordinated with the appropriate SSA.

As described in Chapter 102, OCCU's supervision policies require a specific supervisory strategy for each corporate. Planning for on-site supervision presence is ongoing. Ongoing supervision activity may be daily, weekly, monthly, or quarterly. Appendix A of this chapter contains a checklist of standard on-site supervision activity. The CMS, CFS, and the SSA if the corporate is state chartered, will complete a separate checklist for each assigned corporate.

Actual supervision activities will vary between Type II and Type III corporates and between individual corporates as situations warrant. Type II corporate supervision activities may be less frequent or reduced in scope compared to those for a Type III corporate since the CMS are only on-site part-time.

The CMS will tailor the regular supervision activities to the specific corporate. In addition, the CMS will exercise judgment by recommending any additional supervision deemed necessary to the CFS.

Following the conclusion of the annual examination the CMS, CFS, and SSA if the corporate is state chartered, will develop a detailed supervision plan for the following year. The plan will outline supervision activities addressing significant risk areas or areas of concern for each quarter. The plan will be submitted to the Director of OCCU for final approval. The plan may be reviewed and revised as necessary.

Use of Other NCUA Resources
When planning on-site supervision activities, the CMS may determine a need to utilize other specialized NCUA examiners. These include but are not limited to:

1. OCCU Information Systems Specialist;
2. OCCU Subject Matter Examiners; and
3. Office of Strategic Program Support and Planning Investment Officers.

The CMS will be actively involved in the examination and supervision planning process. However, another corporate examiner may serve as the EIC and perform monthly supervision. This will allow the CMS to focus on the corporate's risk activities. The EICs will be rotated every three years or as necessary.

Recommendation For Continued On-site Presence
The CMS will work with the EIC after the conclusion of each annual examination to develop the supervision plan for the following year and contingent plans for the subsequent two years. This plan will include a recommendation regarding the continued level of on-site supervision. The planning process will include the SSA if the corporate is state chartered. The plan will be submitted to the Director of OCCU for approval.

Communication with SSA
The CMS is expected to keep the SSA or his/her designee informed of any material issues discovered during on-site supervision. To facilitate effective communications, the CMS will provide the SSA with a schedule reflecting the dates of on-site supervision activity and phone numbers where the CMS may be reached. When practicable, on-site supervision will be scheduled to allow participation by SSA staff. When SSA staff is unable to participate in the on-site supervision activities, the CMS will maintain regular contact with the SSA or his/her designee via telephone and/or e-mail to ensure information is communicated timely.   The CMS will facilitate meetings between OCCU supervisors and the SSA when necessary.

Training

Maintaining an on-site supervision presence offers the CMS opportunities to gain in-depth knowledge of corporate operations. The CMS will share this knowledge with other corporate examiners by developing and instructing focused training courses. These courses will be developed to provide logical progressive training for both new and seasoned corporate examiners.

The CMS will also serve as mentors for new corporate examiners. The new examiners will spend time on-site with the CMS and receive orientation training regarding corporate credit unions and their unique role in the credit union system. Maintaining a regular on-site presence provides ready access to corporate policies and procedures as well as opportunities to observe corporate operations. This type of orientation training is intended to accelerate the development of new corporate examiners.

Periodically, the CMS may be called upon to develop and deliver presentations to NCUA staff and external groups. These presentation opportunities afford OCCU an opportunity to share in-depth knowledge of corporate credit union investment products and correspondent services with both NCUA staff and others.

Chapter 104

STATE-CHARTERED CORPORATE CREDIT UNIONS

Introduction

NCUA recognizes state regulatory agencies are primarily responsible for the supervision of state-chartered federally insured corporate credit unions (FISCCU) and non-insured corporate credit unions (NISCCUs). Since all corporate credit unions provide deposit, liquidity, and correspondent services to federally insured credit unions, however, NCUA has an obligation to assess the risk FISCCUs and NISCCUs present to the National Credit Union Share Insurance Fund (NCUSIF). This obligation is reflected in Parts 704 and 741 of NCUA's Rules and Regulations.

Ongoing supervision is a key element of determining that FISCCU's and NISCCU's are operated in a safe and sound manner. Although state and NCUA examiners have distinct roles and responsibilities in the oversight of FISCCUs and NISCCUs, both employ similar processes in administering their duties.

A cooperative and coordinated effort between NCUA's Office of Corporate Credit Unions (OCCU) and State Supervisory Authorities (SSAs) is essential to ensure FISCCUs and NISCCUs are effectively regulated and supervised, and that risk to the NCUSIF is properly identified and monitored.

Information Sharing

NCUA and SSAs will make every reasonable effort to share information regarding FISCCUs and NISCCUs under their mutual jurisdiction, and on issues affecting the corporate system as a whole. Each SSA will provide OCCU copies of examination reports or other supervision activities performed independently for use by OCCU in monitoring risk to the NCUSIF. SSAs and OCCU will copy each other on correspondence and reports to FISCCUs and NISCCUs under their mutual jurisdiction.

The SSA may also request copies of OCCU examination reports and other related documentation for corporate credit unions serving credit unions the SSA regulates. OCCU will make reasonable efforts to satisfy all such requests. SSAs may be requested to enter into Confidentiality Agreements with NCUA before such information will be shared.

Joint Examinations/Insurance Reviews

Scheduling

When NCUA and the SSA jointly participate in the examination or on-site supervision of a FISCCU or NISCCU, appropriate NCUA and SSA staff will coordinate scheduling of all on-site contacts. NCUA and the SSA will mutually agree upon the dates of all onsite contacts with sufficient advance notice to allow both agencies to participate.

Designation of Examiner-in-Charge

Both the SSA and NCUA may designate an examiner-in-charge (EIC) for a joint examination and insurance review. Each agency will be responsible to ensure that its EICs are properly trained and have adequate experience to serve in that capacity.

To clarify the distinction between supervisory and insurance activities and objectives, the designations "Supervisory EIC" and "Insurance EIC" may be used for the SSA and NCUA EICs, respectively, if desired, and mutually agreed upon by the agencies.

Examination Report Format, Scope, and Process

NCUA will adhere to the Corporate Examiner's Guide for the standard format, scope, and process to be followed for each FISCCU and NISCCU examination. To maximize efficiency and minimize redundancy, NCUA and the SSA will share examination work papers and other relevant documentation to the maximum extent feasible.

Each joint examination and insurance review will include a formal planning process. The EICs will jointly develop the scope and team assignments to be used during the examination. To ensure effective use of resources, examination scopes will be determined on a risk-assessment basis and mutually agreed upon prior to the start of examination fieldwork. The SSA and NCUA EICs as part of the pre-examination planning process will agree to arrangements for sending the examination request lists to the FISCCU or NISCCU. In addition, the SSA and NCUA EICs will develop a plan for issuing a transmittal letter to the FISCCU or NISCCU.

During the planning process, the EICs will also determine which agency will write the examination report. All examination reports will be subject to review and approval by both agencies prior to transmittal to the institution. Production of a single examination report incorporating the findings and recommendations of each agency is preferred. In the unlikely event production of a single examination report is not possible, the SSA and NCUA may issue a separate regulatory and insurance report, respectively, if either agency determines separate reports are necessary.

The SSA and NCUA EICs should strive to reach compatible conclusions and recommendations. The SSA and NCUA EICs will discuss all findings, conclusions, and recommendations before presentation to, or discussion with, corporate credit union management. If the SSA and NCUA EICs cannot reach mutual agreement on examination and supervision related issues, or on matters to be included in the examination report, they will defer to their respective supervisors for resolution before discussing the issues with corporate credit union officials.

Additional On-site Supervision

In addition to review of independent SSA examinations or participation in joint examination and insurance reviews, NCUA monitors FISCCUs and NISCCUs monthly. Monthly monitoring procedures include review of: 5310 reports; board packages; other electronic or telephonic means; correspondence; and other information provided by the SSA. Under normal circumstances, these examination and monitoring processes provide sufficient information for OCCU to assess NCUSIF risk from each FISCCU or NISCCU.

Both OCCU and SSAs recognize additional onsite supervision may be necessary under certain circumstances, and will strive to ensure such supervision is conducted in a cooperative and mutually beneficial manner. If either the SSA or NCUA independently determines additional on-site supervision is necessary, the SSA and OCCU will notify the respective agency, inform each other of the issues or concerns involved, and invite each other to jointly perform such supervision. Whether the additional supervision is performed jointly, or independently, the SSA and NCUA will provide each other with copies of all correspondence related to the on-site supervision.

Corporate Credit Union Training

Both NCUA and SSAs are committed to ensuring examiners participating on corporate credit union examinations are well trained. To that end, and at its discretion, NCUA will make as much of its corporate credit union related training programs provided to OCCU examiners available to SSA examiners, as is reasonably possible. The SSA and NCUA recognize that some training programs (e.g., for Capital Markets, Information Systems, Payment Systems) are developed for specific NCUA positions and are unavailable to other OCCU staff. Likewise, these specialized training programs are not available for SSA staff.

Corporate credit union training may include participation in examinations or other activities conducted at various federal or state chartered corporate credit unions. Each SSA may request participation in any OCCU examination(s) to provide training opportunities for the SSA's corporate examiners. OCCU will make reasonable efforts to accommodate such requests. SSAs may be required to enter into a Confidentiality Agreement with NCUA and/or other SSAs as a condition of providing this type of training.

SSA participation in corporate credit union training will be coordinated through the NASCUS State Programs Coordinator in the same manner other NCUA training is handled. Each SSA will ensure examiners participating in NCUA provided training opportunities possess the skills and prerequisites appropriate for the training being provided.

Federal Corporate Credit Union Examination Participation

An SSA may request to participate on OCCU examinations or other supervisory activities of federal corporate credit unions to determine the safety and soundness of the corporate serving the credit unions the SSA regulates. OCCU will make reasonable efforts to accommodate such requests. SSAs may be required to enter into a Confidentiality Agreement with NCUA as a condition of such participation.

Release of FCCU Examination Reports

SSAs are also requested to enter into Confidentiality Agreements when requesting copies of examination reports for federally chartered corporates located in their states, if participation in the examination did not occur.

Expanded Authorities and Waiver Requests

Part 704 of NCUA Rules and Regulations require the SSA to act on applications for expanded authorities or waivers of the rule from FISCCUs or NISCCU's before the NCUA Board will consider such applications. If the SSA denies a request, NCUA will concur with the denial. To facilitate this procedure, it is requested that a copy of the SSA denial letter be sent to NCUA.

If the SSA approves a request, NCUA staff will review the request and will provide the NCUA Board with a recommendation. In the event the SSA supports a FISCCU or NISCCU's request for expanded authority, however, the NCUA Board does not approve the request both the corporate and the SSA will be notified of such decision(s). To reduce regulatory burden and maximize resource utilization, SSA and NCUA staff should conduct reviews of these requests, including any activities conducted onsite at the corporate credit union, jointly, whenever possible.

Transmittal Letters

If a joint examination report is issued and signed by both the NCUA and SSA EICs, a standard supplement to the report includes the mailing of a transmittal letter to the chairman of the corporate's board of directors. Unless otherwise agreed, the originator of the transmittal letter will be the SSA in coordination with NCUA. If any SSA does not wish to send a transmittal letter, NCUA may send one.

Correspondence

Copies of all correspondence material impacting the continued safety and soundness of the NCUSIF will be provided to NCUA. Copies of NCUA's correspondence will be routinely sent to the appropriate SSA.

Administrative Actions

Administrative Actions will be addressed in Chapter 501 of this Guide as part of the next Guide revision.

Chapter 201

INVESTMENTS

Introduction

The continued development of new security types and the complexity of instrument structures make comprehension and analysis of investments increasingly difficult. While financial risks borne by corporate credit unions (corporates) are monitored and controlled at the balance sheet level through a formal ALM process, risks inherent in individual investment assets must be understood in order to have sufficient intuition to identify sources of risk and test appropriateness of the measure of risk for a particular instrument.

Prudent investment portfolio management practices, such as managing concentration risk and maintaining diversification, are as important for corporates as for other investors.

Concentration risk is the risk associated with having excessive exposure to securities that have related market and/or credit risk. Concentration in market risk could include, but is not limited to, excessive exposure to interest rate, basis, embedded option and/or liquidity risks. Concentration in credit risk may also include excessive exposure to certain industries, groups, or individuals.

Diversification is an investment management technique used to reduce risk without reducing expected return. Diversification theory holds that price volatility can be reduced while achieving a given return by distributing assets among a variety of asset classes, geographic regions, and issuers. Diversification usually reduces the portfolio risk because returns on various types of securities are not perfectly correlated.

Failure to manage concentration risk or adequately diversify the portfolio may give rise to excessive liquidity risk. Corporates must be especially mindful of liquidity when making investment decisions since investment portfolio(s) are the primary source of funds to meet ongoing and contingent liquidity demands.

While it is true the interest rate risk (IRR) of an asset should be viewed in the context of the entire portfolio or balance sheet, an examiner‟s professional judgment about the source, magnitude and impact of risk begins with an understanding of the risk inherent in individual investment structures. To measure concentrations of interest rate, liquidity, and credit risk, individual investments must be measured accurately and aggregated across all transaction types.

Examiners should ensure corporates "have programs and processes to manage the market, credit, liquidity, legal, operational, and other risks" of investment securities and, where authorized, end-user derivative activities. To this end, Interpretive Ruling and Policy Statement 98-2 (IRPS 98-2) provides guidance covering the broad range of investment instruments permissible for corporate credit unions.

Investment Policies and Procedures

Corporate investment portfolios vary considerably in size and complexity. Similarly, the expertise of corporates‟ investment staff and related internal controls varies considerably from corporate to corporate, largely as a function of the size and complexity of the investment portfolio and the corporate‟s asset size. However, certain minimum infrastructure must exist, dependent upon the risks associated with the type of investment transactions the corporate undertakes. Corporates engaged in the same type of investment transaction(s) must perform similar pre- and post-purchase credit and/or IRR analysis, regardless of the corporate‟s asset size or the size and complexity of the investment portfolio. The existence of compensating internal controls (i.e., ALCO meetings, periodic internal audits of credit and IRR) should not be accepted as a substitute for comprehensive, timely, and professional due diligence and sound internal controls.

Investment policies, procedures, and limits provide the structure for the board to control and the staff to manage investment activities. Section 704.5(a) states: "A corporate credit union must operate according to an investment policy that is consistent with its other risk management policies, including, but not limited to, those related to credit risk management, asset and liability management, and liquidity management."

An effective investment policy should clearly define the risks and cash flow characteristics of authorized investment types. This is particularly important for products that have unusual, leveraged, or highly variable cash flows. A corporate should not acquire a position in a particular type of instrument until the board has a general understanding of the instrument and its impact on the corporate‟s financial condition. The board must also ensure it attracts and retains qualified senior management and staff, with adequate understanding of the instruments and their associated risks.

Policies should clearly outline the approach for managing investments, including financial derivatives. These policies should be consistent with the corporate‟s broader business strategies, capital adequacy, technical expertise, and general tolerance for market, liquidity, and credit risk.

Policies must identify relevant objectives, constraints, and guidelines for both acquiring investments and managing portfolios. Policies should establish a logical framework for identifying, measuring, monitoring, reporting and controlling the various risks involved in the corporate‟s investment portfolios, including any financial derivatives.

Policies must clearly articulate the types of permissible investments and derivative contracts. Permissible investments and derivatives should be consistent with the corporate‟s objectives and strategies. Benchmarks must be established to facilitate the periodic evaluation of the performance and effectiveness of investment holdings, strategies, and programs. Whenever multiple objectives are involved, management should prioritize objectives in light of actual or potential conflicts.

Section 704.5(a) requires an investment policy address, at a minimum:

1. Appropriate tests and criteria for evaluating investments and investment transactions before purchase; and
2. Reasonable and supportable concentration limits for limited liquidity investments in relation to capital. (Limited liquidity investments are defined as a “private placement or funding agreement.”)

Procedures developed by investment personnel typically identify the specific tests, risk analysis processes, and selection criteria for evaluating potential investment positions.

Should a corporate lack sufficient infrastructure for engaging in investments of a particular type (ABS, private placements, etc.), examiners should develop a Documents of Resolution requiring the board of directors to balance the corporate‟s investment activities with its infrastructure. This may require cessation of certain investment activities until an adequate infrastructure is implemented. Regardless of the corporate‟s current asset size or operating authority level, infrastructure should be reasonably adequate to manage unanticipated increases in the level of credit, IRR, and liquidity risk due to changing economic conditions.

It is normal practice for the board to delegate investment authority to senior management. Consequently, the board and senior management are responsible for hiring qualified personnel and ensuring adequate procedures are in place for conducting investment activities on both a long-range and day-to-day basis, in accordance with the board‟s approved investment policy.

There should be clear lines of authority and responsibility in the following areas:

Board responsibilities (authorized through policy):

1. Purchase and sale of investments;
2. Enactment of appropriate limits on risk taking (limits on transaction types and on authorized personnel);
3. Establishment of effective internal controls (both board, management, and internal audit functions); and
4. Enactment of comprehensive risk-reporting and risk-management review processes commensurate with the corporate‟s risk profile.

Staff responsibilities (implemented through procedures):

1. Establishment of adequate systems for measuring risk; and
2. Development and implementation of acceptable standards for valuing positions and measuring performance.

Investment Portfolio Strategies

An examiner‟s evaluation of portfolio risk and return must be coordinated with the ALM review. Specific portfolio management measures are discussed in Chapter 202 (see Setting Financial Goals: The Risk/Return Profile) of this Guide.

The framework for a corporate‟s investment portfolio risk management process includes:

1. The board establishes risk tolerance thresholds (e.g., Net Economic Value (NEV) and credit limits);
2. The board and ALCO periodically approve a risk target (a benchmark) for management to meet that is within the risk limits; and
3. Management optimizes portfolio performance consistent with risk target levels, in light of current market conditions.

The traditional perspective is spreads must be sufficient to cover the cost of operations and provide capital enhancement. Value-based measures of performance, like NEV, have gained increasing acceptance in recent years. By focusing on total return, institutions manage for long-term value, rather than managing to short-term accounting results.

Many institutions historically focused on earnings-oriented measures of return without adjusting for risk. For example, it was common for corporate portfolios to be managed and evaluated *only* by current net interest spread without relating the risk to equity -- that portion of capital required to support risk between the funding source and the portfolio‟s assets. Best practice requires all portfolios to have specific capital allocated in light of the portfolio‟s NEV. A summary of the measures of return performance discussed in Chapter 202 are included in Table 1.

Table 1

Measures of Return Performance:

A. Earnings-oriented measures
   a. Net interest margin
   b. Core Income
   c. Net Income
   d. Return on assets
   e. Return on equity

B. Market value-oriented measures
   a. Market capitalization
   b. Liquidation value
   c. Going-concern value
   d. Net economic value

C. Both – Total Return

Book of Business Approach

Consistent with an earnings-oriented measure, many corporates allocate investments into discreet portfolios and target net interest spreads. These portfolios will usually have defined parameters for maturity and/or cash-flow behavior and are commonly referred to as "books of business."

The typical strategy focuses on acquiring a discrete pool of investment assets with similar maturity and/or payment characteristics to those of a discrete pool of liabilities.

The terms "matched" and "managed" are used to further describe these portfolios. The term "matched" generally means a portfolio‟s assets and liabilities have virtually the same cash flow characteristics and maturity. The term "managed" generally means a portfolio‟s assets and liabilities are not required to have identical cash flow characteristics or maturities.

Corporates calculate the net interest margin, or "spread," associated with these books of business by measuring the accounting income from interest bearing assets and subtracting the cost of interest bearing liabilities. This calculation is usually computed for each book and reconciled to total net interest income.

Common books of business may include:

1. Overnight (or Liquidity) Book. Overnight and core shares are used to fund primarily overnight assets. It is not unusual for a corporate to run an intentional maturity mismatch on a portion of the overnight portfolio by including term assets with floating rate coupons or fixed-rate money market transactions of about 90 days or less.

2. Term Book. Term share certificates are used to fund term investments of substantially similar maturity and payment characteristics. A term book is generally comprised of fully matched transactions with little or no risk to the book‟s net interest margin.

3. Variable Rate Book. Adjustable-rate share certificates (term) are used to fund a combination of floating and/or adjustable rate assets. The rate paid on the shares is adjustable on a daily, monthly or other periodic setting and is typically set on an ability-to-pay basis. Many variable rate certificates may be linked to a specific index (e.g., LIBOR, Fed Funds Effective, or T-Bills) rather than an administratively determined payout rate. A variable rate book is not necessarily a matched portfolio. Portfolio parameters may permit material basis, embedded option and/or maturity mismatches.

4. Membership Capital Book. Member contributed capital is typically a non-maturity instrument. Assets allocated to this book of business vary, reflecting the risk tolerance of the corporate, and often have a combination of short to intermediate maturities. The rate paid on membership shares is generally administered and set on an ability-to-pay basis.

5. Capital Book. The reserves of the corporate are matched against all interest bearing assets not allocated to other books of business. Since reserves and undivided earnings are not interest bearing, the

spread on the capital book is typically expressed as the dollar weighted yield on the assets. Corporates are also permitted to issue paid-in capital shares (PIC) as a supplemental source of capital. The terms and conditions of PIC are unique factors determined at the time of issuance.

A book of business approach can provide an intuitive way to segment total net interest income into individual portfolios and meet regulatory requirements. It does not; however, provide a market value or future-earnings-at-risk perspective unless NEV is incorporated.

Best practice for performance measurement is on a risk-adjusted basis. Examiners need to encourage performance reports for spread management strategies include risk adjustments that reflect NEV exposure. This will permit senior management and officials to comprehend the risk-reward tradeoff that has been achieved.

Balance Sheet Risk Measurement

The IRR associated with individual investments and the aggregate IRR associated with an entire portfolio are captured in NEV. It is essential portfolio risk be adequately modeled and monitored against pre-established NEV limits to avoid Section 704.8 violations and an unsafe and unsound IRR position. Best practices require investment policies and procedures include limits and performance standards for each portfolio, in addition to aggregate limits.

Examiners should review the established risk targets (NEV and liquidity parameters) for each portfolio and determine whether funds are invested accordingly. If portfolio risk significantly varies from the target, it implies the board has granted management the discretionary authority to establish its own benchmark. This makes relative performance an increasingly subjective measure for the board to evaluate. Therefore it is prudent for the board to:

1. Establish the maximum level of risk with which it is comfortable (limits which ideally are more restrictive than the regulatory requirements);
2. Approve periodically management‟s risk target(s) within those board established limits; and

3. Evaluate the portfolio‟s performance in light of those targets.

Regardless of the portfolio management approach taken, corporate staff should periodically review the performance and effectiveness of investment portfolio strategies. The review should be conducted no less than quarterly. Corporates with large or highly complex investment portfolios should conduct this review more frequently. The review should evaluate the extent to which the corporate‟s investments and derivatives are meeting the various objectives, risk tolerance, and guidelines established by corporate policies. Investment reporting prepared for ALCO and the board should include periodic results (risk and return) compared to established performance benchmarks.

Risks Associated With Investment Transactions

The three basic risks assumed by corporates in the investment portfolio are market, liquidity and credit. Interest rate and liquidity risk are defined and discussed in the section of Chapter 202 entitled "Measuring Risk Exposure".

The board of directors has the ultimate responsibility for the level of risk taken by the corporate. Accordingly, the board should approve overall business strategies and significant policies that govern risk taking, including those involving investment and derivative contracts. In addition, the board should periodically reevaluate the corporate‟s business strategies and significant risk management policies and procedures, placing special emphasis on the corporate‟s financial objectives and risk tolerances.

The process of measuring, monitoring, and controlling risk within a corporate should be reasonably independent from those individuals having investment transaction authority.

The nature and degree of this independence should be scaled to the size and complexity of a corporate‟s investment and derivative activities. Corporates with large and complex balance sheets, or with significant portfolios of complex investments, are expected to have risk managers or risk management functions fully independent of individuals who have the authority to conduct transactions. Conversely, corporates with less complex investments (base/base plus authorities) should ensure there is a mechanism for independently reviewing both the level of risk exposures created by investment holdings and the adequacy of the process used in managing those exposures. Depending on the size and nature of the corporate, this review function may be carried out by either management or a board committee.

Regardless of size and sophistication, corporates should ensure back office, settlement, and transaction reconciliation responsibilities are conducted and managed by personnel who are truly independent of those initiating risk taking positions. Where it is truly impractical to fully segregate these functions, risk mitigating procedures must be in place.

Credit risk is discussed below. These risks must be evaluated on-going to establish and maintain a sound risk management system.

Credit Risk of Investments

Corporates are somewhat unique as depository institutions because their assets are predominately comprised of investments and they generally have only nominal amounts of loans outstanding. Part 704 restricts rated investments to those that are investment grade and significantly limits the amount of credit risk exposure a corporate can assume according to each corporate‟s expanded authority level. Regardless, credit risk requires formal consideration in the risk management process.

Definition of Credit Risk[1]

> (1) Exposure to loss as a result of default on a debt, swap or some other counterparty instrument. (2) Exposure to loss as a result of a decline in market value stemming from a credit downgrade of an issuer or counterparty. (3) A component of return variability resulting from the possibility of an event of default. (4) A change in the market‟s perception of the probability of an event of default (affecting spreads).

[1] The Dictionary of Financial Risk Management, Gary L. Gastineau and Mark P. Kritzman, Frank J. Fabozzi Associates, 1996.

NCUA Interpretive Ruling and Policy Statement (IRPS) 98-2[2]

NCUA adopted key elements of the Federal Financial Institution Examination Council (FFIEC) proposed supervisory policy statement on investment securities and derivatives. Key elements of IRPS 98-2 are:

1. The institution should not acquire investments or enter into derivative controls without assessing the creditworthiness of the issuer or counterparty.

2. The credit risk arising from these positions should be incorporated into the overall credit risk profile of the institution as comprehensively as practicable.

3. Institutions should be legally required to meet certain quality standards (i.e., investment grade) for security purchases.

4. Institutions should maintain and update ratings reports from at least one nationally recognized statistical rating organization (NRSRO).

5. Institutions should be required to establish limits on individual counterparty exposures. Such limits should define concentrations relating to a single or related issuer or counterparty, a geographical area, or obligations with similar characteristics.

6. In managing credit risk, institutions should consider settlement and pre-settlement risk. It includes the risk a counterparty will fail to honor its obligation at or before the time of settlement. The selection of dealers, investment bankers, and brokers is particularly important in effectively managing these risks.

7. The approval process for banks, broker/dealers, and other counterparties should include a review of each firm"s

[2] The NCUA Board passed IRPS 98-2 on April 7, 1998 with an effective date of October 1, 1998.

financial statements and an evaluation of its ability to honor its commitments.

8. An inquiry into the general reputation of the broker/dealer is also appropriate. This includes review of information from state or federal securities regulators and industry self-regulatory organizations such as the National Association of Securities Dealers concerning any formal enforcement actions against the dealer, its affiliates, or associated personnel.

9. The board of directors is responsible for supervision and oversight of the investment portfolio and end-user derivative activities, including the approval and periodic review of policies that govern relations with securities dealers.

10. Sound credit risk management requires credit limits be developed by personnel who are as independent as practicable of the acquisition function.

11. In authorizing issuer and counterparty credit lines, these personnel should use standards consistent with those used for other activities conducted within the institution and with the organization‟s overall risk management policies and consolidated exposures.

Effective risk management addresses risks across all types of instruments on an investment portfolio basis and ideally, across the entire institution. Corporates need to recognize the inherent credit risk associated with investment and lending activities and integrate credit risk management with that of market and liquidity risk management. The basic steps set forth by this FFIEC policy statement will help to promote a more effective identification, measurement, monitoring, reporting, and controlling of the institutions‟ credit risk.

<u>Sources of Credit Risk</u>

Investments have varying degrees of credit risk depending upon:

1. The risk of the obligor/counterparty; and
2. The structure of the transaction (quality of the underlying collateral, level of subordination and/or credit enhancements).

Corporates should devote credit analysis resources proportional to the amount of credit risk inherent in the activities authorized by the board. For example, when assessing the risk of default, an unsecured transaction with a lower potential collection rate (like bank time deposits, corporate debt, commercial paper or federal funds) should receive more timely credit reviews than a highly secured transaction (like repurchase agreements or asset-backed securities). However, a clear understanding of the quality of the collateral in structured securities and how they behave in adverse market conditions is critical to controlling risk. Collateral performance should be reviewed as often as the servicer provides the appropriate report. Transactions with lower credit risk should still receive appropriate attention from the standpoint of market and liquidity risk.

The frequency and depth of credit reviews done by corporates should be driven by the relative degree and magnitude of credit risk. Credit risk exposure has traditionally been measured by the face or par amount of a transaction since that often is viewed as the total potential loss. However, the actual recovery rate in the event of default will vary from one instrument to the next based upon the priority of the holder‟s claim and the amount of credit support (enhancements) in the structure. For example, a $10 million repurchase agreement fully secured by U.S. Treasury securities has less credit risk than a $10 million bank time deposit ($100,000 FDIC insurance notwithstanding).

Corporates need to make sure each source of credit risk is properly measured, monitored, reported and controlled. Complex investment structures, such as mortgage-backed and asset-backed securities (MBS and ABS), may involve numerous components of credit exposure that need to be tracked on a global basis to ensure all concentrations are identified.

Corporates must have a clear and consistent methodology for measuring the relative amounts of credit risk inherent in each transaction and make sure these risk measures are aggregated across all transaction types for each entity concerned. Some forms of credit enhancement provided by a single entity, such as private insurance or a letter of credit, may exist in various different securities within the same portfolio.

For example, at the base and base-plus levels, concentration limits are established in Part 704. Part I and Part II authorities (prescribed in Appendix B of Part 704) permit the corporate to set its own limits on certain transactions. In establishing expanded authority limits that exceed base and base-plus authorities, it is particularly important increasingly sophisticated methodologies be used for credit risk measurement.

Table 2 details instruments, obligors and relative quality (degree of enhancement).

Table 2

Instrument	Obligor/ Counterparty	Maturity	Quality
Sale of Fed Funds	Banks, credit unions, some Government Sponsored Enterprises (GSEs) (i.e., FHLB)	Typically 1 day	Unsecured obligations of financial institutions
Negotiable CDs	Banks	Typically 1-6 months, minimum 14 days	Deposits up to $100,000 insured by FDIC
Deposit Notes	Banks	Typically 18 months to 5 years	Deposits up to $100,000 insured by FDIC
Eurodollars Non-negotiable time deposits Negotiable CDs	Banks: Foreign branches of U.S. banks or foreign banks	Overnight to 5 years 1 year or less	Unsecured obligations of banks
Securities Purchased under Agreement to Resell and Securities Sold under Agreement to Repurchase	Broker/dealers, banks	Majority is overnight, typically 1 day to 1 month; terms may exceed 1 year	Secured by securities and cash; securities "sold" typically exceed value of cash received
Securities Lending	Broker/dealers, banks	Typically 1 day to 1 month	Secured by securities and cash
Commercial Paper and Asset-backed Commercial Paper	Corporations, including bank holding companies, and broker/dealers.	Typically 270 days or less	Unsecured obligations of corporations
Corporate Debentures Notes, Bonds	Corporations	Range from 1 to 30+ years	Unsecured obligations of corporations
MBS and ABS	Trust or special purpose vehicle (SPV) generally sponsored by corporations, including GSEs, finance companies, bank holding companies, broker/ dealers, bankruptcy remote trusts, and special purpose entities	Original maturities of 1 to 30 years (amortizing assets have WAL < than stated maturity)	Secured by underlying assets including mortgages, real property and various types of receivables
Mutual Funds	Investment company	Open-ended	Pro rata interest in the assets of the fund (all investments permitted by the fund must be permissible by regulation)
U.S. Treasury Securities Bills, Notes, & Bonds	U.S. Government obligation	Up to 1 year 2 to 10 years Over 10 to 30 years	Regarded to be free of default risk
Sovereign Debt	Foreign government obligations	Typically 3 months to 10 years	Highly rated sovereign debt has little or no default risk; very remote cross-border risk (balance of payment problems)
Foreign Bank Deposits	Non-domestic banks	see Eurodollars	Unsecured obligations of banks; also includes cross-border and center risk (economic/political)

Additional types of instruments, obligors and relative quality (degree of enhancement) are included in Table 3.

Table 3

Instrument	Obligor/ Counterparty	Maturity	Quality
Swaps, Options, Forwards	Typically broker/dealer or bank; may be a special purpose company	Typically 1 month to 5 years (longer expirations exist)	Can be collateralized, credit risk is to a counterparty
Exchange Traded Futures	Organized exchange	1 month to 10 years	Performance bond (margin) and daily mark-to-market; credit risk is to the exchange
Transaction Risk Purchases/Sales	Broker/dealers, banks	Exposed between trade & settlement	Potential market risk (replacement cost)
Extension of Credit to Members	Natural Person Credit Unions, CUSOs, and trade associations	Typically short-term	Can be collateralized by securities or cash
Settlement Risk	Broker/dealers, banks	Short, not delivery vs. payment (DVP)	Exposed to possibility counterparty may declare bankruptcy prior to completing payment

<u>Credit Risk, NEV, and Liquidity</u>

There is a danger corporates may focus upon high credit ratings and simply consider the probability of default (i.e., the higher the rating the less the probability of default). This view relates to the first definition of credit risk previously addressed under the heading of Credit Risk of Investments. Failing to recognize the impact on NEV of credit events other than an event of default ignores a major component of risk. This concept relates to the second and fourth definitions under the same aforementioned heading.

Corporates need to consider credit risk in a mark-to-market framework in order to understand the implications for NEV and liquidity. The volatility of value due to market events (i.e., defaults, downgrades, or other negative news) can have an adverse affect on a corporate's NEV. As NEV declines, the ability to meet potential liquidity demands diminishes.

Regardless of the accounting treatment, corporates should be cognizant of the effect a change in obligor credit quality (also termed a "migration") will have on fair value. Since corporates have a substantial obligation to address contingent liquidity demands, the impact a change in value has upon liquidity is significant (Section 704.9). This is true whether the change in value is driven by either market or credit events (or both).

The integral relationship between market and credit risk makes it difficult to fully separate these into independently managed components. As securities migrate down the ratings scale (one rating downgrade followed by another), the tendency is for price volatility to geometrically increase. Prudent risk managers seek to monitor this potential in order to timely immunize or rebalance the portfolio when credit and market risk exposures exceed acceptable targets or limits.

Corporates need to consider how they will quantify and control concentrations (i.e., obligor, originator, industry, type of instrument, etc.) of credit risk and how the risk will change when market and/or credit conditions change. Thus, understanding how changes in credit quality affect value is an important part of managing the corporate‟s targeted NEV and liquidity levels.

Credit Risk Management

Credit Risk Policies

Credit risk policies may be integrated with a corporate‟s overall ALM and investment policies. It is not imperative credit risk policies be stand-alone, but corporates with increasing levels of expanded authority are likely to establish more elaborate guidelines. Section 704.6(a) requires policy to address, at a minimum:

1. The approval process associated with credit limits**.** This implies a formal management process is adopted to develop and ratify any appropriate limits incorporated into policy. The approval process need not be elaborate, but it should be supported by written procedures. Furthermore, the process should be addressed in the scope of the audit and periodically evaluated for compliance purposes.

2. Due diligence analysis requirements**.** Different transactions represent different levels of complexity as well as varying degrees of risk. Corporates should develop standards and requirements commensurate with exposures. Resource allocation should ensure credit risk evaluations are sufficiently in-depth and timely for each type of material credit risk exposure taken.

3. Maximum credit limits with each obligor and transaction counterparty, set as a percentage of capital**.** The selection and establishment of lines to

broker/dealers, banks, and counterparties is particularly important in effectively managing credit risk. A corporate‟s policy should identify criteria for selecting these organizations and should list all approved firms. The approval process, at a minimum, should include a documented review of each firm‟s financial statement and an evaluation of its ability to honor its commitments. These reviews should be periodically updated.

4. Concentrations of credit risk (e.g., originator of receivables, insurer, industry type, sector type, and geographic). Section 704.6 requires the establishment of maximum concentration limits per obligor and counterparty. The corporate should establish and maintain its own limits (within the regulatory parameters) based upon the preferences and risk tolerance of its board, the corporate‟s operational infrastructure, and overall financial and managerial soundness. A corporate‟s credit policy should also include guidelines on the quality and quantity of each type of investment that may be held. It should provide credit risk diversification and concentration limits. Such limits may define concentrations as those of a single or related issuer or counterparty, in a geographical area, or obligations with analogous characteristics. Policies should include procedures for addressing deterioration in credit quality, such as increased monitoring and stop-loss limits.

The policies of the corporate should recognize credit risk as a risk posed by investment and derivative activities. As such, the corporate must operate under a credit risk management policy commensurate with the investment risks and activities it undertakes.

Sound credit-risk management requires credit analysis be conducted by personnel who are independent of the acquisition function.

<u>Analysis and Approval</u>

The process of evaluating credit instruments should be guided by caution. The cost of approving a mistake may outweigh the opportunity loss of rejecting a "good" credit. The introduction of credit risk to the balance sheet should be undertaken with the same care and diligence as all other portfolio risks (commensurate with the exposure).

The credit analysis and approval process should involve substantive and timely information. Prudent due diligence requires sufficient, in-depth analysis be conducted for obligors and counterparties ("credits") considered for approval. The minimum credit ratings and maximum concentration limits set for base and base-plus corporates in Section 704.6 reflect recognition of existing resource constraints within some corporates. Where best practices cannot or will not be employed, exposure to credit risk should be limited to an immaterial percentage of capital.

The more complex the credit or the greater the potential exposure, the more analysis required. Common sources of information an analyst may utilize include financial statements, press releases, rating agency analyses, discussions with company officers and/or rating agency analysts, fixed income and equity research from securities firms and articles in trade publications. Most of these resources will be maintained in the credit file. Section 704.6 requires information remain in a corporate‟s possession for at least as long as an instrument is in portfolio and until the next examination (if matured or sold between examination reviews).

Examiners should sample credit files to determine the resources utilized. Information should be reasonably current. There should be evidence the analyst(s) is keeping abreast of new developments and critical developments are shared in the reporting process. Reaction to credit news (also termed "credit events") should be evidenced in the minutes of ALCO discussion and included in management‟s risk reports.

The content of credit analysis documentation does not necessarily need to be formal or elaborate. Many analysts make notes directly on the resource materials held in file. Best practice requires an analyst prepare a formal summarization of a credit, with a rationale for its initial approval or reaffirmation, which is signed by the personnel or committee which makes the approval/disapproval decision.

Approval authority should not be superficial. Some institutions simply adopt regulatory limits on types, ratings, and concentrations, and make little effort to consider the appropriateness of establishing different limits. A good manager will set limits tighter than regulatory constraints if such limits express the preference and risk tolerance adopted by the board. This recognizes legality is not an automatic acceptance criterion. Examiners should encourage management not to automatically approve counterparties, obligors, and limits based solely upon prevailing minimum regulatory requirements.

Credit Ratings

A credit rating is an opinion of the general creditworthiness of an obligor, or the creditworthiness of an obligor with respect to a particular debt security or other debt obligation, based upon certain risk factors. Rating agencies provide ratings and research that serve as a valuable tool for investors. However, ratings are not a substitute for prudent due diligence and should only be considered as one factor in an investment decision.

NRSROs are rating agencies recognized by the U.S. Securities and Exchange Commission. Section 704.6 requires that all debt instruments have a credit rating from at least one NRSRO. The NRSRO used at the time of purchase serves as the source to verify any change in rating (compliance with the minimum regulatory ratings). If management decides to change the NRSRO(s) it uses for monitoring its ratings, it should document this decision and report it to the ALCO. Should a corporate use multiple NRSRO ratings to qualify an investment at the time of purchase, Corporate Credit Union Guidance Letter 1999-2 provides guidance regarding regulatory compliance reporting.

NRSROs typically issue different ratings for short-term instruments than for long-term instruments. The long-term ratings are the measure of credit quality that is emphasized by most risk managers. Table 4 includes some rating agencies and their description of long-term ratings.

BBB- represents the bottom of "investment grade"

Table 4: Long-Term Issue Credit Ratings

Rating Agency			
S&P	Fitch	Moody"s	Description of S&P Rating*
AAA	AAA	Aaa	(S&P) "An obligation rated „AAA" has the highest rating assigned by Standard & Poor"s. The obligor"s capacity to meet its financial commitment on the obligation is EXTREMELY STRONG."
AA	AA	Aa	(S&P) "An obligation rated „AA" differs from the highest rated obligations only in small degree. The obligor"s capacity to meet its financial commitment on the obligation is VERY STRONG."
A	A	A	(S&P) "An obligation rated „A" is somewhat more susceptible to the adverse effects of changes in circumstances and economic conditions than obligations in higher rated categories. However, the obligor"s capacity to meet its financial commitment on the obligation is still STRONG."
BBB	BBB	Baa	(S&P) "An obligation rated „BBB" exhibits ADEQUATE protection parameters. However, adverse economic conditions or changing circumstances are more likely to lead to a weakened capacity of the obligor to meet its financial commitment on the obligation."
Gradation Quality			
+ -	+ -	1 2 3	These symbols are used to provide more detailed gradation of quality.
AA CCC	AA CCC	Aa Caa	Range of ratings for which quality gradations are provided.

* Descriptions related to Standard & Poor"s Rating. While agencies tend to use similar definitions, examiners should consult the particular rating agency"s description for a precise description of the investment"s rating.

The long-term ratings described in Table 5 are below the minimum ratings permitted in Part 704 for any level of authority for all corporates.

Table 5: Long-Term Issue Credit Ratings

Speculative grade begins with BB+

Rating Agency			
S&P	Fitch	Moody‟s	Description S&P Rating*
"Obligations rated „BB", „B‟, „CCC‟, „CC‟, and „C‟ are regarded as having significant speculative characteristics. „BB‟ indicates the least degree of speculation and „C‟ the highest. While such obligations will likely have some quality and protective characteristics, these may be outweighed by large uncertainties or major exposures to adverse conditions."			
BB	BB	Ba	(S&P) "An obligation rated „BB‟ is LESS VULNERABLE to nonpayment than other speculative issues. However, it faces major ongoing uncertainties or exposure to adverse business, financial, or economic conditions which could lead to the obligor‟s inadequate capacity to meet its financial commitment on the obligation."
B	B	B	(S&P) "An obligation rated „B‟ is MORE VULNERABLE to nonpayment than obligations rated „BB‟, but the obligor currently has the capacity to meet its financial commitment on the obligation. Adverse business, financial, or economic conditions will likely impair the obligor‟s capacity or willingness to meet its financial commitment on the obligation."
CCC	CCC	Caa	(S&P) "An obligation rated „CCC‟ is CURRENTLY VULNERABLE to nonpayment, and is dependent upon favorable business, financial, and economic conditions for the obligor to meet its financial commitment on the obligation. In the event of adverse business, financial, or economic conditions, the obligor is not likely to have the capacity to meet its financial commitment on the obligation."
CC	CC	Ca	(S&P) "An obligation rated „CC‟ is CURRENTLY HIGHLY VULNERABLE to nonpayment."
C	C	C	(S&P) "The „C‟ rating may be used to cover a situation where a bankruptcy petition has been filed or similar action has been taken, but payments on this obligation are being continued."
D	DDD	WR	(S&P) "An obligation rated „D‟ is in payment default. The „D‟ rating category is used when payments on an obligation are not made on the date due even if the applicable grace period has not expired, unless Standard & Poor‟s believes that such payments will be made during such grace period. The „D‟ rating also will be used upon the filing of a bankruptcy petition or the taking of a similar action if payments on an obligation are jeopardized."

* Descriptions related to Standard & Poor‟s Rating. While agencies tend to use similar definitions, examiners should consult the particular rating agency‟s description for a precise description of the investment‟s rating.

Short term ratings are described in Table 6.

Table 6: Short-Term Issue Ratings

	Rating Agency			
	S&P	Fitch	Moody‟s	Description of Short-term Rating*
Permissible minimum investment grade (Part 704) (See Expanded Authorities)	A-1	F-1	P-1	"A short-term obligation rated „A-1‟ is rated in the highest category by Standard & Poor‟s. The obligor‟s capacity to meet its financial commitment on the obligation is strong. Within this category, certain obligations are designated with a plus sign (+). This indicates that the obligor‟s capacity to meet its financial commitment on the obligation is extremely strong. "
	A-2	F-2	P-2	"A short-term obligation rated „A-2‟ is somewhat more susceptible to the adverse effects of changes in circumstances and economic conditions than obligations in higher rating categories. However, the obligor‟s capacity to meet its financial commitment on the obligation is satisfactory."
Not permissible	A-3	F-3	P-3	A short-term obligation rated „A-3 exhibits adequate protection parameters. However, adverse economic conditions or changing circumstances are more likely to lead to a weakened capacity of the obligor to meet its financial commitment on the obligation."
	B	B	NP (not prime)	"A short-term obligation rated „B‟ is regarded as having significant speculative characteristics. The obligor currently has the capacity to meet its financial commitment on the obligation; however, it faces major ongoing uncertainties which could lead to the obligor‟s inadequate capacity to meet its financial commitment on the obligation."
	C	C		"A short-term obligation rated „C‟ is currently vulnerable to nonpayment and is dependent upon favorable business, financial, and economic conditions for the obligor to meets its financial commitment on the obligation."
	D	D		A short-term obligation rated „D‟ is in payment default. The „D‟ rating is used when payments on an obligation are not made on the date due even if the applicable grace period has not expired, unless Standard & Poor‟s believes that such payments will be made during such grace period. The „D‟ rating also will be used upon the filing of a bankruptcy petition or the taking of a similar action if payments on an obligation are jeopardized."

* Descriptions related to Standard & Poor‟s Rating. While agencies tend to use similar definitions, examiners should consult the particular rating agency‟s description for a precise description of the investment‟s rating.

Corporates should maintain updated ratings reports from one of the major rating services. Individual ratings are usually publicly available, but research reports and news releases are generally obtained through a paid subscription. A paid subscription usually enables the corporate to receive e-mail notification of ratings action on securities in its portfolio once they establish it with the NRSRO. It is critical information be obtained as timely as practical. The ratings and other opinions issued by ratings agencies are not recommendations to buy securities and there is not a warranty on the accuracy, timeliness, completeness, or fitness of the information provided. It is simply one tool to assist an investor in making investment decisions.

Management may (but is not required to) use multiple rating agencies. As noted earlier, corporates should refer to Corporate Credit Union Guidance Letter 1999-2 for guidance when electing to use multiple NRSRO ratings. Management should have procedures in place addressing instruments that receive different credit quality ratings from different NRSROs ("split ratings"). Good credit managers will seek to discover reasons behind split ratings on instruments they hold or consider for purchase. If ratings become split after purchase, many corporates consider this an appropriate criterion for placing it on the credit watchlist. It can signal either a warning (possible deterioration) or an opportunity (possible improvement). Experienced portfolio managers know both circumstances are significant.

Examiners should be alert to whether a corporate is subscribing to multiple rating agencies as a means of "shopping" for a favorable rating. If the corporate"s designated NRSRO is different for each bond being purchased, "cherry picking" may be indicated. A review of the supporting analysis should help determine if the analyst is mimicking the most favorable research or if independent judgment is really exercised. Analysts are not expected to possess greater insights than rating agencies, but they are expected to understand the implications and conclusions of the research and form an independent judgment.

Some rating agencies have been slow to alter their credit outlook on an issuer, industry, or region which eventually resulted in substantial credit quality changes (more than one gradation change in credit ratings at one time). Because corporates are limited to the top investment grade scale, large changes in credit quality are a concern since they generally trigger regulatory requirements (Section 704.10 – Investment action plan). Credit risk managers must be mindful credit ratings are generally a "lagging" indicator.

Measuring and Monitoring Risk

The credit exposures inherent in corporates" investment activities have multiplied and become more complex as new instruments and debt structures have come to market. Financial products are increasingly complex in part because of the proliferation of credit enhancement mechanisms supporting these instruments. These include, but are not necessarily limited to, third-party guarantees, posted collateral, margin arrangements, credit derivatives, and netting. Additionally, new mortgage products such as interest only, option arms, and negative amortization loans have been widely securitized. These new loan types present additional challenges when evaluating the credit risk of a structured security.

With this growth there is an increasing need for more sophisticated risk measurement techniques. The name of an instrument and the par amount of a transaction do not provide a quantitative measure of inherent credit risk. Credit analysts and portfolio managers alike must track the credit features on both a transactional and portfolio basis in order to aggregate and control the various levels of credit exposure to any one obligor, counterparty, insurer, and/or guarantor.

In order for corporates to properly ensure policies and regulations governing credit risk are adhered to, quantitative measures of exposure must be established, measured, monitored, and enforced. Prudent practice dictates this process must be as independent from the personnel initiating the investment transactions as practical.

Reporting and Documentation

The reporting of credit risk exposures and the supporting documentation (for approvals and monitoring) are key elements of credit risk management. The board, senior management, and other oversight authorities depend upon the quality of reporting to make determinations about the magnitude, compliance, and appropriateness of credit risk exposure. Management and the board cannot fulfill their respective control and oversight responsibilities absent meaningful risk reporting.

The more clear and valid the documentation, the more timely board and senior management can assess the risk and make strategic decisions. The methodologies for measuring credit risk and the formats for reporting credit risk information should be clearly documented in policies and procedures.

Personnel reporting lines are also important. The credit analyst is responsible for tracking the exposures of the corporate, monitoring limits, and reacting to changes in creditworthiness. Senior management is responsible for managing the overall risk posture of the institution; this includes management of aggregate risk exposures. The ALCO and board of directors have a fiduciary responsibility to be aware of the risk assumed by management and be assured management is actively managing the risk.

The corporate should have strong internal control procedures that ensure the integrity of credit risk information. The extent of automated information and the ability of an analyst to maintain current evaluations are other factors that may affect the quality of credit risk information.

<u>Reacting to Change</u>

One of the reasons a corporate should develop its methodologies for measuring credit risk exposures and setting consistent risk-based limits is to engender a risk management culture that appropriately reacts to change. In order for corporates to best manage credit risk exposure, management should be predisposed to take rational and timely steps towards rebalancing or reducing credit risk in the portfolio as needed. To this end, the chief risk officer and/or credit analysts should have delegated authority to take action to reduce credit exposure as deemed necessary.

Credit downgrades result in volatility in instruments" value and liquidity. Management must be able and willing to take corrective action when adverse developments occur. To provide this flexibility, most corporates classify large portions of their securities portfolios as available-for-sale (AFS). Other than divestiture, there are few alternatives available to mitigate deterioration in credit quality once it becomes known to the market. Corporates with Part IV authority, where specifically authorized may utilize credit derivatives to mitigate risks. However, this may be cost prohibitive if the market has already recognized the credit deterioration.

Administration

Minimum regulatory limits on permissible investments (permissible to buy or hold as collateral) are restricted to those with high credit quality. A number of these transactions have high credit ratings only because they are supported by collateral or other credit enhancements.

In some cases, the counterparty risk would not be acceptable without added credit enhancement. This means managers must closely evaluate and monitor the aspects of the transaction that provide the credit support. Typical credit enhancements such as collateral, performance margin, or a third-party guarantee are features that should be monitored as part of standard operating procedures. An ongoing review of these enhancements is necessary to identify, measure, monitor and control credit risk.

Collateral administration involves checking the market value, legality and control (perfected security interest) of securities accepted as collateral in investment and borrowing transactions. The integrity of the credit risk measurement process rests, in part, on determining the mark-to-market value of collateral and repurchase securities.

Securities accepted in a repurchase or securities lending transaction should be independently valued by the corporate or an agent separate from the counterparty. Collateral should be checked on an ongoing basis to confirm it meets policy and repurchase agreement requirements. (Note: This could be required as often as daily depending on agreements and degree of risk to the portfolio.)

Additionally, monitoring of securities that have inherent credit enhancements is important. For example, surveillance of the underlying receivables on MBS and ABS investments is the responsibility of the credit risk management function. Credit personnel should not view collateral or other structural enhancements as an excuse to ignore the amount of inherent credit risk in a transaction. Despite the fact credit enhancements increase the potential for a higher rate of collection in an event of default, it also requires more sophisticated measurement and monitoring processes.

An increasingly diverse array of methods are available to enhance credit quality. Credit managers must actively track these enhancements across the entire portfolio and regularly monitor the amount of exposure to ensure the credit risk policies of the board are followed.

Investment Products and Practices

Section 704.5(c) outlines various investment activities in which corporates may engage. Those investments must be U.S. dollar denominated and subject to the credit policy restrictions set forth in Section 704.6.

In a quality oriented investment culture, investment managers typically view the portfolio selection process as one of exclusion and rejection rather than search and acceptance. These investment managers realize the penalty for mistakenly rejecting an investment offering probably would not be significant. However, the acceptance of an unsound investment risk could be costly and possibly devastating.

Investment managers with quality oriented investment cultures typically have programs for obtaining and evaluating current information on potential/existing securities in their investment portfolios. Also, these managers only purchase securities from reputable and financially secure dealers.

Table 7: Minimum Credit Ratings at Time of Purchase

Type Investment[1]	Base & Base Plus		Part I		Part II	
	Short	Long	Short	Long	Short	Long
Investments with Long-Term Ratings		AA-		A-		BBB (flat)
Investments with Short-Term Ratings	A-1		A-2		A-2*	

[1] Assets must be 704-permissible.

*Provided that the issuer has a long-term rating no lower than BBB (flat) (or equivalent) or the investment is a domestically issued asset-backed security.

Authorized investment activities are listed in Part 704. Allowable investment products are discussed in reference 11, Comptroller of the Currency"s Examiner"s Guide to Investment Products and Practices.

Financial Derivatives (Expanded Authority)

Financial Derivatives are broadly defined as instruments that derive their value from the performance of underlying assets, interest or currency exchange rates, or indices.

Since managing financial risks (e.g., market, liquidity, credit, etc.) has become more important to corporates due to the advent of more sophisticated investment products, the use of off-balance sheet products will continue to grow. This section outlines some commonly known off-balance sheet derivative products.

Options

The owner of an option contract has the right to buy or sell a specific asset, at a specific price, on or before a specified date. The party granting the right is referred to as the option seller, or writer, and the party receiving the option is called the option buyer or holder. The seller is obligated to perform on the contract, whereas the purchaser has a right, but not an obligation, to perform on the contract.

A call option gives the buyer the right to purchase the underlying instrument. A put option gives the buyer the right to sell the underlying instrument. Purchasing an option is considered a long position, since the buyer holds the right to exercise. The seller of an option holds a short option position, since the right to exercise has been sold. (See Table 8)

The purchaser of a call option expects to profit from the price of the underlying instrument exceeding the strike price, or exercise price, within the life of the contract. The purchase of a put option expects to profit from the price of the underlying instrument declining below the exercise price of the contract just as the short-seller of the underlying benefits from a price decline. The exercise price (or strike price) is the price at which the contract owner has the right to buy or sell the underlying instrument.

Table 8

	Buyer/ Purchaser	Seller/ Writer
CALL	Long Call = Long exposure to the underlying security	Short Call = Short exposure to the underlying security
PUT	Long Put = Short exposure to underlying security	Short Put = Long exposure to the underlying security

Swaps

A swap generally is a contract between two counterparties to exchange net cash flows on agreed upon dates, for a specific period of time, on an established notional principal. The payment to one or the other counterparty is the difference between the two cash flows. The contracts are generally entered into by a swap dealer and a customer (corporate), rather than two customers. However, since these are over-the-counter transactions, two counterparties could enter into a swap agreement without going through a broker/dealer.

Although swaps are over-the-counter instruments (not traded on the organized exchange), there is a degree of standardization in the contracts since the advent of the International Swap and Derivatives Association (ISDA). The master swap agreement establishes the basic language governing all swap transactions between the two counterparties. However, counterparties may change the master agreement as needed. The standard ISDA agreement may be customized to some degree by attached schedules and credit annexes.

The most common type of swap used by corporates is the interest-rate swap. This swap can be broken down into two categories: coupon swap and basis swap. A coupon swap exchanges an interest payment stream of one configuration for another on the same notional principal (e.g., fixed rate for floating rate). A basis swap figures payments on two floating rate indices (e.g., LIBOR for Prime). An interest-rate swap also can be used to lower the corporate‟s cost of funds by taking advantage of the credit spreads between the fixed and floating rate markets. While it may reduce interest rate risk, a measure of credit and liquidity risk is introduced (it‟s not likely to be a riskless transaction). The credit risk in a swap transaction centers on the counterparty receiving the net payment.

Futures

A futures contract is an obligation to deliver or receive a specified amount of a commodity or financial instrument at a specified price on a specific date in the future. No cash is passed between the buyer and seller at the inception of the contract. Also, futures contracts rarely settle by actual delivery of the underlying; instead, they are offset or cash settled.

Futures contracts are traded on several exchanges in the U.S. and abroad and are available on financial instruments such as government securities and Eurodollar time deposits. The typical use of a futures contract is to hedge the risk of a particular security, portfolio of securities, or as an asset/liability tool to hedge overall balance sheet exposure. Since futures are exchange traded, the credit risk concern is failure of the exchange, not an individual counterparty. The exchange guarantees the settlement of the contracts. To protect itself, the exchange requires participants keep a margin account that may be called in the event a counterparty fails to perform.

Forwards

A forward contract is a customized obligation to receive or deliver a specified amount of a commodity or security, at a specified price, on a specific date in the future. The terms of the contract are negotiated directly by the counterparties and can be terminated only with the consent of both parties. The contract is sold or bought immediately, but not paid until some future date. This feature, along with the lack of an exchange acting as an intermediary, gives forward contracts credit risk which is not evident in futures contracts.

The most common types of forwards are interest rate forwards and forward rate agreements (FRAs). These are contracts to pay or receive a specified interest rate, at a specified date in the future. An FRA is a single period interest rate swap.

Financial derivatives are discussed in greater detail in Chapter 202, Appendix B, entitled "Derivative Instruments."

Investment and Risk Management Reporting

An accurate, informative, and timely management information system is essential. Examiners should evaluate the adequacy of a corporate‟s monitoring and reporting of risks, returns, and overall performance of investment and derivative activities to senior management and the board of directors.

Investment reports are typically an integral part of the ALM reporting process since investments represent the majority of a corporate‟s assets.

The frequency of reporting should provide responsible individuals with adequate information to judge the changing nature of the corporate‟s risk profile, and to evaluate compliance with stated policy objectives and restraints.

A clear, concise executive summary format is the best means for communicating complex information in a compressed time setting. Management reports should translate measured risk from technical and quantitative formats to those that can be easily read and understood by senior managers and directors.

The corporate should have a common conceptual framework for measuring and limiting risks in reports to senior managers and directors. These reports should concisely assess and report the performance of investments and portfolios in meeting the corporate‟s stated objectives.

Security Safekeeping

Listed below are the assignment programs currently in use by corporate credit unions. These programs periodically change. Therefore, the list should not be considered all-inclusive.

The Security Safekeeping Program (SSP):

1. Provides safekeeping services to participating credit unions holding United States Government and Federal Agency Securities.

2. Covers traditional custodial services such as monthly safekeeping reports, coupon and principal collection, and other maintenance services.

Security Liquidity Program (SLP):

Provides participating credit unions a line of credit in an amount, which approximates the market value of eligible securities available to the program.

The Reverse Repurchase Transactions (RRT) Program:

1. Involves a reverse repurchase transaction which represents the sale of a security for a "price" with a simultaneous commitment by the seller to repurchase the security at a future date at a specified "price."

2. Invests the interest earned from the proceeds in a corporate or certificate account of equal amount and maturity.

3. Requires Generally Accepted Accounting Principles (GAAP) presentation of income and expense transactions at gross amounts (netting is not permitted).

The Collateral Investments (CI) Program:

1. Allows credit unions to secure their investments in the corporate with United States Government and Federal Agency Securities.

2. "Sells" securities to the investing credit union via a repurchase transaction.

Security Safekeeping Policy: The corporate's investment policy should explicitly detail all authorized methods for safekeeping securities in-house or with other institutions. Safekeeping controls should be strengthened by the presence of specific procedures which have been designed and implemented to ensure adequate separation of duties and controls. Access control limitations should be similar to systems employed in the wire transfers area.

Safekeeping policies and procedures should be written with risk assessment in mind. "Prevention control" rather than "discovery" should be the underlying theme and objective.

Security Safekeeping Environment: Corporates safekeep their own investments, as well as those of member credit unions, through various service programs.

The "liability limitations" specified in the safekeeping contract and the qualifications of the safekeeping institution (such as its safekeeping experience, financial strength, and internal control strength) are key elements considered when assessing a safekeeping arrangement. Corporates typically safekeep investments through U.S. Central Federal Credit Union (U.S. Central). However, they often have other arrangements with banks, other safekeeping facilities, or the Federal Reserve. While assessing the internal controls of the safekeeping institution is important, evaluating the corporate‟s assessment of its safekeeping institutions is equally as critical. The impact of an unauthorized security transfer could be similar to that of an unauthorized wire transfer by exposing the corporate to financial and credibility losses. The examiner should ensure compliance with Part 703, NCUA Rules and Regulations.

Internal Risk: Corporates typically attempt to minimize their risk by acting as a "pass through" to outside safekeeping institutions. Contracts, bailment for hire agreements, and procedures for member credit unions are often utilized to control the risk of potential legal liability or loss from a breach of security occurring outside the corporate's walls.

Securities held in street name are more easily transferred and converted to cash. Controls surrounding access to these securities need to be functionally equivalent to wire transfers. Similar to cash, many investments can be transferred using wire transfers or through correspondent banking arrangements.

Other Programs

In addition to corporate network developed programs, the examiner may encounter "non-network" developed programs. Such programs may be developed in-house, by other corporates, or other outside financial entities.

Separation of Duties: Written procedures should describe the securities transfer process and individual responsibilities. Segregation of duties in the movement of securities is a key internal control element. Examiners should ensure adequate segregation of duties is in place over the transfer of corporate and member securities.

The majority of security transfers are affected via U.S. Central. The controls over this system should be reviewed to ensure they are adequate to prevent unauthorized transfers. Like the Federal Reserve‟s system, requests for securities movement are initiated by electronic means. Access to the U.S. Central system and its input/ transfer screen (DCHT) is password controlled. The examiner should determine that the verification function is not disabled.

A corporate utilizing security safekeeping systems should perform ongoing reconciliations (routine and random) throughout the day.

Account Reconciliation: At any time during the day, the corporate should have the ability to identify and document the location of its securities (as well as those of its participating members). The corporate should have the capability of reconciling its position (i.e., inventory/activity, including updated input from the custodian) at any point during the day. Safekeeping policies and procedures should require a reconciliation of the safekeeping account be performed daily and all securities in safekeeping (both corporate and member) be reconciled at least monthly to a master data base.

Re-establishment of Controls: The potential risk associated with the lack of control in the safekeeping process is material and immediate. The priority of establishing or reestablishing control of this area must also be immediate.

Summary

The growth and complexity of investment and financial products continually change the risk characteristics within the corporate credit union system. As a result, examiners and credit union personnel must have a thorough understanding and knowledge of the risks within a corporate‟s investment portfolio. To meet this objective, corporates must have a sound investment portfolio management process in place. This process must include, but not be limited to, sound investment policies and procedures to guide the process, strong management information systems for measuring, monitoring and reporting risk, adequately trained staff, and an independent testing of the overall process for compliance.

Examination Objectives

Investment Review Objectives:

1. Determine if policies, procedures, practices, and internal controls are appropriate for the corporate‟s level of operating authority and practices.

2. Assess the level of competency/qualifications of staff/management in relation to the level of complexity of the securities purchased.

3. Determine if corporate staff is operating according to established policies and procedures.

4. Determine the scope and adequacy of the internal and external audit functions.

5. Determine the overall quality and appropriateness of the investment portfolio and how it affects the soundness of the corporate.

6. Determine if the corporate is in compliance with applicable laws and regulations.

7. Determine if investments are properly recorded and classified.

8. Initiate corrective action when policies, procedures, practices, and internal controls are deficient, the investment portfolio represents an unacceptable risk to the corporate and/or the National Credit Union Share Insurance Fund, or when violations of laws and/or regulations have been noted.

Examination Procedures

See Corporate Examination Procedures - Investments (OCCU 201P and 201.1P).

Examination Questionnaire

See Corporate Examination Questionnaire - Investments (OCCU 201Q and 201.1Q).

References

1. NCUA Rules and Regulations

2. FFIEC Supervisory Policy Statement on Investment Securities and End-User Derivatives Activities (1997 Statement)

3. Controller"s Handbook on Risk Management of Financial Derivatives

4. Commercial Bank Examination Guide

5. Office of Thrift Supervision Regulatory Handbook

6. The Dictionary of Financial Risk Management, Gary L. Gastineau and Mark P. Kritzman, Frank J. Fabozzi Associates, 1996

7. The Encyclopedia of Banking & Finance, Tenth Edition, Charles J. Woelfel, Irwin Professional Publishing, 1994

8. "Standard & Poor"s Corporate Ratings Criteria", Standard and Poor"s, The McGraw Hill Companies, N.Y., New York. 1996

9. Duff & Phelps

10. NCUA Interpretive Ruling and Policy Statement (IRPS) 98-2

11. Comptroller of the Currency"s Handbook: Investment Securities

DERIVATIVES

Introduction

Appendix B to Part 704 authorizes corporates which apply for and receive Part IV Expanded Authority to engage in derivative activities.

A derivative is a financial contract with cash-flows based on the value or level of an underlying asset, index, or reference rate. The most common derivatives are swaps, futures, forwards, and options.

The market for derivative instruments has grown rapidly since the 1980's, reflecting a broad range of applications for these products as well as their wide acceptance by financial institutions, institutional investors, and corporate treasurers.

Derivative products are used primarily to manage and control risk. Corporates should use derivatives only consistent with authorities granted under Part IV. The most common use of derivatives by corporates is to structure share products for their members.

Types of Derivative Instruments

Derivatives can be divided into two distinct groups (a) forward-based products and (b) option-based products. Forward-based products include futures, forward transactions, and swap products. Option-based products include puts, calls, caps, floors, collars, and swaptions. Some derivatives are traded on organized exchanges, while others are traded in the over-the-counter markets.

"Exchange-traded" derivatives are standardized contracts traded on the futures and options exchanges. Each exchange operates a corporation known as a "clearinghouse" through which all contracts are reconciled, guaranteed, and settled. The clearinghouse places itself between the buyer and seller of each contract, making itself the counterparty to each contract.

"Over-the-counter" (OTC) contracts, on the other hand, are agreements entered into through private negotiations. Parties seek each other out and negotiate a trade. A number of large securities firms and commercial banks "make a market" in derivatives and are known as "derivatives dealers." Swaps, forward agreements, options, caps, and floors are actively traded in the OTC market.

Interest Rate Swaps

An interest rate swap is an agreement between two parties to exchange a series of cash flows at specified intervals known as payment or settlement dates. The cash flows, or interest payment streams, are based on notional principal amounts. No actual principal amounts are exchanged. Interim payments are usually netted, with the net amount being paid to one party or the other.

Interest rate swaps are used primarily to manage interest-rate exposure and to lower debt financing costs. Swaps provide a means to transform an existing cash flow stream into a more desirable cash flow stream. For example, a swap can be used to transform floating rate liabilities into fixed rate liabilities. Because swaps are negotiated agreements, virtually any kind of payment stream can be swapped. The most common type of swap is the "fixed/floating" interest rate swap described below.

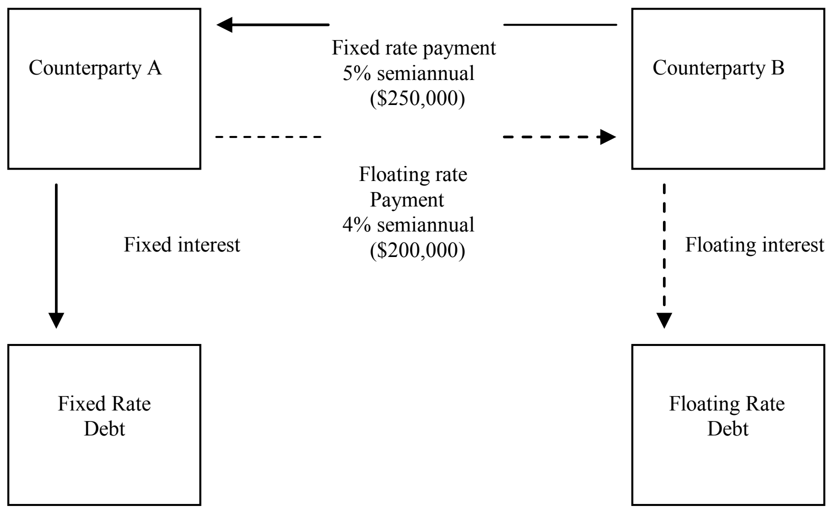
Fixed/Floating Interest Rate Swap

A fixed-for-floating interest rate swap is a swap in which a fixed interest payment stream is exchanged for a floating rate payment stream. The party that agrees to make fixed rate payments is known as the "fixed rate payer," and the party that makes the floating rate payments is known as the "floating rate payer." In effect, a fixed-for-floating swap enables the fixed rate payer to transform floating rate instruments into fixed rate instruments.

A basic example of a fixed-for-floating swap is shown in Figure 1. In the example, Counterparty A has \$10 million of fixed rate borrowings it wants to convert into floating rate borrowings, and Counterparty B has \$10 million of floating rate borrowings it wants to convert into fixed rate borrowings. Both parties agree to enter into an interest rate swap with a notional amount of \$10 million. The agreement requires Counterparty B to make semiannual payments to Counterparty A at a fixed rate of 5 percent for three years. In exchange, Counterparty A agrees to make floating rate payments based on the six month London Interbank Offered Rate (LIBOR) with an initial rate of 4 percent.

Counterparty B (the fixed rate payer) will make a net payment of \$50,000 to Counterparty A on the first semiannual payment date. On that date, the floating rate for the next six months is reset based on the prevailing six month LIBOR. If LIBOR increases after the swap is initiated, Counterparty A's cost of funds will rise since it is obligated to make floating rate payments to Counterparty B. Counterparty B, on the other hand, will benefit if rates rise, since it will receive higher floating rate payments while its payments remain fixed at 5 percent of the notional amount. Corporates exposed to rising rates can reduce their exposure by entering into a fixed-for-floating swap as the fixed rate payer.

Figure 1
Fixed-to-Floating Interest Rate Swap



* Floating rate payment is reset semiannually based on six-month LIBOR.

Basis Swaps

Basis swaps are swaps where each side of the swap is based on a different floating rate index (e.g., one month LIBOR against one month Average Federal Funds effective). Basis swaps are also known as "floating-to-floating swaps."

A "yield curve swap" is a type of basis swap. In a yield curve swap, the interest rate for each side is indexed to a different maturity point of the yield curve for a particular security, but one leg of the swap is tied to a long-term rate. For example, a yield curve swap may have the 10 year Treasury note yield as the index for one side and the three month Treasury bill yield as the index for the other side. The value will change in response to changes in the shape of the yield curve between payment dates. For example, if the short end of the yield curve increases (decreases) relative to the long end, the value of the swap will increase (decrease) to the counterparty that receives the three month Treasury rate.

Another common basis swap is a "COFI/LIBOR swap." Cost of Funds Index (COFI) represents the weighted average cost of funds at the savings institutions in the Eleventh District of the Federal Home Loan Bank System. Some institutions that offer adjustable rate mortgages (ARMs) indexed to COFI use COFI/LIBOR swaps to hedge their COFI-based ARMs. An institution that enters into a swap to pay COFI and receive LIBOR will convert the ARM portfolio from a COFI-based index to a LIBOR-based index. As long as movements of the LIBOR index closely match movements in the institution's actual cost of funds, the swap should lower the institution's interest rate risk exposure.

Swap Termination

A corporate that has entered into a swap may wish to reverse or terminate the swap prior to maturity. There are two ways to unwind a swap position. One way is to negotiate a termination settlement with the original counterparty. The other is to enter into a new swap that is a mirror image of the existing swap to offset the existing position.

Swap Variations

Most swaps have a specified maturity date and a fixed notional amount. Some swaps, however, have notional amounts that amortize over time. These are commonly called index amortizing swaps because the notional value declines based on a prepayment index (i.e. Fannie Mae 30 Year Fixed). Swaps can also be callable, in which case the swap can be terminated at the option of the corporate if interest rates increase or decrease beyond the "strike rate." A "swaption" is an option to enter into a swap at a future date. A "forward swap" is a firm commitment to enter into a swap at a specified future date.

Accounting

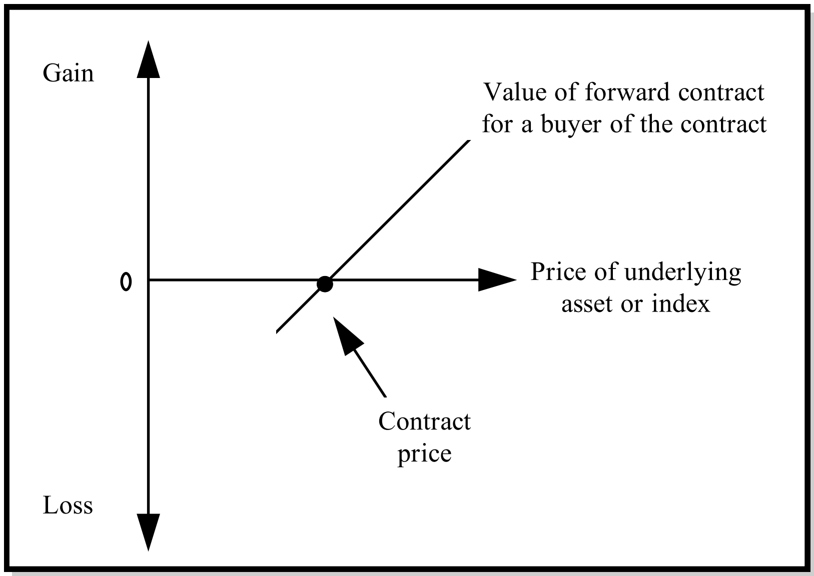
Interest rate swaps are recorded using hedge accounting if the institution can demonstrate that the swap reduces exposure to interest rate or cash flow risk. See, Statement of Financial Accounting Standard No. 133. Since a swap typically has no initial market or book value on the transaction date, only the accrual of periodic net interest cash flows typically will flow through the income statement for highly effective hedges. If a swap is terminated prior to maturity, the gain or loss must be amortized over the remaining life of the swap. Swap positions that are not highly effective at reducing interest rate or cash flow risk must be marked-to-market, to the extent of ineffectiveness. Market value changes in the affected swaps will also flow through the financial statements. Examiners should analyze the characteristics and terms of each swap to determine whether the swap is being used to reduce risk.

Forward Contracts

A forward contract obligates one counterparty to buy, and the other to sell, a specific underlying financial instrument at a specific price, amount, and date in the future. Contracts specifying settlement in excess of the cash market practice for spot settlement are considered to be forward contracts. (Spot settlement for mortgages, for example, are once a month.) Forward contracts exist for a multitude of "underlyings," including currencies, commodities, and mortgages. Forward contracts are traded over-the-counter and are customized to fit the particular objectives of the counterparties.

Figure 2 shows the payoff profile of a forward contract. As shown, the change in the value of a forward contract is roughly proportional to the change in the value of the underlying asset or index. The value of the contract is conveyed at maturity through cash settlement or delivery. If the price of the underlying (asset or index) is higher than the contract price, then the buyer makes a profit. The gain to the buyer equals the loss to the seller.

Figure 2
Value of Forward Contract -- Long Position

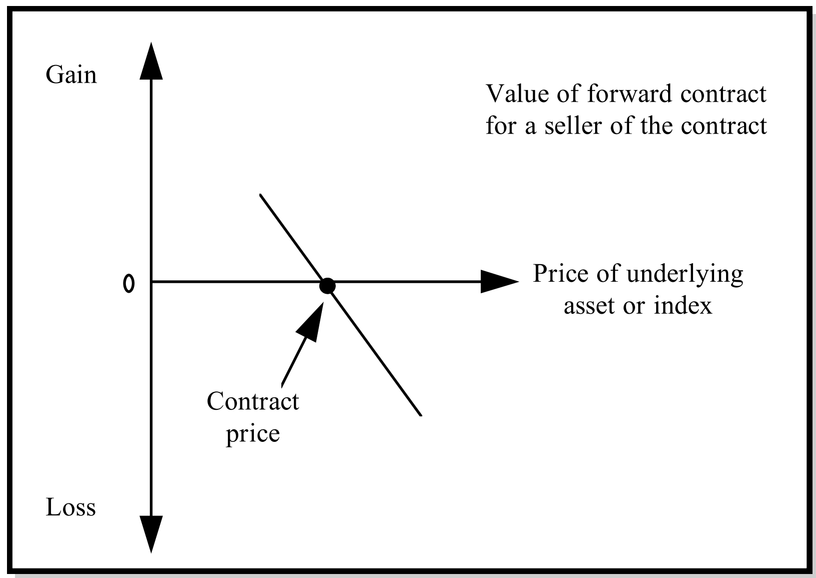


Forward contracts create two-way credit risk. The counterparty on the side of the contract that has a positive replacement value is exposed to credit risk of the other party. However, the market value of a contract can swing from a positive value to a negative value and vice versa. Therefore, each party must assess the creditworthiness of its counterparty since each side is exposed to a potential gain or loss. The value of the forward contract is conveyed on the maturity date of the contract. No payments are made at origination or during the life of the contract. The contract owner will either receive or make a payment at maturity depending on the price movement of the underlying asset or index.

Forward contracts are often used by mortgage bankers to hedge their operations. Institutions that originate mortgage loans for sale into the secondary market usually hedge the price risk of holding loans temporarily by arranging forward contracts to sell their loans. The forward sale of mortgage loans transfers the price risk of holding the mortgages in the "pipeline" to the counterparty. The payoff profile of a forward sale is shown in Figure 3. The seller of the forward contract is "short the underlying" and, therefore, gains if the value of the underlying asset declines.

Forward contracts to sell mortgage production can be "firm" or optional commitments. Firm commitments require both parties to perform on the contract (delivery of mortgages or cash settlement), regardless of market conditions. In contrast, optional commitments, such as “standbys,” require performance only at the option of the party that purchased the option.

Figure 3
Value of Forward Contract -- Short Position



Institutions typically attempt to match the terms of the forward agreement to the terms of the item giving rise to the risk exposure. For example, assume an institution originates 30 year fixed rate mortgages and expects to close most loans within a 45 day period. As loan production accumulates, the institution enters into a firm forward commitment to sell 30 year loans with a settlement date 45 days in the future. For the portion of the pipeline that is uncertain as to closure, a standby agreement may be used to hedge the market risk.

In general, forward contracts to buy mortgages or MBS (i.e., the “long position”) will increase the overall interest rate risk exposure of a typical corporate. Examiners should scrutinize long forward positions to determine if they are being used for speculative purposes.

Examiners also should look for “pair offs,” in which forward positions are closed out prior to settlement with offsetting forward contracts, usually at a profit. Pair off activity is considered presumptive of speculative intent.

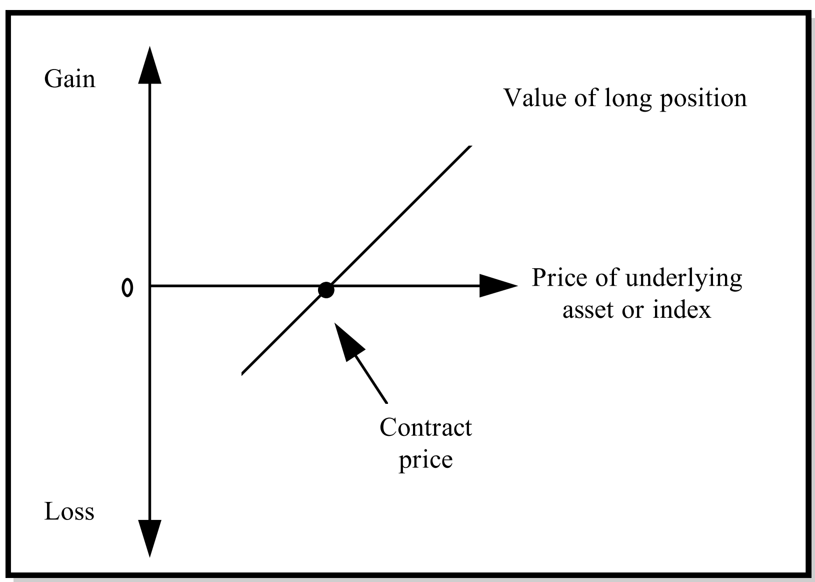
Futures Contracts

A futures contract is a legally binding agreement to make or take delivery of a standardized quantity and quality of a commodity or financial instrument on a specified date in the future. The value of a futures contract responds to changes in the price of the underlying commodity or financial instrument in much the same manner as the value of forward contracts. Futures contracts are traded on recognized exchanges, and the exchange clearinghouse is the counterparty to each trade.

Futures contracts based on a financial instrument or a financial index are known as financial futures. Financial futures include interest rate futures, stock futures, and currency futures.

Financial futures can be an effective means of controlling interest rate risk. The most commonly used interest rate futures are those with Treasury bills, notes, and bonds, as well as Eurodollar time deposits as the underlying.

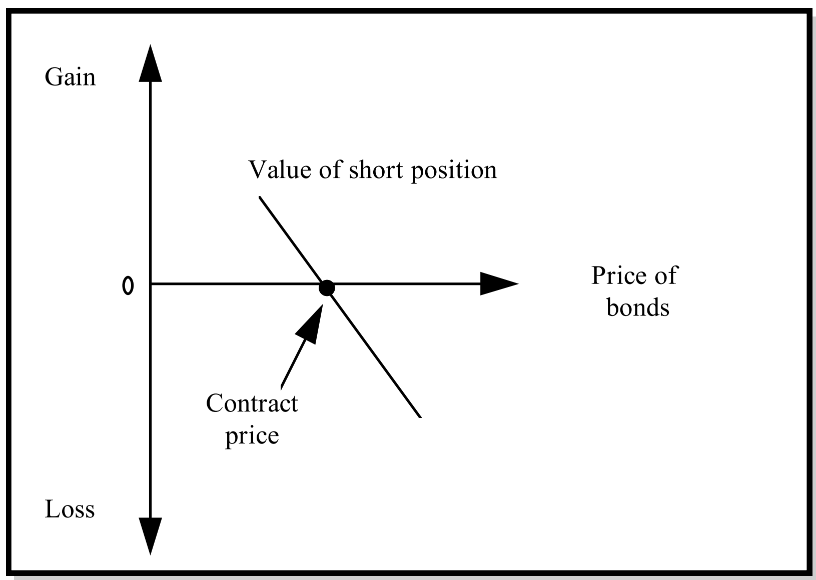
Figure 4
Value of Futures Contract -- Long Position



The buyer of a futures contract takes a "long position" in the market and is said to be "long the futures." The contract can be sold at any time before settlement. In the case of an interest rate futures contract, such as a Treasury bond contract, a long position will profit if interest rates decline. Lower interest rates mean higher contract prices because interest rates and bond prices are inversely related. Conversely, an increase in rates will produce a loss on the long position. For the payoff profile of a long futures contract, see Figure 4. Note, futures contracts obligate their owners to purchase a specified asset at a specified exercise price on a specified maturity date.

A seller of a futures contract takes a short position in the market. In essence, sellers promise to deliver a commodity or financial asset even though they may not own the asset. A short position in a Treasury bond contract will profit if Treasury bond prices decline (i.e., if Treasury bond interest rates increase). Selling a futures contract (a short position) is an example of a hedging strategy that can be used to reduce the interest rate risk exposure of an institution that loses value when interest rates rise. The payoff profile of a short futures position in Treasury bonds is shown in Figure 5.

Figure 5
Value of Treasury Bond Futures Contract -- Short Position



Compared with swaps and forwards, the credit risk of futures contracts is minimal for three reasons. First, futures contracts are "marked-to-market" daily and any change in the value of the futures contract is conveyed, or "cash settled," at the end of each day. (In contrast, the value of a forward contract is conveyed in a single payment at maturity. With a swap contract, changes in value are conveyed periodically throughout the life of the swap on each settlement date.) Second, buyers and sellers of futures contracts are required to post a performance bond, which is known as the "margin," with their brokers. The initial margin account is established when the contract is opened, and gains and losses on the futures contract are added to or subtracted from the margin account at the end of each day. If losses cause the margin account to fall below a specified level, the customer is required to post additional margin or the account will be closed out. And third, an exchange clearinghouse is the counterparty to each futures transaction and guarantees settlement of the transactions.

Examiners should review any deferred gains or losses related to futures activity. The related accounting documentation must demonstrate a highly effective hedge has been achieved to justify hedge accounting.

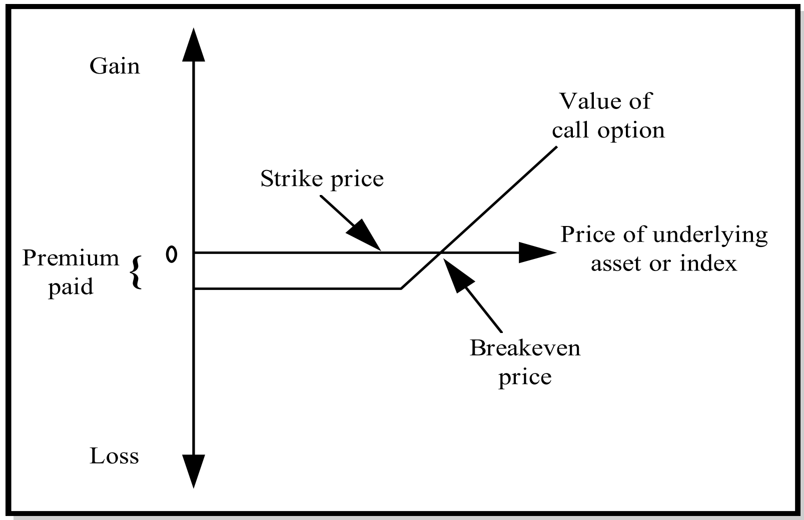
Options

An option gives the holder the right, but not the obligation, to buy or sell a designated asset or instrument at a specified price, called the "strike price," during a given period of time or on a specific date. The writer (or seller) of the option grants this right to the buyer in exchange for a sum of money that is referred to as the "option premium," or the option price. An "American option" may be exercised at any time during the life of the contract. A "European option" may only be exercised on the expiration date. Option contracts are traded on exchanges and in OTC markets.

The buyer of any option is said to hold the "long position" and the seller (writer), the "short position." When the underlying asset is owned by the writer of the option, the position is "covered." When the writer does not own the underlying asset, the writer's position is said to be "naked."

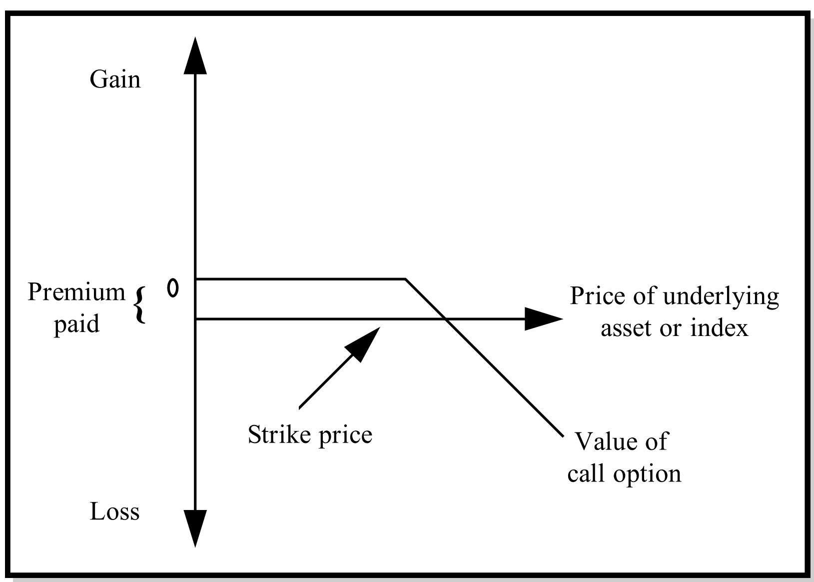
A "call option" gives the buyer (the long position) the right to buy the underlying asset at a predetermined strike price for a specified period of time. The buyer of a call option benefits if the price of the underlying asset rises above the strike price by an amount sufficient to cover the option premium. If the option is not exercised before expiration, the option will expire worthless. The profit potential of the long call position is substantial, while maximum loss on the option is limited to the option premium. The payoff profile of a long call position is shown in Figure 6.

Figure 6
Value of Call Option -- Long Position



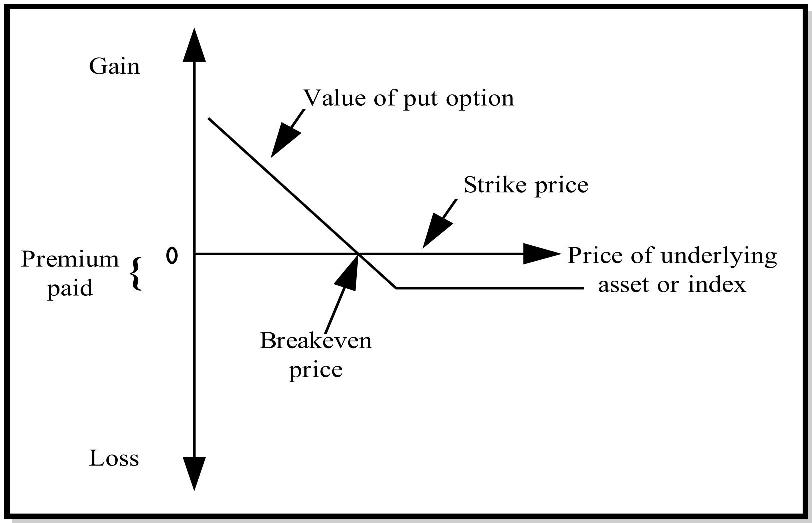
The payoff profile of the seller (the short position) is shown in Figure 7. Note, the profile of a short call option position is the opposite of a long call. Also, note the profit potential of the short call position is limited to the amount of the option premium, while the loss potential is substantial.

Figure 7
Value of Call Option -- Short Position



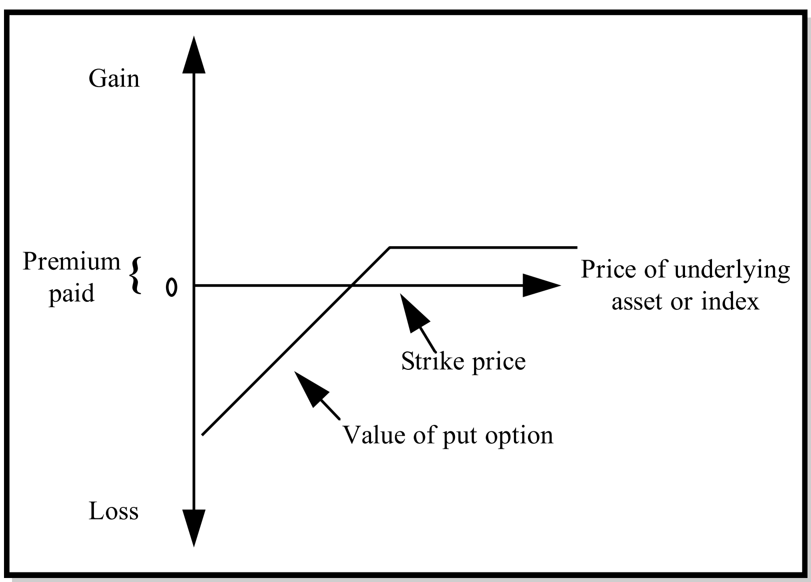
A "put option" gives the buyer (the long position) the right to sell a designated asset (or instrument) to the option writer at a specified price for a specified period of time. The buyer of a put option benefits if the price of the underlying declines sufficiently to cover the option premium. The payoff profile of a long put is shown in Figure 8.

Figure 8
Value of Put Option -- Long Position



The payoff profile of someone that is short a put option is shown in Figure 9. Just like a short call, the profit potential on a short put is limited to the premium received for writing the option, while the downside potential is substantial.

Figure 9
Value of Put Option -- Short Position



The value of an option is influenced by five factors:

1. strike price;
2. current price of the underlying instrument;
3. time to expiration of the contract;
4. expected volatility of yields (or prices) over the remaining life of the option; and
5. short-term risk free interest rate over the life of the option.

The premium of an option has two main components: intrinsic value and time value. The intrinsic value is the difference between the strike price and the price of the underlying security. Prior to expiration, any premium in excess of intrinsic value is called time value. Time value is also known as the amount an investor is willing to pay for an option above its intrinsic value, in the hope at some time prior to expiration its value will increase because of a favorable change in the price of the underlying security. The longer the amount of time for market conditions to work to an investor's benefit, the greater the time value.

Caps, Floors, and Collars

Interest rate caps, floors, and collars are customized interest rate options that can be used to manage interest-rate risk.

Cap - A “cap” is a contract that provides the buyer with protection against a rise in interest rates above some specified rate. An underlying interest rate index is specified in the contract. The most common index is LIBOR. The buyer pays a premium for the option. The contract will specify the notional amount of the contract, the maturity, the settlement frequency, the interest rate index, and the level of protection (i.e., the strike rate of the cap). A cap can be used to synthetically set a maximum rate on floating rate borrowings. If rates rise above the cap rate, the buyer will receive a payment that will offset the increase in interest expense on the floating rate borrowings above the cap rate. Thus, a cap can be used to fix the maximum rate a borrower would pay out on a floating rate obligation, while allowing the borrower to benefit from a decline in rates. (An institution can also sell a cap to generate income through receipt of a premium.)

Floor - A “floor” is a contract that provides the buyer with protection against declining interest rates. A commercial bank with a relatively large portfolio of floating rate loans might, for example, buy a floor to protect its net interest earnings against a decline in rates. For a premium, the buyer of a floor receives the difference between the strike rate (floor) and the actual rate on the index if the index falls below the floor. No payments exchange hands if the strike rate on a floor is greater than the current index rate. The seller of a floor receives a premium.

Collar - A "collar" is a combination of the purchase of a cap at one rate and the sale of a floor at another rate. The cap and floor rates are usually set so the cost of the cap equals the premium on the floor, resulting in a zero cost collar. For an institution exposed to rising rates, a collar provides protection if interest rates increase above the strike rate on the cap. In exchange for that protection, the institution gives up the benefits of lower funding costs if rates fall below the strike rate on the floor.

Swaptions

A "swaption" (or swap option) is an option on a swap. It gives the buyer the right, but not the obligation, to enter into a specified swap at a future date.

Standby Agreements

A standby agreement is a put option (agreement to sell at a specified price) on mortgages or mortgage-backed securities. They are usually used by mortgage bankers to offset the risk of loans that would be expected to close if interest rates increase, but are otherwise uncertain as to closure. An institution pays a fee to purchase this protection.

Short standby positions (short puts) involve the receipt of a fee for taking on the risk of having to purchase loans in an adverse environment. Short puts are usually speculative. They should be viewed by examiners as speculative unless an institution can demonstrate otherwise.

Risks of Derivatives

The use of derivative instruments can be highly beneficial but, as with other types of financial products, their use entails certain risks. The primary risks include credit risk, market risk, and operational risk.

Credit Risk

Credit risk is the risk a loss will occur if a counterparty defaults or otherwise fails to perform on a contract. The evaluation of credit risk is particularly important in the case of derivatives because the creditworthiness of counterparties can vary significantly. By comparison, counterparty risk on exchange-traded contracts is generally viewed as minimal because the exchanges guarantee the performance of each contract. In addition, credit exposures on exchange-traded options are minimized by margin requirements and daily settlement practices imposed by the exchanges.

The credit risk exposure of derivatives consists of two distinct elements: current exposure and potential exposure.

Current exposure is the market value of the derivative at any point in time. The market value (or replacement value) of a derivative is equal to the net present value of the derivative's future cash flows. It is the cost of replacing the contract with a new one if the counterparty defaults. The current exposure can be either positive or negative. When the current exposure is positive, the contract represents an asset and the holder of the contract will suffer a loss if the counterparty defaults. When the market value of the contract is negative, the contract represents a liability; therefore, no credit loss will occur in the event of default since the contract has no value. (The current exposure on exchange-traded contracts is negligible since exchanges require daily settlement of gains and losses on contracts.)

The potential exposure of a derivative contract is the potential mark-to-market exposure that could occur if market conditions move in an adverse way. Potential exposure is only an estimate because future market conditions cannot be known with certainty. Market participants use various statistical techniques, such as Mount Carlo simulation, to estimate potential exposures.

For an audit loss to occur on a swap, two conditions must exist. First, the market value of the contract must be positive, and second, the counterparty must default on the contract. The same is not true for options contracts. With options, a counterparty default can result in a loss to the buyer of the option, even if its mark-to-market value is zero, since the buyer pays a premium to the seller when the contract is initiated. Obviously, the premium would be lost if the counterparty went out of business and would not perform on the contract.

Collateral arrangements are often used in derivative transactions to reduce exposure to counterparty risk. In swap transactions, collateral arrangements are subject to negotiation and can be unilateral or bilateral. Under a unilateral arrangement only the weaker counterparty is required to post collateral, while under a bilateral arrangement no collateral is posted initially, but either side may be required to post collateral if a "triggering" event occurs, such as a credit downgrading or a sharp movement in rates.

Netting arrangements are also used to reduce risk when a party has two or more swap transactions with the same counterparty. Typical netting arrangements call for all transactions with the same counterparty to be "netted" in the event of default, that is, all contracts between the two parties are marked-to-market and those with negative values are offset against those with positive values.

If netting does not apply, no offsetting occurs in the event of default. As a result, a practice known as "cherry picking" may occur. For example, a firm may have two swaps with the same counterparty, one with a positive replacement value and one with a negative replacement value. If the firm enters bankruptcy it may attempt to seek relief from the swap that has a negative replacement value (a liability) and attempt to force the counterparty to continue to pay on the swap with a positive value.

Forward contracts to sell mortgage production can be "firm" or optional commitments. Firm commitments require both parties to perform on the contract (delivery of mortgages or cash settlement), regardless of market conditions. In contrast, optional commitments, such as "standbys," require performance only at the option of the party that purchased the option.

Market Risk

Market risk is the risk of loss on the value of the contract arising from changes in market conditions, including interest rates (interest rate risk), supply and demand factors (liquidity risk), and other factors that affect the price of the contract. Sources of market risk differ for different types of derivatives. It is important for end-users to understand the forces that cause the market prices of the derivatives they use to change so they can simulate the performance of the derivatives under different scenarios.

Operational Risk

Operational risk is the risk of losses occurring due to a failure of internal systems and controls, human error, or fraud.

Management Guidelines for Derivative Instruments

Corporates using derivative products should do so only in accordance with safe and sound practices. Levels of activity should be reasonably related to the corporate's needs and financial sophistication. Management should evaluate the appropriateness of using derivatives in the context of its total portfolio risk. Such evaluations should assess the effect of the derivatives on the corporate's earnings and net economic value (i.e., the net present value of assets, liabilities, and off-balance sheet items). A corporate should consider the liquidity and price volatility of derivative products prior to use. In general, the use of derivatives should be limited to transactions and strategies that lower or do not increase an institution's overall exposure to interest rate risk.

Corporates with Part IV Expanded Authority that use derivatives should adhere to the following guidelines:

Board of Directors' Approval

The board of directors should adopt, and vigorously enforce a written policy authorizing and governing the use of derivative products. The policy should (1) identify the authorized derivative instruments and (2) mandate recordkeeping systems sufficiently detailed to permit internal auditors to determine whether personnel have operated in accordance with the board's authorization.

Management should report periodically to the board regarding compliance with the board's policies on the use of derivative products.

Business Plan

Institutions are required to have a comprehensive business plan detailing their overall interest rate risk management and investment strategy. That plan should include a description of the institution's derivative strategies and objectives.

Internal Controls

An institution should establish internal controls and procedures that include periodic reports to management, segregation of duties, and a program to ensure adherence to internal policies and procedures as well as the prevention of unauthorized transactions and other abuses.

Segregation of Duties

Internal systems and procedures established to monitor derivative products should provide for segregation of duties among those responsible for execution, record-keeping, verification and confirmation of transactions. Management should designate who is authorized to commit the institution to derivatives transactions.

Position Limits

Management should establish specific position limits (expressed in terms of notional dollar amounts, or as a percentage of assets or capital) for each major type of derivative product. The limits should be consistent with the institution's intent, level of management expertise, the sophistication of its internal controls and monitoring systems, its asset/liability structure, and its capacity to maintain liquidity and absorb losses from capital. The board of directors, the asset/liability committee, or the internal auditors should review positions periodically to ascertain conformance with such limits. If the review is performed by the internal auditors, the auditors should report their findings to the board of directors or an appropriate committee of the board on a regular basis.

Aggregating Credit Exposures

Credit exposures on derivatives, and all other credit exposures to counterparty, should be aggregated taking into consideration enforceable netting arrangements. Credit exposures should be calculated regularly and compared to credit limits.

Sensitivity Analysis (Stress Testing)

Prior to using derivatives a sensitivity or simulation analysis that demonstrates the effect of the derivative on the institution's net economic value should be performed under various interest rate scenarios.

Depending on the nature and size of the transaction, the institution may wish to undertake a more comprehensive analysis to gain a better understanding of the expected performance under a wide range of interest rate scenarios. A more comprehensive analysis might, for example, include an evaluation of the effects of non-parallel shifts in the yield curve, cyclical changes in interest rates, and changes in the spread between key short-term interest rates. With respect to mortgage-related derivative products, the analysis might also show the effect on earnings and net portfolio value of holding prepayment speeds constant over a range of interest rates, and holding interest rates constant over a range of prepayment speeds.

Marking-to-Market

Corporates should mark their derivatives positions to market, on a regular basis, for risk management purposes, such as NEV reporting.

Professional Expertise

Corporates using derivatives must ensure their derivatives activities are undertaken by staff with the appropriate experience, skill levels, and degrees of specialization.

Institutions that retain investment advisors to assist in formulating portfolio strategies involving derivative products should not place undue reliance on, or delegate decision-making authority to, such advisors. Decisions made on the basis of recommendations of third parties should be documented.

Counterparty Credit Risk

To limit counterparty credit risk associated with over-the-counter derivative transactions, corporates should engage in transactions only with financially strong counterparties. Management should conduct a credit analysis of the counterparty prior to entering into a transaction. In addition, management should investigate the dealer's general reputation for fair and honest dealings with customers. Corporates should also conduct an inquiry of appropriate state or federal securities regulators and securities industry self-regulatory organizations concerning any formal enforcement actions against the dealer, its affiliates or associated personnel.

Corporates using derivatives should assess both the benefits and costs of credit enhancement and related risk reduction arrangements. Where it is proposed credit downgrades would trigger early termination or collateral requirements, a corporate should carefully consider its own capacity and that of its counterparties to meet the potentially substantial funding needs that might result.

Legal Review

Management should carefully review all contractual and account documents related to derivative transactions, to ascertain the rights and obligations of all parties to the transactions, including margin and collateralization requirements, and the recourse available to each party. Management should thoroughly understand those rights and obligations to avoid possible misunderstandings.

Master Agreements

Corporates using derivatives are encouraged to utilize one master agreement as widely as possible with each counterparty to document existing and future derivatives transactions, including options. Master agreements should provide for payments netting and close-out netting, using a full two-way payments approach. These agreements are standardized by the International Swaps and Derivatives Association and are know as ISDA agreements. A corporate should not engage in a derivatives transaction with a counterparty unless it has a properly executed ISDA agreement in place.

Accounting Treatment

Derivative transactions must be accounted for and disclosed in accordance with generally accepted accounting principles (GAAP). SFAS 133 governs derivatives accounting. Management should consult with its independent auditor to ensure compliance with GAAP. Where GAAP does not specifically address the accounting treatment for a particular derivative instrument, the accounting treatment employed by the institution should be documented, and recorded, including the basis for the adopted treatment.

Evaluation of Hedging Transactions

For hedging transactions, internal reports should show the market value of the derivative instruments and reconcile the gains and losses to the changes in the value of hedged balance sheet items. For example, if an institution purchased futures contracts to hedge the market value of a group of assets, the institution should compare the performance of the futures contracts in tandem with the performance of the hedged assets in order to evaluate the overall performance of a hedging program.

Examination Objectives

The objectives of the derivatives review are to:

1. Determine what derivatives activities are approved for use by the corporate.
2. Determine if policies, procedures, and strategic plans regarding the corporate's use of derivatives adequately address safety and soundness, earnings, and compliance with laws and regulations.
3. Determine if the corporate is in compliance with the provisions of its Part 704, Appendix B Part IV approved authorities.
4. Determine the corporate has retained staff qualified to engage in the approved derivatives transactions and they are operating within the corporate's policies.
5. Determine management has adequately analyzed its derivative instruments prior to executing transactions and assessed they are appropriate based on the corporate's portfolio, asset/liability structure, and capital position.
6. Determine if the corporate has appropriate accounting and risk management systems to monitor its derivative transactions.
7. Determine if internal management reports provide the necessary information for informed risk management decisions and for monitoring the results of those decisions.
8. Initiate corrective action when derivative policies, procedures, practices, and internal controls are deficient.

Examination Procedures

See Corporate Examination Procedures - Derivatives (OCCU 201.1P).

Examination Questionnaire

See Corporate Examination Questionnaire - Derivatives (OCCU 201.1Q).

References

1. NCUA Rules and Regulations (Section 704.8)
2. Regulatory Handbook, Thrift Activities (OTC) Volume II
3. Comptrollers Handbook, Interest Rate, Funds Management
   http://www.occ.gov/handbook/FundsMgt1.pdf
4. Comptrollers Handbook, Liquidity
   http://www.occ.gov/handbook/liquidity.pdf
5. Comptrollers Handbook, Risk Management of Financial Derivatives
   http://www.occ.gov/handbook/deriv.pdf

ASSET AND LIABILITY MANAGEMENT (ALM)

Introduction

Asset/Liability Management (ALM) is the process of managing the composition and pricing of a corporate credit union's (corporate's) assets, liabilities, and off-balance sheet instruments. It also encompasses controlling exposure to financial risk with the goal of maximizing the efficiency of capital over the long term. ALM, therefore, includes the processes by which an institution: (1) manages and prices its funds, (2) controls its exposure to financial risk, and (3) manages its net interest margin and net economic value.

ALM centralizes management oversight of the above functions to ensure the common goal of achieving the corporate's financial objectives. ALM recognizes no individual asset, liability, or off-balance sheet portfolio exists in a vacuum. Rather, ALM explicitly considers each portfolio to be a critical link in the integrated and dynamic process of balance sheet management, and an integral part of the corporate's overall risk/return profile.

The ALM process includes both the decision-making processes and analytical systems involved in managing a corporate's risk/return profile. The decision making process should be comprehensive, and should include the Asset/Liability Committee (ALCO), policies, procedures, and controls to support the ALM function. Analytical systems (i.e., asset/liability models) should provide for comprehensive, timely, and accurate analyses of an institution's global risk/return profile, as well as those of potential strategies.

In assessing an institution's ALM, the examiner's general focus should be to:

1. Ascertain whether the ALM decision-making framework (ALCO, policies, procedure, controls, etc.) is sufficient to guide the major financial functions (listed above).

2. Verify the analytical systems and instruments available to management are properly implemented and used appropriately in managing the institution's risk/return profile.

Setting Financial Goals: The Risk/Return Profile

A corporate's overall financial return objectives are generally stated in terms of earnings (net interest margin) or value (net economic value) maximization, within the constraints imposed by risks from external and internal factors. Risk is generally characterized as the variability of returns. The greater the risk embedded in individual assets, portfolios, or the overall institution, the greater may be the variability of returns over time.

Management is constantly faced with the fact that, at any given point in time, higher returns (earnings or value) are expected if the corporate takes on greater risk; this is the risk/return tradeoff. Whether to position for a higher expected return at the risk of greater variance in realized return is the issue that confronts the management of each of the financial functions overseen by ALM.

For example, when the Treasury yield curve is relatively steep, a corporate can enhance current and expected earnings by borrowing short-term funds and investing in longer term assets. However, rising yields will immediately reduce net economic value and result in reduced realized earnings over time (all other things being equal). If a corporate has derivative authority, it may choose to reduce its overall interest rate risk (IRR) exposure by synthetically extending its liability duration with a pay-fixed interest rate swap; in this case, the reduced risk will lower the expected return and the expected variance of returns.

This tradeoff between risk and return heightens the difficulty of consistently achieving overall financial goals. Short-term earnings targets may be met by accepting greater risk, but long-term earnings objectives may be compromised. As a result, a rational decision-making process for determining a corporate's optimal risk/return profile and analyzing the impact of numerous risk/return alternatives is crucial to successful financial management. This process is called the ALM decision making process.

ALM is therefore a process of optimization, in which the risk/return tradeoffs of potential strategies are analyzed, and only those that most efficiently support the achievement of the institution's overall financial objectives should be implemented.

Measures of Return

An institution's overall financial objectives with respect to return are usually stated in terms of earnings or market value maximization. In specifying these goals, a number of specific measurement gauges may be appropriate, either individually or in combination. These include both earnings-based and market value-based performance measures, as shown in Table 1.

Corporates traditionally specified financial objectives in terms of earnings-oriented performance measures. While earnings-oriented performance measures are still commonly used in the corporate credit union industry, market value-oriented measures are also viewed as critical indicators of corporate financial strength.

Table 1

Measures of Return Performance

A. Earnings-oriented measures
   1. Net interest margin
   2. Core income
   3. Net income
   4. Return on assets
   5. Return on equity

B. Market value-oriented measures
   1. Market capitalization
   2. Liquidation value
   3. Going-concern value
   4. Net economic value

C. Both--Total Return

Earnings-Based Measures

Net Interest Income (NII) - NII is interest income minus interest expense. NII is the primary source of income for a corporate and a key indicator of earnings performance and stability. This measure makes no adjustment for assets that earn no interest or liabilities that bear no explicit interest cost.

Net Interest Margin (NIM) - Net interest income is called NIM when expressed as an annualized percent of moving daily average net assets (DANA). A corporate can optimize its net interest margin by effectively allocating resources among earning and non-earning assets, maintaining low levels of non-performing assets, providing adequate liquidity funding, and maintaining a strong capital position. In a volatile interest rate environment, large changes in NIM may indicate a significant exposure to IRR and potential risk management concerns.

Core Income - Core income includes NII and fee-based income less operating expenses. It excludes non-recurring income and expense items so a measure of the institution's fundamental current earning power can be attained.

Net Income - Net income is still the performance measure most utilized by investors, even though it is one of the least meaningful. It is very short-term in focus and can be easily manipulated to generate the appearance of favorable earnings trends. For example, non-recurring gains can be recognized to inflate earnings or to mask the impact of negative underlying developments. Reliance on these gains will negatively affect future earnings (all other things being equal).

Return on Assets (ROA) - ROA is net income divided by average assets. To the extent the numerator is distorted by the shortcomings noted above, this measure should be used cautiously or adjusted to account for non-recurring items. As a ratio measure, the ROA is convenient for other comparative analysis, as is the return on equity measure (below).

Return on Equity (ROE) - ROE is net income divided by average equity. The usefulness of this measure is also dependent on the accuracy of the numerator. The ROE is widely used by institutional investors as the key measure of performance.

Market Value-Based Measures

The measures of return discussed so far are based on reported earnings (i.e., accounting data). In contrast, market value measures reflect economic value.

Market Capitalization - Market capitalization is equity shares outstanding times the price per share. Since corporates are mutual organizations, this measure is not applicable.

Net Economic Value (NEV) - NEV is equal to the difference between the market value of assets and liabilities, plus the termination value (mark-to-market value) of off-balance sheet instruments. The NEV may be computed under different assumptions. NEV represents, in effect, the present value of long-term earnings streams. By focusing on stabilizing its market value, a corporate will also stabilize its long-term earnings. For this reason, market value measures have gained acceptance in financial institutions.

The overriding management objective is the efficient use of capital. The more efficiently capital is employed by a corporate, the more value is added to members in terms of dividend rates, services and protection from adverse events. Optimization of NEV is a management goal that serves the members' demand for a satisfactory return on their investment (ownership in the corporate). Return on capital flows directly to the members in the form of dividends on shares and indirectly in the form of NEV increases and services (to the extent that they are offered at or below a member's alternative cost).

A corporate computes NEV using its own assumptions, models, and methodologies. The corporate examiner should review this process, particularly the assumptions, for reasonableness. NEV must be produced at least quarterly, and as frequently as monthly, depending on the level of expanded authorities and/or amount of unmatched embedded options in the balance sheet. NEV is measured for a base case as well as a series of permanent, instantaneous and parallel shifts of the Treasury yield curve. During times of extremely low interest rates, the required downward shock tests may be suspended per guidance from the Director of the Office of Corporate Credit Unions. This analysis of NEV sensitivity is an invaluable tool in the assessment of IRR exposure.

Liquidation Value - Liquidation value is the residual value that would remain if all assets, liabilities, and off-balance sheet instruments were sold, terminated, or offset today (or in the short term). Current market prices are used to value all assets, liabilities, and off-balance sheet instruments for which market prices are available. If prices are not readily available for certain items, then the value is computed based on a discounted cash flow analysis using current market factors.

Liquidation value is the "bottom line" to an insurance fund, such as the National Credit Union Share Insurance Fund (NCUSIF), because to the extent the proceeds from asset sales are not sufficient to cover the balance of deposits, the fund will experience losses.

Going Concern Value - The going concern value generally assumes an institution must value not only its existing portfolios, but also those additions to the portfolio that can be expected as growth occurs or run-off is reinvested. In other words, the institution can be assumed to be a going concern, as opposed to being liquidated on a one-time basis.

Total Return

Total return has long been the accepted measure of performance for investment securities, but it has only recently gained acceptance in the depository institution industry as a performance measure. Total return incorporates earnings and market value appreciation in the assessment of performance. The total return concept thus considers both short-term and long-term earnings levels and stability.

Selecting a Measure for Returns

Each corporate must determine the relative merits of each performance measurement, then clearly state and internally communicate the return objectives for the overall institution, as well as each financial function. Just as importantly, the institution must clearly enumerate the constraints (risks) within which those return objectives must be achieved. In this regard, the framework for identifying and measuring risk exposure also must be determined.

Measuring Risk Exposure

Sources of Risk Exposure

The most significant sources of risk to a corporate are interest rate, liquidity and credit risks. Interest rate and liquidity risks are most relevant to the ALM process. In addition, widening credit spreads have periodically caused material increases in risk exposure and this risk must be adequately managed. Other risks include operational risk, fraud, and the risk of disasters or catastrophes. Since the measurement of these risks is discussed in more detail in other Guide sections, they are only briefly described here.

IRR - IRR is the primary focus of the ALCO and the ALM decision-making process. It arises from three primary sources: (1) the mismatch between the maturities or durations of assets, liabilities, and off-balance sheet instruments; (2) option risk including, the risk asset/liability durations will change as interest rates change; and (3) basis risk, the risk asset and funding/hedging rate spread relationships will change.

Mismatch risk is the most prevalent source of IRR. Option risk arises from the prepayment, cap, floor, and other options embedded in underlying mortgages, CMO tranches, adjustable-rate loans, term deposits, and other products. These options heighten the difficulty of hedging IRR because they contribute to the volatility of underlying asset and liability durations.

Basis risk occurs when unhedged or unhedgeable changes in interest rate spread relationships (between assets and liabilities or hedges) contribute to the instability of net interest earnings or value. For a typical corporate, this risk usually arises when it buys assets indexed to LIBOR, PRIME or COFI and issues liabilities to members based upon Treasuries or Fed Funds. Basis risk tends to have less of an impact on corporates than changes in the general level of interest rates.

These three sources of IRR, and the measurement and management of IRR, are discussed in the IRR Management section of this chapter (Page 202-31).

Liquidity Risk - Liquidity risk is the risk funds may not be available to meet cash outflows when they arise. This may occur because of insufficient cash flow, insufficient borrowing sources or because the assets designated as cash equivalents are not able to be sold quickly without causing a considerable loss due to a decline in the market value. Liquidity risk also can become significant if the financial condition of an institution is deteriorating and members, depositors, and/or creditors begin to withdraw or demand payment of their funds. Section 704.9 requires corporates to regularly monitor sources of internal and external liquidity and to model projected liquidity through a series of successively deteriorating scenarios. No explicit liquidity ratios or measures are specified in the regulation. However, it is important corporate credit unions develop meaningful liquidity measures and monitor them regularly.

A corporate should strive to maintain an amount of liquidity that is most efficient given its overall economic situation which in turn reflects the anticipated funding demands of its members. As a practical matter, corporates should maintain liquidity in excess of their projected day-to-day requirements. Additionally, corporates are considered bankers' banks and cannot incur daylight overdrafts at the Federal Reserve Banks. Therefore, daily liquidity management is of paramount importance. The maintenance of minimum liquidity levels represents a constraint on ALM. These and other aspects of liquidity management are discussed later in this chapter (Page 202-39)

Credit Risk - Credit risk is the risk due to uncertainty in a counterparty's ability to meet its obligations. It includes a counterparty's failure to repay principal and interest and/or perform on a derivative contract in a timely manner. This type of risk encompasses the exposure to loss as a result of a decline in market value stemming from a downgrade of an issuer or counterparty, or a change in the perception of the probability of default (widening credit spreads).

The impact credit risk can have on market value affects NEV and liquidity. Therefore, it is important the credit risk management process be reviewed by the ALCO. This process includes: asset quality review (including credit ratings, financial performance, level of credit enhancements, etc.); underwriting policies and guidelines; restructurings/workouts; and reserving levels. Credit risk involving investments is discussed further in Chapter 201, Investments.

Other Risks - Operational risk, fraud, and disaster risks have not traditionally been managed or overseen by the asset/liability manager or the ALCO. However, these risks should be considered within the overall risk management function. Since the ALM function will direct the corporate wide flow of funds, adequate procedures and controls must be installed to avoid inefficiency and fraud. Also, ALM applications and data must be backed up frequently and stored in an off-site location to enable the continuation of ALM operation in the event of a disruption. Thus, the ALCO must have reasonable assurance management responsibilities, internal controls, and information systems are adequate to provide clear guidance and control in the execution of balance sheet strategies.

Quantifying Risk Exposure

The risk of a given ALM strategy is typically quantified through the use of asset/liability models to perform simulation or sensitivity analyses. Important assumptions used in the projection of earnings or valuation of assets and liabilities are altered, and the change in expected returns (earnings or value) is determined. Asset/liability modeling is discussed in more detail later in this Section under "Asset/liability Modeling and Analysis" (Page 202-14).

Recent advances in computer technology have made risk quantification feasible for virtually any individual portfolio or balance sheet. Of course, risk analysis is only as good as the data and assumptions (including those not subjected to the sensitivity analysis) used in the model. Examiners must therefore review and critique the risk quantification methodology used by the corporate. Additionally, the corporate should obtain an independent third party validation of the implementation of its risk measurement system. All corporates are required to conduct a fair value (NEV) assessment of the balance sheet for a variety of rate scenarios. Other assessments should also be performed.

Once a methodology has been developed for measuring the risks in a corporate's balance sheet, limits for risk exposure must be established. Then management can concentrate on identifying and executing the most "efficient" strategies. Efficient strategies are those that best support the achievement of the institution's optimal risk/return profile. This may be done on a total balance sheet basis or for discreet portfolios, sometimes termed "books of business."

Optimization: Achieving an Efficient Risk/Return Profile

Once the institution's return objectives and risk constraints have been established, management must select strategies that most efficiently support attainment of goals. This process is called "optimization."he best optimization framework results in the selection of strategies with the highest return for the same (or similar) level of risk. Since the expected returns are quantifiable, and the variability of expected returns (risk) can be quantified through sensitivity analysis, a relatively objective selection framework results. Comparing two strategies with the same quantified risk exposure, the strategy with the higher return is considered most efficient, or that with the highest risk-adjusted return. By adjusting expected returns for the level of anticipated risk (variability of expected returns), this framework puts all the alternatives on a common measurement basis to facilitate decision making.

The cornerstone of a successful ALM/ALCO process is a technically rigorous asset/liability model that allows management to quantify risk/return tradeoffs. Optimization leads to the risk/return profile most desired by the board and management. The optimization framework is at the top of the ALM decision making process, which includes the ALCO, ALM policies, and related procedures and controls.

The ALM Decision-Making Process

The ALM decision-making process consists of:

1. the ALM policy framework;
2. the Asset/Liability Committee;
3. a comprehensive asset/liability model; and
4. related procedures and controls.

A shortfall in any of these process components can potentially disrupt the entire ALM function. If, on the other hand, these components are well designed and utilized, an institution will most likely attain its desired risk/return profile and overall financial objectives.

Examiners should review the ALM policies and asset/liability modeling process. It is usually very instructive to observe an ALCO meeting during the examination, since this is the core of the ALM decision-making process.

The ALM Policy Framework

Board policy and delegated authorities are crucial to the ALCO and the ALM function. Every portfolio in the corporate is affected by the ALM process, and each decision has an impact on both current and future profitability. Elements of an acceptable ALM policy are outlined in Table 2.

Table 2

General Outline of Asset/Liability Management Policy

I. Objectives of ALM
   A. Implement Board-Approved Policies
   B. Integrate the Financial Functions
   C. Determine Desired Risk/Return Profile
   D. Analyze Risk/Return Tradeoffs of ALM Proposals

II. Delegation of Authority from Board of Directors

III. The ALCO

IV. Asset/Liability Management Functions
   A. ALCO Support
   B. Asset/Liability Modeling and Analysis
   C. Execution of ALM Strategies

V. Risk Limitations
   A. IRR
   B. Liquidity Risk
   C. Credit Risk
   D. Other Risks

VI. Internal Controls/Guidelines
   A. Internal Controls (position limits, transaction authority, authorized dealers, etc.)
   B. Guidelines (approved security/instrument types, transaction/position limits, etc.)

The ALM policy legitimizes the ALM function within a corporate and provides a formal framework for its operation. Therefore, examiners should review the ALM policy of every corporate. Some corporates may alternatively refer to their ALM policy as the investment policy or funds management policy.

Examiners should determine whether: (1) the policy limits are reasonable given the corporate's financial condition and expertise of staff, (2) management is complying with the board-approved policies, and (3) periodic reports to the board are adequate.

The Asset/Liability Committee

The ALCO is at the core of an integrated, centralized ALM process. The objectives of the ALCO are to:

1. Implement board-approved policy.

2. Oversee and integrate the financial functions, and ensure a centralized approach to funds management, risk management, and earnings/capital management.

3. Set overall return objectives and quantify risk constraints, thereby defining the institution's risk/return profile.

4. Review the risk/return tradeoffs of potential ALM strategies to ensure they most efficiently support the achievement of the desired risk/return profile.

The ALCO decision-making process is just as important for small corporates as large ones. Relative to asset size, many asset/liability decisions in small corporates frequently have a greater impact on funds availability and earnings than those of their larger counterparts. The larger corporates tend to have a greater depth of personnel to staff an ALCO, but small corporates must rely on a few key managers and volunteers to carry out this critical function.

Part 704 requires corporates to have a formal ALCO. The committee should be comprised of key managers and must include at least one director. A typical ALCO will include the CEO, the CFO, the investment personnel (risk takers), the asset/liability and credit risk managers (risk monitors), and any other senior managers who routinely participate in the financial activities and strategies of the corporate.

The ALCO structure should be assessed by the examiner on a case-by-case basis, and recommendations should be made if it becomes evident during an examination that decision making is hampered or the representation on the committee is not adequate. The ideal size and composition of the ALCO will depend upon the strategic direction of a corporate and the relative size or importance of various portfolios.
Sometimes a committee that is too large is more of an impediment than a benefit to the decision-making process.

In some large corporates, the ALCO is further broken down into an internal or management ALCO and a board ALCO. By having a management ALCO, a corporate can have more frequent and technical discussions regarding the execution of strategies approved by the board ALCO. Board ALCO meetings tend to coincide with the monthly board meetings and permit officials who are not formal members of the committee to attend. This dual structure can permit the board to expeditiously review and challenge ALM reports without having to wade through technical details not directly related to strategic goals and risk oversight.

<u>ALCO Meetings</u>

A board ALCO should meet at least monthly. A management ALCO, if constituted, customarily meets more frequently and should be available to meet on short notice, if necessary, to respond to financial market developments. Participation on either ALCO is a major commitment to the institution. ALCO attendance should be mandatory and a quorum should be established to facilitate decision making in the absence of one or more members.

Examiners should verify appropriate emphasis is placed on the ALCO decision-making process. For example, if the CEO often fails to attend the ALCO meetings, or if the ALCO is otherwise relegated to a secondary status, the committee is unlikely to achieve its objectives. This situation may occur even if the corporate has a well-structured ALCO, good ALM policies, and a proficient modeling capability. The ALCO should function as a risk management body and not as an investment committee simply dedicated to analyzing perceived market opportunities.

Training for ALCO (and board) members is an important component of a strong ALCO process. Periodic training is necessary to keep abreast of market trends, products, and contemporary best practices in risk management. Training may be conducted by the staff of the corporate but should be augmented from time to time with professionals from outside the company who are known or regarded experts on the topic presented. The ALCO should keep a formal log of its training sessions and it should be reviewed by the examiners.

<u>ALCO Functions</u>

The functions of the typical ALCO are presented below. Depending on the size of the institution, complexity of its portfolio, and its asset/liability mix, the ALCO process may vary. The following functions should be considered.

1. Receive direction from and facilitate oversight by the board of directors. Provide periodic reports to the board regarding policy compliance, such as IRR exposure reports, earnings/capital projections and analysis. Periodically review ALM policy and recommend changes to the board;

2. Determine financial objectives and establish policy for each of the financial functions;

3. Coordinate funding of investments, lending (if any), and other activities. Project and review, at each meeting, the funding surplus/deficit with comprehensive short-term and long-term cash flow forecasts. Optimize cash resources, investment of liquid funds, and access to borrowed funds;

4. Coordinate product pricing. Oversee product-pricing mechanisms to ensure spread requirements are achieved and maintained. Set product prices on an incremental basis in conjunction with funding costs;

5. Direct proposed ALM strategies or transactions through technically rigorous simulation and scenario analysis;

6. Direct computation and monitoring of NEV. Ensure the reconciliation of NEV calculations to book value, and review economic and earnings effects of ALM decisions;

7. Set limits with regard to IRR exposure, both in the context of NEV and NII sensitivity (if NII measures are required by policy). Identify and approve measurement methodologies for the quantification of IRR;

8. Oversee investment portfolio management activities. Ensure excess liquid funds are optimally invested in securities that complement the institution's overall risk/return profile;

9. Monitor the economic environment, including regional and national economic conditions, interest rates, prepayment trends, volatility, and related regulatory developments;

10. Direct hedging operations (if any), including hedge analytics, related policy development, and integration with the overall risk/return profile. Specify the range of instruments that can be used to hedge the various kinds of risk exposures;

11. Direct capital market activities, including raising capital, debt issuance, dividend policies, and merger/acquisition analysis. Ensure these activities are integrated with the management of the overall risk/return profile; and

12. Ensure product development activities support the institution's overall risk/return objectives.

Examiners should review the ALCO's performance. It is important the ALCO function be centralized. A lack of centralization weakens the control of risk. Thus, the responsibilities detailed above should not be managed outside of this process by staff whose authority supersedes the ALCO.

Asset/Liability Modeling and Analysis

<u>Asset/Liability Modeling</u>

The ALM decision-making process should be centered around quantified measurements of the institution's overall risk/return profile and those of potential ALM strategies and instruments. Management should use a reliable asset/liability model in its ALM operations. An institution's asset/liability model should allow the asset/liability manager and the ALCO to identify and further analyze efficient ALM strategies. The model serves both strategic and risk monitoring objectives.

A model must be able to:

1. Accept a wide variety, and potentially a large volume, of data input and assumptions;

2. Accurately measure the risks associated with all instruments on the corporate's balance sheet.

3. Perform sensitivity and simulation analyses (described below) under different scenarios;

4. Generate concise and decision-oriented summary reports;

5. Allow for quick turnaround of "what if" analyses; and

6. Accommodate new instruments and products.

Examiners should review the ALM modeling process to determine whether the corporate's model (if any) is capable of performing the above tasks. Management should maintain its asset/liability model(s) commensurate with the scope and complexity of their activities.

Most asset/liability models have the same general design. Data concerning the institution's current balance sheet position (and off-balance sheet items) are entered (either manually or through an automated process) with the key earnings and value parameters for each portfolio. For example, the earnings parameters for fixed-rate mortgage related securities include the expected cash run-off (determined using a prepayment assumption) in each forecast period, the weighted-average coupon, and expected incremental activity in the portfolio.

Next, assumptions concerning future interest rates, prepayment conditions, spreads, volatility, and incremental activity are entered. Many of these assumptions are "shocked," or altered by certain amounts to enable the corporates to view their impact on earnings and net economic value. Then, decision-oriented reports are generated to support the ALCO function and ALM decision making.

Asset/liability models are used to perform sensitivity and simulation analyses in the measurement of IRR exposure and the analysis of proposed strategies. Sensitivity analyses are used to study the impact of strategies and assumptions on NEV in different environments. Simulation analyses review the impact of different strategies and assumptions on earnings. Ideally, a corporate's asset/liability model will be capable of quickly generating numerous sensitivity and simulation analyses. Such models allow for the analysis of both risk and return, within the context of both market value and accounting earnings. This kind of comprehensive analysis best facilitates the identification of the desired risk/return profile, and the analysis of risk/return tradeoffs.

Some corporates perform asset/liability modeling only to meet regulatory requirements pertaining to IRR measurement, rather than to support management analysis and decision making. Others have limited ability to model dynamic assets with embedded options yet they are inclined to buy such instruments. Also, some institutions do not have an adequate process in place to check or edit the model after manual data entries have been made (discussed earlier). Any such shortcomings should be noted in the examination report if identified by the examiners.

Another frequent problem in the asset/liability modeling area is unnecessarily cumbersome reports are generated for the ALCO, rather than summary-level analytical reports. The ALCO reports must contain useful information, not unintelligible reams of data. Sometimes, the computers used to run asset/liability software are too slow to support iterative sensitivity or simulation analysis. In such cases, the ALCO gets only a limited analysis, and may limit its requests for additional analysis, due to the lack of sufficient computer power. The need for and benefits of comprehensive analysis should drive the analytical process. Therefore, management should be made aware of computer power or report generation limitations that needlessly impede ALM analytics. In such cases, management should be encouraged to upgrade its capabilities. Examiners should be concerned when the ALCO has an appetite for risk-taking strategies, but is unwilling to implement an adequate model for cost or other reasons.

Other problems that become evident in the examination of the A/L modeling function include:

1. Overreliance on outside consultants;
2. Use of overly simplistic assumptions (example: basing all liability pricing off one key or index rate);
3. Overreliance on manual data entry;
4. Overly complex or condensed chart of accounts in asset/liability model (aggregation of instruments); and
5. Inexperienced personnel involved in the modeling function.

Other Modeling/Analytical Requirements

In addition to the asset/liability model, which is used to measure institution-wide IRR and the impact of traditional balance sheet ALM strategies, other models will likely be necessary to value specific instruments or to project assumptions for the asset/liability model or other purposes.

Those models may include:

1. Mortgage-derivative analysis (e.g., Bloomberg or other servicers);
2. Off-balance sheet derivatives:
    a. interest rate swaps;
    b. options;
    c. futures contracts; and
    d. forward agreements;
3. Mortgage (or other) prepayment forecasting;
4. Volatility term structures;
5. Hedge analytics (hedge ratio calculations, regression analysis);
6. Interest rate projection (forward Treasury yield curve analysis, cost of funds index projection);
7. Secondary marketing analysis (net exposure calculations, fallout projection);
8. Trading portfolio (technical analysis, charting, program trading);
9. Product profitability (transfer pricing, functional cost analysis); and
10. Budgeting.

Examiners should review most, if not all of these models, especially if they have a material impact on the ALM function. The review process should basically be the same as the review of the asset/liability model. In many cases, institutions rely on outside vendors, brokers, or consultants to perform analyses or calculations. Generally speaking, the over-reliance on an outside party for analysis used in an institution's key decision-making processes should be considered an unsafe and unsound practice. If the corporate does rely heavily on vendors, it should have a strong vendor management process and contingency procedures in place.

If the output from outside models is used in conjunction with the corporate's asset/liability model, the information or data provided should be reviewed for reasonableness. The utilization of automated interfaces between models limits input error and should be used whenever possible. The external models and the assumptions used must be consistent with the asset/liability model, otherwise, incongruence may undermine the process.

IRR Models

Measures of IRR require reliable information on the amount and timing of the cash flows generated by an institution's assets, liabilities, and off-balance sheet instruments. Because this information is not always known with certainty, assumptions must be made to perform the analysis. Depending on the type of analysis, these assumptions may include: (1) how market interest rates will change (over the period of analysis); (2) how instruments with rate dependent cash flows vary with interest rate changes; (3) how management will administer interest rates that are under its control (such as rates on shares and membership capital), when the general level of interest rates changes; and (4) in NII models, how management will reinvest interest and principal cash flows.

Two types of models are commonly used by depository institutions to estimate the interest rate sensitivity of NII: maturity gap models and NII simulation models. Likewise, there are two types of models commonly used to estimate the sensitivity of NEV: duration gap models, and NEV simulation models.

Maturity gap and simple duration gap models are similar in that they implicitly make assumptions about the way interest rates and cash flows behave. Perhaps the most serious shortcoming of these models is they assume cash flows do not change in response to interest rate changes. For example, the model assumes adjustable-rate loans do not reprice again after their next reset and mortgage prepayment rates as well as share decay rates do not vary. The result is the estimated change in NII or the change in the NEV of the institution is the same for a given increase in rates as it is for an equivalent decrease. However, in reality, the prepayment option embedded in mortgage assets results in asymmetric price changes for mortgages. That is, price increases when rates fall tend to be less than price declines when rates rise. The value of most corporate balance sheets shows a similar sensitivity. This sensitivity cannot be accurately estimated by gap and duration models that assume cash flows are the same in all interest rate environments.

NII and NEV simulation models, on the other hand, permit these assumptions to vary, but necessarily rely more heavily on the analyst to make choices about certain behavioral relationships incorporated into the model. Even though they rely more heavily on parameters set by analysts, NII and NEV simulation models can be much more accurate than their less sophisticated counterparts if appropriate assumptions are used.

When assessing any measure of IRR of a corporate, the examiner should carefully evaluate the reasonableness of the assumptions used in the analysis.

<u>Maturity Gap Models</u>

Maturity gaps are relatively easy to calculate compared to other measures of IRR, and during the 1980s were the most commonly used measures of IRR in depository institutions.

Maturity gap analysis measures the difference, or "gap," between the dollar value of assets and liabilities maturing or repricing during a given time period. The dollar gap is often expressed as a percentage of assets. When multiplied by a hypothetical change in interest rates, the dollar maturity gap gives a rough estimate of the effect of such a rate change on NII.

To calculate the maturity gap, principal balances of interest-earning assets and interest-bearing liabilities are categorized by maturity/repricing intervals or "buckets" (e.g., under one year, one to three years), depending on when the principal cash flows will be received or when their interest rate will next be adjusted. In more sophisticated gap models, the timing of the principal cash flows is adjusted by incorporating the effects of asset amortization, mortgage prepayments, core share decay, and the effects of off-balance sheet hedging instruments.

As an example of a maturity gap calculation, assume a corporate with \$10 million in assets estimates \$3 million will reprice during the next year (by having principal mature, prepay, amortize, or having the coupon adjust). Further, it is estimated \$6 million of liabilities will reprice during this time. This institution is said to have a "one-year gap" equal to negative 30 percent [(\$3m-\$6m) /\$10m].

$$\text{GAP} = \frac{(\$\text{Assets Repricing}) - (\$\text{Liabilities Repricing})}{\$\text{Total Assets}}$$

To estimate the effect a change in interest rates has on an institution's interest margin, the gap as a percent of assets is multiplied by the hypothetical rate change. For example, the estimated effect of a 1 percent rise in interest rates on NII over the next year would be approximately 0.30 percent or 30 basis points (1.0 percent x -30 percent = -0.30 percent). Given assets of \$10 million, this decrease in interest margin would translate to a reduction in NII of \$30,000 over this period.

Although maturity gaps are relatively easy to measure and do provide a rough measure of NII sensitivity, they have a number of well-known shortcomings including the following:

1. Maturity gap models typically focus exclusively on near-term NII. This focus hides the risk to NII of longer-term repricing mismatches. This ignores potentially adverse effects on not only earnings but also liquidity.

2. The repricing intervals chosen for analysis are arbitrary and there may be significant mismatches within a repricing interval that will be ignored in the analysis. The most common repricing interval analyzed by depository institutions is the one-year gap and the one to three-year gap. A cash flow to be received in one year should have a different effect on interest-rate exposure of an institution than an identical cash flow to be received in two and one-half years. Yet the one to three-year gap model would treat these two cash flows as equivalent in terms of their effect on the IRR of the institution.

3. Using maturity gaps to estimate the change in NII resulting from a change in interest rates assumes all interest rates change by the same amount--an unlikely occurrence. When the general level of interest rates increases by 1 percent for example, some interest rates, such as those paid on short-term transaction accounts, typically increase by a smaller amount, if at all.

4. It is not possible to properly incorporate the effect of exchange-traded options or the options embedded in many financial instruments such as early withdrawal options on share certificates, the caps and floors in ARMs, and mortgage prepayment options. These options have a significant effect on the rate sensitivity of a financial instrument, neglecting to incorporate them into the analysis will misstate the IRR of an institution.

<u>NII Simulation Models</u>

NII simulation models project interest-related cash flows of all assets, liabilities, and off-balance sheet instruments in an institution's balance sheet in order to estimate future net interest earnings over some chosen period of time. They are often referred to as "dynamic" NII simulation models because changes in operating strategies, relative interest rates, early withdrawal of shares, and prepayments can be built into the model.

NII sensitivity is calculated as follows. First, "base case" NII is projected for the current interest rate environment. Cash flows for each instrument are projected using assumptions about amortization characteristics, prepayment rates on mortgages, and share decay rates. Assumptions must be made regarding how the principal and interest cash flows received during the period of analysis will be reinvested.

Next, various simulations are done under alternative interest rate scenarios. For example, many models estimate the value of NII over the next year if interest rates were to increase or decrease by 100, 200, or 300 basis points. As in the base case scenario, interest cash flows are projected over the period of analysis, and will depend on assumed share decay rates, prepayment rates, and on how rates on adjustable-rate assets and shares are assumed to change in each interest rate scenario. (To project how the coupons on adjustable-rate assets will change, information on the time to first reset, reset frequency, and the presence of any rate caps or floors is needed.)

The larger the differences in projected earnings between the base case and the alternative interest rate scenarios, the higher the level of IRR.

NII Simulation offers the following advantages:

1. NII simulation models can provide more accurate estimates of the effect of changing interest rates on the future interest income of instruments with embedded options by varying prepayment rates according to the interest rate scenario being simulated. The value of other embedded options (e.g., lifetime caps on ARMs) and off-balance sheet instruments in an institution's balance sheet can be similarly assessed.

2. Interest rates on different instruments can be assumed to change by different amounts when there is a change in the general level of interest rates. For example, changes in rates on core shares can be assumed to lag behind changes in other rates.

Simulation analysis also has a disadvantage. Like gap analysis, NII simulation models typically measure the effect of a change in interest rates over only short periods of time, such as one year. Models that project NII over longer periods of time sometimes aggregate these future cash flows in a manner that implies cash flows received in the distant future are as valuable as those received in the near future. For example, a model may indicate if rates increase by 100 basis points, an institution will lose \$100 during the next year but will gain \$100 in year two of the analysis. In fact, the present value of the \$100 received in two years is less than the value of \$100 received in year one. NII models projecting NII over long periods should take the time value of money into account.

Analysis of the Sensitivity of Net Economic Value

The net economic value "N" equals the estimated present value (or "economic value") of assets "A," less the present value of liabilities "L," plus or minus the present value of all off-balance sheet items "O."
Thus,

$$N = A - L + O$$

Two types of models are commonly used to analyze the sensitivity of NEV: the duration gap model and the NEV sensitivity model. Both models require detailed information on the amount and timing of all future cash flows deriving from all financial instruments in the balance sheet as well as the specification of appropriate discount rates.

<u>Duration Gap Analysis</u>

Duration gap is the difference between the weighted-average duration of assets and liabilities, adjusted for the net duration of all off-balance sheet instruments. It is a measure of the percentage change in the NEV that would be expected if interest rates were to change by 100 basis points. This measure is a "point" estimate and is accurate for only small changes in interest rates.

To calculate the duration gap, the duration of each item in the balance sheet is separately calculated. The duration "D" of each instrument is weighted by the ratio of its market value to the net value of the balance sheet, and the weighted durations of all assets, liabilities, and off-balance sheet instruments are netted as follows.

$$D_N = D_A(A/N) - D_L(L/N) + D_O(O/N)$$

There are several different forms of the duration measure including simple (or Macaulay) duration and modified duration. Modified duration is the measure most often used to calculate the duration gap, and because it requires calculation of simple duration, both measures are described below.

Simple Duration

Simple duration was developed to provide a measure of the average time to receipt of the cash flows of a financial instrument. It measures the weighted average time until payments are received, where the weights are the proportion of the total present value of the instrument received in each period.

Calculation of the simple duration of an instrument requires three steps. First, calculate the present value of each cash flow (principal and interest) by discounting them by the instrument's required yield. (The sum of these present values equals the estimated price or market value of the instrument.) Second, multiply each present value by the number of years until it occurs, and sum these time-weighted present values. Third, divide the sum of the time-weighted present values from step two by the sum of the unweighted present values from step one.

Modified Duration

Modified duration is a measure of the interest rate sensitivity of an instrument and is obtained by dividing simple duration by 1+ (Yield-To-Maturity /Number of Coupon Periods per Year). Modified duration indicates the expected percentage change in the price of a bond for every one percent change in market interest rates. The formula is presented below:

$$Dmod = \frac{D}{(1+(YTM/n))}$$

where Dmod = modified duration;
D = simple duration of the instrument;
YTM = yield to maturity; and
n = number of coupon periods per year.

For example, if a security had a modified duration of 2.566, the market price of the security would change inversely by 2.566 percent for every 1.00 percent change in market interest rates. After the duration of each item in the balance sheet has been calculated, each instrument's duration is weighted by the ratio of the market value of that instrument to the NEV, and netted.

One difficulty in calculating the duration gap lies in obtaining economic values for each instrument. If market price quotes cannot be obtained, the economic values may be calculated using present value analysis as described in the next section on the NEV sensitivity model. Book values are sometimes used to calculate the duration gap when market values are not available or not easily estimated. When economic values diverge significantly from book values, the use of book values may result in significant error in the estimation of the interest rate sensitivity of balance sheet value. Other drawbacks of duration gap analysis are listed below.

1. Duration gap analysis provides accurate estimates of price sensitivities of instruments only for small changes in interest rates, those less than 100 basis points. Modified duration assumes the percentage price change due to a rate change of a given magnitude will be the same when rates rise or fall (although opposite in sign). However, this is not true when rates change by a large amount. For a simple bond with no embedded options (such as a non-callable Treasury security), a large decrease in rates will result in a larger percentage increase in price than the percentage decrease in price that would result from an equal increase in rate (this phenomenon is known as convexity). The analysis is further complicated when analyzing financial instruments with embedded options such as

mortgage loans. Because borrowers tend to prepay their loans when refinancing rates fall below the coupon on the loans, the value of the loan will not rise as much as it would have had borrowers not prepaid (negative convexity).

2. Duration does not take the shape of the yield curve into account. The present values in the modified duration computation are usually calculated using the same discount rate (the required yield) for each future cash flow irrespective of when that cash flow will occur. This causes long maturity cash flows to be overvalued and short maturity cash flows to be undervalued, biasing the estimated duration.

NEV Sensitivity Analysis

The measure of IRR deemed most important by NCUA is the sensitivity of the NEV to changes in interest rates. A corporate's NEV is defined as the present value of assets minus the present value of liabilities plus the net market value of off-balance sheet contracts. The sensitivity of NEV is the change in a corporate's NEV that would result from a shift, or shock, in the term structure of interest rates, for example, by plus or minus 100 basis points.

Unlike simple duration gap, this measure may be used to estimate the change in economic value for substantial changes in interest rates, like 100 or 200 basis points or more. These larger changes in interest rates allow the measure of IRR to depict the corporate's economic exposure across a wider range of possible outcomes.

The remainder of this section is devoted to a brief overview of NEV sensitivity analysis. In particular, two methods of measuring the economic value of financial instruments are discussed.

Measuring NEV: Static Discounted Cash Flow Approach

The value of a financial instrument can be estimated by projecting the amount and timing of the future net cash flows generated by the instrument, and discounting those cash flows by appropriate discount rates. This procedure is commonly referred to as discounted cash flow analysis, or present value analysis.

The basic formula for the present value of a financial instrument is as follows:

$$PV = CF_1/(1+i_1) + CF_2/(1+i_2)^2 + \ldots + Cf_m/(1+i_m)^m$$

CF_1 is the estimated amount of the first cash flow generated and i_1 is its discount rate. The discount rate used for each projected cash flow is the yield currently available to investors from cash flows resulting from alternative instruments of comparable risk and duration.

The accuracy of any valuation derived from the discounted cash flow analysis depends on the accuracy of both the cash flow estimates and the discount rates used. These cash flows and discount rates must be estimated not only for the current scenario, but for each of the alternate interest rate scenarios being estimated.

1. Estimating Cash Flows

Under each interest rate scenario, a single path of future interest rates is assumed, based on future rates implied by the current term structure of interest rates. (In fact, this analysis is referred to as "static" cash flow analysis because each scenario depicts a single hypothetical path of interest rates, as opposed to the numerous paths used in the option adjusted spread [OAS] analysis described below.) Cash flows are calculated within each scenario based upon the assumed path of interest rates depicted in that scenario.

Cash flows may differ across scenarios for two reasons. First, mortgage prepayments and share attrition rates will differ since mortgage holders and share holders can be expected to make different decisions about these actions under different interest rate environments. Such differences in behavior are modeled by specifying a relationship between the interest rate scenario and the rates of prepayment and attrition, thereby changing the magnitude and timing of principal and interest cash flows. Second, the magnitude of interest cash flows differs across scenarios as adjustable-rate instruments (such as ARMs or demand accounts) reprice in future periods and receive different future coupon rates under different scenarios.

2. Discount Rates

The rate used to discount a cash flow should represent the yield obtainable in the market for a cash flow of similar maturity and risk.

There are two common methods for arriving at the discount rates for a particular instrument. The simpler method is to discount every projected cash flow by the yield of comparable instruments. In this case, each of the "*i* s" in the preceding equation would equal the current market yield of the instrument for which cash flows are being discounted.

A more complex, and more accurate method is to use non-constant discount rates based on the yields of zero-coupon instruments with maturities equal to those of each respective cash flow. In practice, this is done by calculating for each cash flow a discount rate that has two components: a risk-free component, which is represented by the zero-coupon Treasury yield for the same maturity, and a fixed spread, which compensates investors for prepayment, credit, and liquidity risk. This fixed spread is calculated as an increment to each of the risk-free components that causes the sum of the discounted cash flows to equal the observed market price of the instrument.

For either of the methods used, the discount rates in the alternate interest rate scenarios are typically adjusted by adding or subtracting the amount of the interest rate shock (e.g., for a plus 100 basis point scenario, add 100 basis points to each discount rate).

Measuring NEV: Option-Based Pricing

An option-based pricing approach is a more sophisticated approach to valuing assets (and, less frequently, liabilities) that contain embedded options.

The most important options in corporates' balance sheets are the prepayment options in mortgage securities and the caps and floors in adjustable-rate mortgage securities. When mortgage rates fall, mortgage prepayments typically accelerate, forcing corporates to reinvest the proceeds at lower yields. Interest rate caps and floors prevent the coupon rates of adjustable-rate assets from moving above or below a certain level when interest rates change. Both of these types of options can have a significant effect on the interest rate sensitivity of the instruments in which they are embedded.

In large part, the values of these options depend on the volatility of interest rates. When mortgage rate volatility increases, there is a greater chance that mortgage rates will fall sufficiently below the rates on existing mortgages so as to induce prepayment. Likewise, the greater the volatility of the index on which adjustable-rate loans are based, the more likely the coupon will be constrained by any rate cap or floor.

Option-based pricing models, also known as OAS models, use an interest rate simulation program to generate numerous (hundreds or even thousands) random interest rate paths that, in conjunction with a prepayment model, are used to estimate mortgage cash flows along each path. These cash flows are then discounted and averaged to arrive at a single mortgage price.

OAS models provide more accurate estimates of the value of these embedded options (and, therefore, of the mortgages themselves) than static discounted cash flow models. In a static cash flow analysis, the option has no value unless it is "in the money" (i.e., the prepayment option is exercised because rates have fallen and the homeowner chooses to refinance, or the rate cap or floor is effective). In fact, like exchange-traded options, these options have value even when they are not in the money, because it is possible they will be in the money at some future date. Market participants will pay more or less for the instrument containing the option depending on the likelihood of exercise.

The sensitivity of NEV is a valuable measure of IRR because it estimates how the economic value of an institution changes when interest rates change. In addition, the results are easy to interpret. However, it is a complex measure that requires extensive modeling, and, as with any measure of IRR, the results are sensitive to the assumptions used.

Procedures and Controls

To ensure the integrity of the ALM decision-making process, internal procedures and controls must provide for efficient data flows. This is especially important because of the need to receive and input cash flow data from every major department in the corporate, and to make coordinated decisions affecting the entire institution based on the analysis of that data. The size of the corporate and the volume of transactions should be taken into consideration by examiners.

If the ALM process is not functioning properly, examiners should focus on the related operating procedures and internal controls. In a large institution, the documented procedures typically will need to be quite extensive to accommodate a large volume of data flow from numerous functional areas to the asset/liability manager.

Internal Procedures

Procedures must be documented and in place that allow for the smooth and timely flow of data to the asset/liability modeling function, the ALCO, and other areas. Flow charts documenting this physical flow of data from all departments are usually very informative. If such flow charts do not exist, management should be encouraged to develop them.

Procedures also must be developed to verify data entry required in the asset/liability modeling, cash flow forecasting, pricing analysis, and other key computational ALM operations. Required analytical processes for certain strategies, such as hedge ratio calculations or mortgage-derivative analytics, should also be documented. Processes should be in place to confirm individual strategies or transactions are not in violation of NCUA Regulations and those of other agencies.

The corporate must develop formal procedures to investigate unusual changes in security pricing and option adjusted spreads. Such anomalies may indicate an error or a problem. By having formal investigative procedures for this process, the corporate ensures timely and consistent treatment of any such issues.

Other procedures are necessary to accommodate the ALM function at certain institutions. These should be assessed on a case-by-case basis.

Internal Controls

In small corporates, internal controls are more important as it is more likely an individual may be performing multiple incompatible functions (i.e., a senior manager may not only be involved in ALCO decisions, but may also execute transactions, oversee the disbursement of cash, and authorize the related accounting entries). Examiners should take exception where the organizational structure does not provide for sufficient segregation of duties and adequate compensating controls have not been established. Critical responsibilities must be properly separated to ensure adequate internal control to the extent possible.

Examiners should also verify internal controls in the ALM function are adequate in the following areas: transaction authorizations - both internal (officers authorized to transact business) and external (e.g., approved dealers); position/transaction limits; regulatory requirements or limits; and other guidelines. Policies and procedures for the individual financial functions usually elaborate on these control features.

Executing ALM Strategies & Decisions: The Financial Functions

Structured appropriately, the ALM decision-making process should result in effective strategies to guide an institution toward achieving its overall financial objectives. These strategies are then implemented by the financial functions which are the portfolio-level operations that carry out three elements of the ALM process: (1) funds management and pricing; (2) risk management; and (3) earnings/value management.

Examiners should review the procedures for communicating actionable decisions to the functional areas, and the reports generated for the board which summarize the nature and purpose of each major transaction. Additionally, examiners should look to the policies and procedures in each of the functional operations to verify the strategies selected by the ALCO have been executed efficiently.

The Three Elements of the ALM Process

Funds Management and Pricing

This element consists of the functions involved in the origination, purchase, sale, maturity, and/or other activities involving the flow of funds. Therefore, asset (primarily investments) and liability management falls into this category. To ensure the most efficient and profitable movement of funds, cash management and liquidity management fall into this area.

The pricing of assets and liabilities is an integral part of funds management. Share and loan products are generally priced by management, while investments and borrowed funds are dictated by the market, hence, to a lesser extent controlled by management. As a result, pricing effects the management of funds in all portfolios (books of business), and the increase or decrease in the net funds flow.

The primary purpose of the ALM function is to coordinate funding and pricing decisions in order to optimize the integration of the financial functions. These decisions will then pave the way for the maximization of capital and the control of risk exposure.

Risk Management

The attributes of the asset, liability, and off-balance sheet portfolios will have a direct bearing on an institution's overall risk exposure. The maturity and pricing characteristics of each portfolio affect overall IRR exposure, while earnings and capital strength impact liquidity risk.

Interest rate and liquidity risks are the primary risk management concerns of the ALCO. The measurement of IRR is discussed in the IRR Management section (below). Hedging and/or derivatives can be used to offset IRR exposure.

Earnings/Value Management

A corporate's financial objectives are met by achieving desired returns, as measured by earnings or economic value, and by minimizing the variability of those returns. In the ALM context, earnings management primarily entails the management of the net interest margin (also called spread management), and value management refers to the management and stabilization of net economic value. The risk/return tradeoffs constantly facing management will have different implications for earnings and NEV.

Earnings and NEV management are closely related to pricing and risk management (discussed above). If, for example, the ALCO chooses to invest in only short-term Treasuries, these assets will be less profitable than more risky alternatives. However, the limited credit risk associated with this strategy will promote the stability of earnings and value. Another example, if the ALCO chooses a strategy that results in greater IRR exposure, then future earnings variability will be heightened.

The spread management function is designed to maintain the net interest margin requirements of the institution. In this regard, it is crucial that share pricing is under the purview of the ALM function. Finally, the management of capital markets activities and the computation of net economic value are crucial to the management and monitoring of an institution's overall NEV.

IRR Management

Introduction

IRR can be defined as the sensitivity of a depository institution's earnings and NEV to changes in interest rates. IRR results from the differences in the way the value of assets, liabilities, and off-balance sheet instruments are affected by interest rate changes.

The interest rate sensitivity of a corporate's balance sheet depends on the characteristics of the financial instruments comprising the balance sheet. Corporates' liabilities include a large percentage of overnight shares. Since shares typically reprice faster than investment assets, most corporates are exposed to rising interest rates. This means their NEV and earnings decline when interest rates rise and increase when interest rates fall. However, there are some institutions that experience decreased earnings and declining net worth when interest rates fall, due to their balance sheet composition.

The interest rate sensitivity of a financial instrument depends on many factors including: (1) maturity (generally, of two otherwise identical instruments, the one with the longer maturity will be more interest rate sensitive); (2) repricing characteristics (instruments such as adjustable-rate bonds that reprice frequently to market interest rates are typically less interest rate sensitive than fixed-rate instruments); and (3) the presence of embedded options (such as prepayments, interest rate caps, and deposit withdrawal options that affect the timing of the cash flows generated by the instruments).

To properly evaluate the IRR exposure of a corporate, the effect of interest rate changes on the entire balance sheet must be analyzed. It can be extremely misleading to conclude an institution is significantly exposed to IRR on the basis of a few very rate sensitive instruments. In fact, the interest rate sensitivity of those instruments may be offset by other instruments in the balance sheet less rate-sensitive, or inversely affected by rate changes. Corporate investments may have a corresponding liability that has substantially similar characteristics and this permits the risks associated with the asset to be transferred to the holder of the liability (a "matched" transaction).

Both the board of directors and management of a corporate are responsible for the management of IRR.

In general, IRR management involves the following steps: choosing target measures (e.g., NII and NEV); setting limits on acceptable levels of interest rate exposure for each target measure; estimating the interest rate sensitivity of each target measure; and restructuring or hedging the balance sheet if the estimated interest rate sensitivity exceeds the established exposure limits.

Summary of Section 704.8 (Limits on IRR)

The objective of IRR management is to control an institution's exposure to changes in interest rates to maintain adequate levels of earnings and capital over a range of possible interest-rate environments. Requirements for the management of IRR are established in 704.8(d). The board of directors is responsible for the development of a policy for controlling IRR. It is management's responsibility to ensure the policy is successfully implemented by establishing adequate guidelines and procedures. Further, management is responsible for reporting the implementation and monitoring of such policy to the board on a periodic basis (at least quarterly for base case corporates). The board shall review the results of operations and make adjustments to the policy as needed.

It is important to understand the responsibilities of management and the board of directors regarding the measurement and management of IRR. The following sections summarize those responsibilities.

Policy Statement

The board's policy statement shall include established limits on the institution's IRR exposure, identify the contents of reports to be made by management to the board, and specify the frequency the directors will review IRR management (at least quarterly per Section 704.8(d)). The delegation of responsibility for managing the institution's exposure to IRR should be clearly defined in the board's policy statement. Specific authorizations and restrictions should be provided regarding the institution's investment and trading activities (if any), the use of derivatives and synthetic instruments (corporates with Part IV authority), and hedging strategies.

Periodic Review

Periodic reports by management to the board of directors should demonstrate compliance with the exposure limits. Table 3 illustrates the type of interest rate sensitivity analysis management should prepare to demonstrate compliance with its board's exposure limits. In columns [3] and [5], XYZ's management is reporting neither NII nor NEV would be reduced by more than the percentages permitted by the board of directors, shown in columns [2] and [4], under any of the prescribed interest rate environments. Finally, the levels of NII and NEV used as denominators in calculating columns [3] and [5] should be reported as memo items.

Measurements of the sensitivity of the institution's NII and NEV will be necessary for management to demonstrate compliance with the board of directors' limits on exposure (as in columns [3] and [5] of Table 3). A corporate should be able to explain the reasons for any large differences between their own NEV sensitivity estimates and those produced by a periodic independent third party review.

Table 3
Current Exposure of XYZ Corporate to
Hypothetical Changes in Interest Rates

[1]	[2]	[3]	[4]	[5]
		Percentage Change		
Change In	Net Interest Income		Net Economic Value	
Interest Rates	Board	Projected	Board	Projected
(in basis points)	Limit	Change	Limit	Change
+300	-75	-70	-50	-40
+200	-50	-30	-25	-15
+100	-20	-10	-10	-5
0	0	0	0	0
-100	-20	15	-10	10
-200	-50	35	-25	15
-300	-75	40	-50	15

Note:
Net interest income projected under constant interest rates: $400
Net economic value under current interest rates: $1,000

Because any system of IRR management will rely on certain assumptions, management should document the assumptions underlying its interest rate sensitivity analysis and demonstrate to the board they are reasonable. For example, management would need to explain how prepayments would be expected to behave under various interest rate scenarios and how they would affect the sensitivity measures. If more elaborate sensitivity analysis is used, the assumptions being made in that analysis should be discussed with the board and documented.

Requirements for NEV Models

This section describes the minimum requirements NEV models used by institutions for regulatory compliance should meet. The requirements concern three general areas: (1) the items that are properly included in the NEV measure, (2) how cash flows are estimated in the base case interest rate environment and the alternate interest rate environments, and (3) what discount rates should be used in the base case and alternate rate scenarios.

Items Included in NEV Measure

NEV should include the estimated present value (or economic value) of all existing assets, liabilities, and off-balance sheet items associated with the corporate's balance sheet. For example, the estimates will not include the value of new investments management projects it would make under the various interest rate environments, or the value of new share accounts they believe the corporate will attract. It, however, should include the value of all off-balance sheet instruments and any forward settling investment transactions already executed at the cutoff date.

For their internal use, institutions may want to produce estimates of the interest rate sensitivity of their balance sheets on a going concern basis, taking into account future business (e.g., interest rate "ramps"). For regulatory purposes, however, NEV should include only the value of existing instruments.

Estimation of Cash Flows

The cash flows of all instruments must be estimated separately for each interest rate scenario. The cash flows of many financial instruments held by corporates change depending on the course of interest rates. It is not acceptable for institutions to estimate the cash flows of these instruments for the base case and assume those same cash flows would also be realized in the alternate interest rate environments. NEV models should consider the fact coupons on adjustable-rate investments and shares, mortgage prepayment rates, and core share decay rates will change depending on the interest rate scenario. Institutions should document mortgage prepayment rates and deposit decay rates assumed in each interest rate scenario.

To the extent possible given their data systems, institutions should use disaggregated data to estimate the economic market value of their instruments. If sufficient information is available, each individual balance sheet component (investment, share, etc.) can be valued separately using information on amortization, coupon, maturity, and any options embedded in the instrument to estimate future cash flows. Corporates should disaggregate instruments to the extent practical, grouping only very similar instruments together.

For example, if not valued separately, fixed-rate mortgage-backed pass-through securities, at a minimum, should be stratified into several coupon ranges (e.g., 7 to 8 percent; 8 to 9 percent, etc.). Adjustable-rate mortgage-backed securities (ARMs) should be segregated by index type, adjustment frequency, and distance to the lifetime cap (for example, those close to their lifetime cap should be valued separately from those with rates, say 2 percentage points from their cap). Shares should be segregated by type. This stratification permits the application of appropriate parameters (prepayment rates, decay rates, etc.) to each type of instrument and will result in more accurate economic value estimates.

Discount Rates

When estimating economic values, institutions should choose discount rates that reflect the risks of holding a particular instrument, including credit and liquidity risks. There are a number of possible methods of determining appropriate discount rates for financial instruments. The most common but least accurate method is to discount all future cash flows of a particular instrument by a constant discount rate that reflects the required yield of the instrument. For a typical upward-sloping term structure, this method overvalues long-term cash flows and undervalues short-term cash flows. A more accurate method involves discounting cash flows of different maturities by different discount rates. Under this method, the discount rate of any particular cash flow of a given maturity is equal to the estimated "risk-free" rate plus a fixed spread that compensates investors for the risk of holding the instrument. The risk-free rate for any given maturity cash flow is represented by the U.S. Treasury zero-coupon yield of the same maturity. The responsibility for choosing a particular discounting method resides with the institution. Like other assumptions necessary to calculate the NEV sensitivity estimates, the details and the rationale for the method chosen should be documented by the institution.

Management Strategy

The board and management are responsible for the institution's IRR management strategy and its implementation. They must understand the strategy and its possible effects on the short- and long-term financial health of the institution.

In formulating an IRR strategy, the board and management should consider the level of expertise needed to implement the strategy. A prudent IRR management strategy should be within the scope of existing management expertise. The corporate should not rely on speculative plans to remedy an excessive IRR exposure, nor should it incur excessive credit or liquidity risk to do so.

Steps taken to manage IRR may conflict with other business goals. To ensure such conflicts are minimized, management's IRR strategy should be developed in conjunction with the creation of a comprehensive business plan for the institution. It may well be the profitability, financial structure and IRR targets an institution would choose independently of one another are not attainable simultaneously. By developing these targets and the plans for achieving them as part of a single process, management can determine which combinations of targets are feasible and can make an informed choice among them.

Evaluating IRR Exposure

To be able to make meaningful judgments about the exposure of an institution to changes in interest rates, it is helpful to measure and compare its exposure with that of other institutions under a standardized framework. The framework adopted by NCUA for this purpose is to examine exposure in the context of how an institution's NEV would be affected by an instantaneous, adverse shift in interest rates of plus or minus 300 basis points. An adverse rate shock is defined as a 300 basis point increase or decrease in interest rates, whichever results in the larger decline in an institution's NEV.

The effect on NEV of an adverse rate shock is viewed relative to the size of the estimated present value of the institution's assets. An institution's NEV ratio is defined as its NEV divided by the present value of its assets (PVA), or:

$$\text{NEV Ratio} = \frac{\text{NEV}}{\text{PVA}}$$

Table 4

Interest Rate Scenario	-300 Basis Point Change	Base Case	+300 Basis Point Change
Present Value of Assets	$105	$100	$80
Present Value of Liabilities	-99	-95	-77
NEV	6	5	3
NEV Ratio	5.7%	5%	3.8%

To detect excessive exposure, it is important to determine both the level to which an institution's NEV ratio is expected to decline as a result of an adverse change in interest rates as well as the magnitude of the decline in the ratio. This can be done through the use of two measures: an exposure measure, which is also referred to as the "post-shock NEV ratio," and a sensitivity measure, which is the decline in the NEV ratio due to shocking.

Exposure Measure

The post-shock NEV ratio is simply an institution's NEV ratio in the aftermath of an adverse interest rate shock.

$$\text{Post-Shock NEV Ratio} = \frac{\text{NEV after Shock}}{\text{PVA after Shock}}$$

$$= \frac{\text{NEV +300}}{\text{PVA +300}} \text{ or } \frac{\text{NEV -300}}{\text{PVA -300}} \text{ whichever is lower}$$

The calculation of the post-shock NEV ratio is illustrated in Table 4, which shows the estimated change in the present value of the assets, liabilities, and capital accounts of XYZ Corporate resulting from a 300 basis point increase and decrease in interest rates.

In Table 4, the adverse scenario is the one in which rates increase 300 basis points. Under that scenario, XYZ's NEV ratio declines to 3.8 percent. Thus, XYZ's post-shock NEV ratio is 3.8 percent.

Again, the post-shock NEV ratio is simply the NEV ratio that results from the most adverse 300 basis point shift in rates. This ratio measures the capital cushion expected to be left in a corporate should an adverse change in interest rates occur.

The post-shock NEV ratio is a function of the sensitivity of NEV to changes in rates and the size of the NEV cushion in the base case scenario. Thus, an institution's post-shock NEV ratio could be low either because its balance sheet is very sensitive to changes in interest rates, causing it to lose a large portion of its NEV in an adverse interest rate move, or because its base case NEV is low. Thus, a low post-shock NEV ratio is not necessarily an indication of high IRR; it may merely indicate the corporate's base case NEV ratio is low.

Sensitivity Measure

The decline in NEV ratio due to shock measures the magnitude of loss an institution would suffer from a specified, adverse move in interest rates. More specifically, it is the absolute percentage point decline in the NEV ratio that would result from a hypothetical 300 basis point change in interest rates. In the preceding example, XYZ's NEV ratio declines from the base case level of 5.0 to 3.8 percent as a result of a 300 basis point increase in rates, a decline of 120 basis points. The decline in the NEV ratio is simply the difference, expressed in basis points, between an institution's base case NEV ratio and its post-shock NEV ratio (e.g., its NEV ratio under the adverse 300 basis point shift in rates).

Taken alone, a large decline in the NEV ratio is not necessarily indicative of excessive risk. An institution with a strong capital position could experience a sharp decline in its NEV ratio, as a result of a 300 basis point rate shock, and still be left with a substantial capital cushion. In summary, exposure analysis can be viewed as a two-dimensional problem that involves estimating both the level to which an institution's NEV ratio will decline as a result of an adverse rate shock, as well as the extent of the decline.

Methods to Reduce IRR

Institutions that project declines in earnings and NEV when interest rates increase may lower exposure by increasing the duration of liabilities or decreasing the duration of assets. This can be accomplished through balance sheet restructuring or hedging. Examples of measures such institutions might undertake include the following:

1. Sell securities;
2. Increase the proportion of short-term and adjustable-rate assets on the balance sheet;
3. Replace short-term funding with longer-term shares and borrowings;

4. Retain core shares, which are typically less interest rate sensitive than CDs; and
5. Use derivative instruments (Part IV expanded authority), such as futures, options, interest rate swaps, and caps, to lower exposure to IRR.

Although the majority of corporates are exposed to rising interest rates, there may be corporates exposed to falling rates. These institutions could lower their exposure by restructuring their balance sheets to lengthen the duration of their assets or decrease the duration of their liabilities.

Liquidity Risk Management and Contingency Funding

Asset/Liability Perspective

Corporate credit unions are first and foremost liquidity centers. Prudent asset/liability management requires a corporate to monitor cash flow and to manage liquidity risk. Cash flow refers to the process by which a corporate obtains and allocates its cash over time. Liquidity risk is the probability a corporate will be unable to: honor members' requests for share withdrawals, meet lines of credit or commitments already approved for members, fund forward purchase agreements, pay bills when due, repay maturing share and borrowed money liabilities, or pledge additional collateral for borrowing money. Liquidity risk management encompasses assets, liabilities, commitments, and collateral.

Liquidity Requirements

Liquidity management is the process a corporate uses to allocate its assets and structure its liabilities to provide sufficient liquidity to meet its needs and its members' demands.

Liquidity management provides the foundation for a corporate's asset/liability system. Corporates provide credit and share services to accommodate members. An illiquid corporate may lose the confidence of its members and the financial markets. Managers must analyze growth, cyclical, seasonal, random, competitive, and regulatory elements to ensure the risk of illiquidity does not outweigh pro forma earnings. Regulators must evaluate how management measures, monitors, and plans its cash flow and liquidity.

Cash flow analysis is related to earnings, but the two are not the same. A corporate may be in a positive earnings status but not liquid, or it may be liquid but not in a positive earnings status. Accounting accruals do not necessarily coincide with cash flow as illustrated below.

1. A zero-coupon or original issue discount security may have been purchased to generate a 10 percent yield. Although the accounting system may periodically accrete the discount to maturity as income, no cash is received. The corporate will generate substantial cash inflow at maturity from the same security that is far in excess of that instrument's yield. Interest income and cash inflow are not synonymous.

2. A corporate might pay 7 percent for savings and share certificates. If shareholders do not require the interest expense to be paid monthly because the interest is credited, the cash paid will be substantially less than interest expense accrued. The corporate will suffer a significantly greater cash outflow than interest expense when the shares are withdrawn. Interest expense and cash outflow are not necessarily synonymous.

3. A corporate with Part IV authorities may hedge its assets or liabilities with a short position in interest rate futures. If interest rates increase (decrease), the corporate will receive (pay) cash flow immediately, but must defer the gains (losses) over the life of the instrument hedged. Hedging does not necessarily generate cash flows that are the opposite of the targeted instrument for an IRR reduction.

4. Certain expenses such as depreciation and amortization are not actual cash flows, rather they are the recognition over time of previous expenditures. These items must be added back when determining net cash flows.

From a financial perspective, management must provide an asset/liability structure that generates positive earnings based on accrual accounting and sufficient cash flow to meet the demands imposed by members, the financial markets, and regulations.

Cash flow is also related to IRR management; however, the two are not the same. The potential repricing of an asset or liability does not imply the instrument is maturing. Similar to cash flow and earnings, the two factors are partially related as illustrated below.

1. A corporate might purchase an MBS backed by adjustable-rate mortgages (ARMs) with a one-year repricing interval. If the ARMs' interest rate index increases, the monthly cash inflow from the loans will increase up to the ceiling imposed by annual and lifetime rate caps (if caps exist in the structure). However, the corporate still has its funds invested in ARMs and does not have the same asset flexibility as if the loans were paid off or called at the end of the year.

2. Most mortgage loans backing MBS include a prepayment option. Mortgagors are much more (less) likely to exercise that option when interest rates decrease (increase). Consequently, corporates receive (back) relatively more cash when prepayment activity is high and reinvestment alternatives are poor, yet receive relatively less cash when prepayments slow down and reinvestment alternatives are good. Cash flow can move in a contrary direction from what is otherwise desired to manage IRR.

3. Fixed-rate shareholders are more likely to withdraw accounts and incur substantial early withdrawal penalties if interest rates have increased sufficiently to make it attractive to reinvest funds elsewhere. A fixed-rate, long-term account may become rate sensitive and require payout when a corporate least wants to locate another source of funds, in a high interest rate environment. By contrast, high rate shares are rarely withdrawn early when rates drop.

4. Corporates with derivatives authority may hedge their IRR exposure by a variety of instruments. For example, a corporate might purchase a put option or an interest rate cap. In either case, a corporate pays an initial fee in cash and may later receive cash (back) if interest rates increase sufficiently beyond a strike price or threshold level. The cash outflow precedes any later potential protection and cash inflow.

From a financial perspective, management must recognize that an asset/liability structure capable of controlling IRR does not necessarily generate an adequate cash flow.

Finally, cash flow relates to capital management. Corporates operating with significant levels of reserves and undivided earnings do not have the same cash flow pressure as highly leveraged corporates. For example:

1. Capital accounts generally do not have a stated maturity. No return of capital is required.

2. Dividend payments on contributed capital (member capital) and repurchase of member capital is discretionary. No return on member capital is specified (dividend is on an ability-to-pay basis). Paid-in capital may also be repurchased (called) on a discretionary basis but the dividend is more likely to be contractually specified.

These preceding statements cannot be interpreted to indicate capital is an entirely free source of funds. Management and shareholders expect capital to be used efficiently with good NEV appreciation and a satisfactory level of share dividends (remember members receive their return on investment through dividends on their shares as well as growth in NEV). However, the return need not necessarily result in a cash outflow as needed to pay contractual interest on debt and to repay contractual principal at maturity. Some shareholders prefer management retain earnings if the corporate is able to generate a high return on equity (better rates and services may result from a stronger capital base). It should be evident cash flow and liquidity management are integrally affected by a corporate's asset/liability structure.

Members' Role in Liquidity Management

Most corporate business is member oriented. Consequently, the role of borrower and shareholder must be understood clearly by a corporate if liquidity is to be managed. Examiners should recognize cash flow and liquidity requirements may differ among corporates based on the type of member relationships.

Corporates solicit shares from members and invest in high quality marketable securities or deposits. The least expensive funds a corporate receives are often derived from short-term shares. When members initiate and control short-term share behavior, liquidity management becomes more difficult. A corporate must be prepared to respond to an immediate surge in member withdrawals and/or demand for borrowed funds since it specifically serves that fiduciary role for its members. Corporates can only maintain longer term liquidity by obtaining longer term liabilities from members and storing it in assets that have cash convertibility (may be sold or pledged as collateral). If corporates have only short-term funds subject to immediate withdrawal, liquidity management requires assets be highly liquid.

While a corporate does not have to respond to the specific needs of each member, it must respond to aggregate shifts in which members' funds movement are not nullified in the aggregate. Differences in the growth rate of shares and the structure of investments may precipitate liquidity problems.

When a corporate mismatches overnight funds with longer duration assets and experiences withdrawals, it must shift the burden of liquidity management to the investment and funding operations conducted in the open financial markets. The corporate may have to draw down cash, sell securities, or borrow money. These actions may reduce observable liquidity (i.e., cash and short-term marketable securities) as well as less apparent liquidity (i.e., remaining borrowing capacity). When shares are growing, a corporate may be: receiving excess funds, replenishing cash, purchasing securities, and repaying borrowed funds.

Management's Responsibilities in Liquidity Management

A corporate must ensure sufficient liquidity is always available. Sufficient liquidity depends on the overall asset/liability structure of the corporate, the condition of the economy, the activities of financial service competitors, and the requirements of its own members.

An examiner must evaluate a corporate's cash flow and liquidity management to determine the following:

1. Reports measure the anticipated excess/deficient cash position of the corporate relative to member needs;
2. Policies that address how a corporate expects to manage its current and potential liquidity position; and
3. Pro forma financial statements that accompany a business plan reflecting adequate available liquidity to effect strategic change.

Liquidity management requires a corporate use sound financial and marketing techniques. The subsequent sections identify more fully the cash flow characteristics of assets, liabilities, and commitments within a corporate. The topics are addressed within a return/risk trade-off. These include:

1. Relative maturity schedules of assets and liabilities;
2. Options included in asset/liability products that complicate liquidity management;
3. Off-balance sheet commitments outstanding;
4. Interest income/expense associated with assets and liability products of varying liquidity; and
5. Operating expenses associated with products of varying liquidity.

A corporate needs cash and access to liquidity when needed, but not excessive cash or liquidity since earnings may be reduced.

Section 704.5(a)(2) of NCUA Rules and Regulations requires a corporate's investment policy address reasonable and supportable concentration limits for limited liquidity investments in relation to capital. Limited liquidity investments are defined as a "private placement or funding agreement." Since such securities do not trade as efficiently in the markets as public offerings, limiting their concentration is a prudent liquidity strategy.

Assets and Liquidity

Measurement

To maximize its net interest margin, a corporate should make adequate, but not excessive, liquidity provisions. Earnings and liquidity are often conflicting objectives. By making excessive provision for liquidity, management may forgo potential earnings. By making inadequate provision for liquidity, management could threaten the existence of the corporate.

Liquidity is a relative quality. There is a wide spectrum of relative liquidity in both assets and in liabilities. Asset liquidity may be measured two ways. First, how easily can an asset be converted to cash by sale in a secondary market or by using it as collateral to borrow money? Second, what certain cash flows will assets generate?

Marketability

Marketability allows a corporate to obtain cash prior to an asset's maturity. The liquidity of an asset is characterized by the speed with which a security can be sold at a price near the last trade. Liquidity is influenced by the asset's market depth, breadth, and resiliency. Deep, broad, resilient markets are liquid.

1. Depth is illustrated by the existence of orders above and below the price at which a security is trading. A deep market also may be characterized by a large order size for the best bid and best offer.

2. Breadth is illustrated by the existence of a substantial volume of potential investors. Broad markets are more stable than markets dependent on a few key investors when transitory order imbalances occur.

3. Resiliency is illustrated by the speed with which new orders occur from a price change or order imbalance. Liquid markets are characterized by small price impacts as a large order is executed in sequential transactions.

Asset liquidity (i.e., depth, breadth, and resiliency) is affected by the market in which it is bought and sold. Assets tend to be most liquid in auction and dealer markets, less liquid in broker markets, and least liquid in a direct-search market. Examiners should evaluate how management selects and monitors assets according to the market in which they trade.

Maturity and Duration

Maturity is a key attribute of relative liquidity of an asset. A short-term asset is inherently more liquid than a long-term one. The secondary market for U.S. Treasury securities is deep, broad, and resilient. Notwithstanding, longer term U.S. Treasury Bonds carry a risk of a larger loss than short-term U.S. Treasury Bills when interest rates increase. A corporate may be reluctant to record an accounting loss in its financial statements. Therefore, long-term securities are less likely to be converted to cash when interest rates increase, as they do during a period of economic expansion or inflation. Further, less cash is received from the sale of a long term bond after an interest-rate increase. Table 5, illustrates how the price of several bonds of different maturity might react to an interest rate change. Short-term securities may be considered liquid because they either mature quickly or may be sold with little loss given a minimal increase in required yields.

The potential price change of a security is heavily influenced by maturity. However, the percentage price change of a security is more closely related to its duration than maturity. Duration measures the time weighted cash flows of a security where the weighting is provided by present value. Short duration assets, not simply short-maturity assets, generally are more liquid than long-duration assets. The duration of an asset is shorter with a short-term maturity, high periodic interest or principal receipts and frequent cash flows.

Table 5

Security Price Change and Interest Rate Shift: Maturity

($1,000 Par, 8% Coupon Security)

Maturity	$ Price @ 8 %	$ Price @ 9 %	% Price Change
1 Year	$1,000	$990	1.0 %
5 Year	$1,000	$960	4.0 %
20 Years	$1,000	$908	9.2 %

Table 6 shows how the percentage price change of three bonds might react to a 1 percent increase in interest rates. The short-term maturity bond has the largest percentage price reaction because it has the longest duration. The maturity, the level of contract payments or coupon, and the payment frequency all affect asset liquidity. Duration provides a more comprehensive surrogate for cash flow than maturity. Either measure significantly affects the cash flow of assets. Examiners should evaluate how management measures and monitors the relative maturity and/or duration of assets.

Table 6

Security Price Change and Interest-Rate Shift: Duration ($1,000 Par)

Maturity	Coupon	$ Price @ 8 %	$ Price @ 9 %	% Price Change
7 Years	0 %	$ 534	$ 494	7.5 %
10 Years	8 %	1,000	935	6.5 %
12 Years	15 %	1,534	1,435	6.4 %

Credit Risk

Another factor affecting cash flow and liquidity management is the default risk of an asset. Assets with more certainty of return enhance liquidity. For this reason, default free securities, issued or guaranteed with the full faith and credit of the U.S. Treasury (e.g., U.S. Treasury bills, notes, and bonds and Government National Mortgage Association [GNMA] securities) are more liquid than similar securities that are privately issued. Next, securities issued or guaranteed by Government Sponsored Enterprises (GSEs) (e.g., Federal National Mortgage Association [FNMA], Federal Home Loan Mortgage Corporation [FHLMC], and Federal Home Loan Bank [FHLB]) are viewed as default remote).

Obligations of financial institutions (e.g., federal funds, certificates of deposit [CDs], and bankers acceptances), corporations (e.g., commercial paper or corporate bonds), and state and local governments (e.g., general obligation or revenue bonds) must be evaluated for credit risk.

An investment-grade bond suitable for providing liquidity means the security has low market and credit risk. As illustrated in Table 7, the top four letter grades assigned to corporate bonds by Moody's Investors Service and Standard & Poor's Corporation are defined to indicate a level of credit risk.

Table 7

Credit Quality and Rating Grades

Moody's	S&P	Credit Quality
Aaa	AAA	Prime Quality
Aa	AA	High Grade
A	A	Upper Medium
Baa	BBB	Medium Grade

The differential in yield and risk is most pronounced between the third and fourth grades. If a medium grade bond is downgraded to Ba or BB, the market no longer considers it investment quality. In general, a corporate may not retain low-grade bonds. However, there are some circumstances under which a corporate may be able to retain a low-grade security. For example, depending upon the individual corporate's expanded and/or operating authority level, and the specific security, Section 704.10 (Investment Action Plans) provides for the possibility of retaining low-grade securities. For the most part, corporates are limited to high-grade instruments which afford the greatest relative liquidity within the credit risk spectrum.

Investment-grade corporate bonds do default. For example, Johns Manville, LTV, and Braniff, among many other issuers, have defaulted on their bonds even though they were each once assigned a single-A or better grade. Recent market events also proved that highly rated securities (AAA) can be downgraded to non-investment grade very rapidly, thus greatly reducing their liquidity. There is a distinct difference in credit quality and yield between a prime quality bond (AAA or Aaa) and a medium-grade bond (BBB or Baa).

Liquidity from cash flow requires assets to have not only a short duration but low credit risk. Management must set limits on the credit risk exposure of its assets. Securities with high credit risk are more likely to have cash flow problems. By definition, low-grade corporate bonds have a higher probability of default and, therefore, could suffer an interruption of cash flow.

Most corporates have some credit exposure that results from corporate bonds, commercial paper, asset-backed securities, federal funds sold, or certificates of deposit from insured banks. The FDIC periodically has favored a policy under which uninsured shareholders face losing a portion of their funds when a troubled bank is liquidated. Banks traditionally had a low rate of failure, compared with other industries, until the early 1980s. Although economic factors affect bank liquidation, variations in operating performance usually can be traced to management. Ratios that measure the financial condition and operations of a bank have been found to have limited predictive power to discriminate problem and failed banks from sound institutions.

Uneven earnings are a key factor indicating the riskiness of a commercial bank. An approved list of acceptable commercial banks should be based on financial ratios and should incorporate some analysis of the accompanying risks. A simple method of managing credit risk of banks by corporates is to restrict investment to the insured portion. Such a strategy may not be practical for larger corporates.

Each corporate with uninsured bank deposit exposure should establish, monitor, and update an approved list of accepted commercial banks. The approved list should include commercial banks displaying adequate capital, consistent earnings, acceptable credit quality, prudent growth, and multiple sources of liquidity. The list should be reviewed at least annually (quarterly for banks where large demand deposits, federal funds sold, or CD exposure exist).

Liquidity risk and credit risk are highly correlated. Examiners should see how management categorizes its assets according to credit risk and classification standards.

Prepayment

All corporate institutions investing, trading, or selling MBS must be concerned with the anticipated life of such instruments. Prepayments affect the investment life, pricing, earnings, and value of loans. Prepayments also affect cash flow. Loans prepaying provide a cash flow earlier than scheduled amortization.

A mortgage may be prepaid due to a variety of factors, including:

1. Seasoning - when mortgagors have paid their mortgage for several years and are more likely to seek a new home or to refinance;
2. Refinancing - when mortgagors are able to obtain a new loan at least 150-200 basis points less than their existing contract rate;
3. Default - which tends to remain high until a fixed payment loan is seasoned with three years or more of satisfactory payments; and
4. Disaster - which may occur from destruction of the property by fire or flood, or from death or disability of the owner.

Prepayment experience also is affected by legal, geographic, and seasonal factors. For example, GNMA securities backed by FHA/VA loans tend to prepay more slowly than other agency pass-through securities because the FHA/VA mortgages historically are less mobile and the underlying loans are smaller; therefore, there is not as great a dollar incentive to refinance. Similarly, certain geographic areas that experience growth, high professional employment mobility, property value appreciation, or retirement migration patterns also prepay more quickly. Variations in a region's economic base can change prepayment activity. Finally, the peak housing activity during the spring and summer months translate directly to prepayment seasonality.

Long-term corporate bonds with embedded options are also subject to prepayments. A call option allows a bond's issuer to retire a bond prior to maturity. Calls are often exercised when interest rates have declined and allow the issuer to refinance the debt prior to maturity at a lower coupon than currently being paid. A put option allows an investor to resell the bond to the issuer, typically at par, prior to maturity should interest rates increase. Calls are very similar to prepayments of mortgage-backed securities (MBS); a corporate receives (back) cash when it is least advantageous to reinvest the proceeds.

As illustrated in Table 8, the relative cash flow and liquidity of assets vary according to a continuum. As management invests in more liquid assets, interest income tends to decline.

Table 8

Asset Liquidity Characteristics

Attribute	Most Liquid	Liquid	Least Liquid
Maturity	<1 Year	<5 Years	>Than 10 Yrs.
Coupon	High	Low	0
Payment Frequency	Monthly	Semiannual	No Coupons
Credit Risk	U.S. Treasury/ Agency	Top 4 Grade	Low Grade
Market	Auction/Dealer	Broker	Direct Search

Management Considerations

A corporate should increase its asset liquidity, short-term, default free or remote, and highly marketable securities when other parts of asset/liability structure are less liquid or place uncertain liquidity demands on the corporate. For example, strong financial arguments exist to increase the proportion of liquid assets when the amount of:

1. Long-duration assets (e.g., zero-coupon bonds) increase;
2. Fixed assets (e.g., equipment, furnishings, or real estate) increase;
3. Assets trading in a broker market (e.g., derivative MBS) increase;
4. Lines of credit or standby letters of credit issued increase;
5. Assets available for pledging against a liability are few;
6. Capital is low or negative and member confidence is threatened;
7. Funding by short-term brokered CDs or uninsured CDs increases;
8. Funding by repurchase agreements or dollar rolls increase;
9. Funding by collateralized borrowed money increases;
10. Hedging with interest rate futures increases; or
11. IRR, as measured by NEV, increases.

Corporates should commit relatively more funds to highly liquid assets whenever the following occur:

1. A large portion of other assets are less marketable or have distant cash flows;
2. Liabilities or shares are subject to disintermediation;
3. Significant commitments to purchase securities or originate loans are outstanding;
4. Little additional access to the financial markets is likely; or
5. Market and member confidence is threatened.

More liquid assets may be used to balance the risk of other financial assets or financial liabilities that are designed to enhance earnings, yet carry more risk.

Such an investment strategy mitigates some of the liquidity pressure otherwise present. The earnings penalty incurred by investing in liquid assets often is offset by other illiquid assets with a long duration, little marketability, or high credit risk exposure that carry higher yields. Further, short-term liabilities and wholesale shares often cost less than longer-term accounts and also may offset the earnings penalty from the additional investment in liquid assets.

Management need not only increase the proportion of short-term, default free assets to enhance liquidity. Liquidity carries a potential earnings penalty. The following are examples of how a corporate can enhance liquidity, while not increasing its investment in short-term, default free instruments:

1. Emphasize core member accounts and intermediate-term shares;
2. Emphasize securities that have predictable, consistent, and homogeneous prepayment or call risk;
3. Maintain assets suitable for pledging against a wholesale corporate advance or a reverse repurchase agreement;
4. Maintain an unused line of credit with a wholesale corporate or a commercial bank;
5. Emphasize securities that are similar to products trading in dealer markets (e.g., MBS or public agencies); or
6. Sell and lease back the corporate's office building.

Liquidity management allows a corporate to respond to anticipated or unanticipated cash flow deficiencies. Liquidity management must consider the entire asset/liability structure.

Liabilities and Liquidity

<u>Measurement</u>

Member - initiated sources and uses of funds provide the foundation for liquidity risk management. When loan demand exceeds normal share growth, management must rely on access to borrowed money or the sale of securities to raise needed cash. Similarly, corporates may reduce reliance on borrowed money and increase temporary investments when the reverse occurs.

A corporate has several alternatives to raise cash through liability management.

Like assets, maturity is a key to relative liquidity. However, reliance on short-term liabilities requires more liquidity than reliance on long-term liabilities. Members have the legal right to withdraw funds or force repayment at maturity. Liquidity risk is increased when management relies on three-month certificates rather than three-year certificates. Liquidity risk is also increased when management relies on short-term borrowing as opposed to longer term advances. Shorter-term liabilities increase liquidity risk. Such liabilities also tend to cost less since they should be priced off the short-term end of the yield curve.

Some share accounts may be withdrawn immediately, or on demand, yet do not necessarily cause an increase in liquidity risk. Although a specific member may withdraw funds immediately, another member may reinvest a like amount of funds. A corporate does not have to respond to the specific needs of each member; it must respond to net aggregate shifts in shares. Clearing accounts may provide a corporate with a very long-term source of funds because members must maintain constant balances to cover daily settlement activities. The account may be considered a core share. Core shares are extremely important when measuring liquidity risk. Core shares are placed by members for reasons principally related to the financial services and the convenience offered by the corporate, rather than simply the interest rate paid. A corporate will lose core shares over time if services or dividend rates become non-competitive. In addition to clearing accounts, membership capital shares and paid-in capital, a portion of regular overnight shares, and share certificates may be considered core shares if supported by proper analysis. The use of early prepayment penalties also helps enhance liquidity as certificate holders will not be as quick to withdraw the funds when it requires foregoing income.

By contrast, other shares require more liquidity because investors have selected a specific account and a specific corporate for one reason, it offers the highest rate of interest. When management posts a lower rate, volatile, or wholesale funds disappear. Volatile liabilities increase liquidity risk. However, a corporate temporarily may meet liquidity needs by posting high interest rates. Management and examiners should distinguish core shares from volatile shares.

Many core share accounts carry high average operating expenses and low share balances. Corporates may more quickly raise desired amounts of funds through the wholesale share market or by borrowing money.

Each corporate must determine for itself whether the advantages of borrowed money exceed the attendant costs. One of the constraints that limits the advantage of borrowing funds is the minimum capital ratio (borrowed funds grow the balance sheet and increase the assets relative to capital). Examiners should review the corporate's related calculations.

Although most corporates choose not to borrow funds, borrowing can be an attractive funding alternative to regular shares. Therefore, a corporate should establish multiple borrowing sources to ensure a source is available when needed. Even when the borrowed money carries higher interest rates than shares, the interest expense is limited to the incremental funds raised, not total funds. An arithmetic example illustrates the difference. Assume a corporate needs to quickly increase cash by 10 percent. In order to acquire the new funds, the corporate believes it must post higher interest rates for all of its share products by 1/8 of 1 percent. For each $10 million of total shares, interest expense thereby increases $12,500 annually. The incremental interest incurred amounts to 1.25 percent for the desired $1 million (10 percent of the $10 million shares). The desired growth could have been more cheaply obtained by borrowed money if its cost was no more expensive than 1.25 percent above the current share rate. Table 9, illustrates various combinations of incremental interest rates needed to attract share funds and targeted growth. The indicated values show how much extra a corporate could pay for borrowed money than shares and break even.

Table 9
Borrowed Money Break-Even Analysis

Incremental Share Rate	Funding Growth		
Increase to Obtain Growth	5%	10%	15%
1/8 of 1%	2.5%	1.25%	.83%
1/4 of 1%	5.00	2.50	1.67
1/2 of 1%	10.00	5.00	3.33

The interest rate differential that can be paid and still break even for borrowed money increases when the corporate otherwise needs to post a higher rate for all savings, or the amount of incremental growth is relatively small. Borrowed money is best viewed as a source of incremental funds to meet liquidity needs.

Management Considerations

Corporates may generate cash flow and manage liquidity through shares and borrowed money. The corporate system's ability to attract shares is also affected by factors external to the actions of a specific corporate. These include:

1. Economic growth and regional booms (loan growth uses up excess liquidity);
2. Decline in personal savings ratios for members of natural person credit unions;
3. Perceived strengths and weaknesses of the corporate credit union system; and
4. Competition from other financial institutions, including other corporate credit unions.

If management has a specific need for funds, a corporate may need to borrow money to obtain cash.

There are a wide variety of specific liabilities corporates may use. Rather than describe each one, the following listing categorizes types of financings that may be used to generate cash:

1. Repurchase Agreements/Dollar Rolls: by selling securities through a reverse repurchase agreement or a dollar roll, the corporate sells a security and simultaneously agrees to purchase the same or a similar security at the end of the agreement (e.g., a week or month).

2. Commercial paper: by issuing commercial paper, the corporate raises non-insured funds from investors, typically with a maximum maturity of 270 days. Some corporates keep a constant amount of commercial paper issued to maintain a market presence.

3. Medium-Term Notes (MTN): by issuing an MTN in the marketplace, the corporate raises funds from investors for several years.

More specialized securities provide for specific cash flows to appeal to certain investors. However, more specific cash flows limit the subsequent marketability of an issue unless information is easily available about the cash flows and the issue is similar to others. A corporate should be concerned with the secondary market of its liabilities because more marketable securities carry less risk to investors and thereby reduce the interest cost. For this reason, a $100 million liability issue may carry a five basis point lower cost than a $50 million issue. Management should have a plan for accessing borrowed money over time. Examiners should review the plans to ensure there is adequate liquidity, and other risks involved with procuring sufficient liquidity are addressed and do not negatively impact the asset/liability structure. Liquidity management is also affected by the existence of commitments and hedging instruments.

Commitments and Liquidity

Corporates often own assets and acquire shares with options that complicate cash flow planning. Table 10 illustrates the cash flow consequence of a change in interest rates for these accounts.

Rising interest rates affect assets and liabilities. Therefore, the corporate may have to search for more sources of cash when it is least desirable. (i.e., during a period of high rates). Options made available to members greatly complicate cash flow planning.

Hedging may partially offset IRR and some liquidity risk. Hedging does effect the cash flows of a corporate. Hedging may increase the perceived liquidity of an asset because the transaction reduces the corporate's reluctance to sell an asset at a loss. The hedge should provide an approximate offsetting gain.

Table 10

Cash Flow and Interest Rate Change*

Account	Option	Effect of Rising Rates	Effect of Falling Rates
Corporate Bond	Call Feature	No Call	Call (+)
Term Share	Early Withdrawal	Withdrawn(-)	No Change

*(+) Cash Inflow; (-) Cash Outflow

Asset/Liability Structure and Cash Flow

Cash Budgeting

Corporates should develop pro forma cash budgets to ensure cash and liquidity will be available in the future. The uncertainty created by MBS prepayments, fixed-rate commitments and share withdrawals reduce the confidence of a cash budget being realized. Therefore, examiners should determine how management anticipates cash flows in the future.

Section 704.8 (ALM): Interpretation and Examples

Prudent risk managers view regulatory requirements as a *minimum* standard. Examiners should expect corporates' risk managers to manage to best practices, not the regulation, as long as those practices do not contradict or ignore regulatory requirements. Where appropriate, a corporate will need to develop additional tests, methodologies, and procedures to manage its risk (additional means beyond the minimum requirements of regulation). Corporate management may fail its basic fiduciary responsibilities if it limits its risk management to only regulatory compliance.

ALM policies may be integrated with the investment policies (or vice versa). In addition, it is acceptable to have all financial risk policies combined into one source so long as the unique considerations of each area are addressed and the respective procedures are in place.

Section 704.8(a) addresses the ALM policy requirements for corporates. Note that it uses the term "at a minimum" in describing policy stipulations.

1. The purpose and objectives of the policy should be consistent with the risk tolerance and risk management philosophy of the organization. The examination review will need to consider if management's actions and performance are consistent with this statement.

2. The policy must address the tests that will be used to evaluate investments prior to purchase. This requirement is integral with the investment policy (prudent portfolio

selection criteria would automatically require this discipline). Corporates have an obligation to develop appropriate criteria for investments. Testing can estimate the impact of a credit migration or default. Analysis of creditworthiness includes probability of default in various scenarios. Testing may also measure the relative liquidity for a type of transaction (depth of market and price risk). Additionally, the effect of a purchase on overall liquidity measurement limits should be addressed. The type of tests required will be a function of an investment's complexity, structure, and/or acceptance in the general marketplace. Before a corporate can buy/sell a new investment type (new in the market or new to the corporate), it must develop appropriate analyses and test parameters and modify its ALM policy *before* engaging in the activity. The type of investments will determine the types of tests that are appropriate. For example, a shock test would not be expected for an overnight Fed Funds transaction although the credit analysis of the counterparty would be expected. Interest rate stress tests would be required for instruments such as structured share certificates or mortgage-backed securities.

3. The policy must address the maximum allowable percentage decline in NEV, compared to base case NEV. A simple example of how this information can be communicated is provided in Table 11.

Table 11

	Maximum Permissible Change in:	
Change in Interest Rates (in basis points)	Net Economic Value (Board Limit)	Net Economic Value (Regulation)
+300	-13.0%	-15%
+200	-10.0%	-15%
+100	-5.0%	-15%
0	-	-
-100	-5.0%	-15%
-200	-10.0%	-15%
-300	-13.0%	-15%

almtbl01

4. The policy is required to include the minimum allowable NEV ratio. Corporates are required by Section 704.8(d)(1) to limit risk exposure to: (1) levels that do not result in a base case NEV ratio or any NEV ratio resulting from the tests…below 2 percent; and (2) levels that do not result in a decline in NEV of more than 15 percent.. The board is expected to prescribe the corporate's NEV policy limit within the regulatory limit. An example of how this information might be presented is included in Table 12.

The effect on NEV of an adverse change in market rates (measured with rate shocks) is measured relative to the size of the estimated present value of the corporate's assets. Thus, the NEV ratio is defined as NEV divided by the fair value of assets, or:

$$\text{NEV Ratio} = \frac{\text{NEV}}{\text{FV}_{\text{ASSETS}}}$$

Table 12

Interest Rate Scenario

	- 300 BP Change	Base Case	+ 300 BP Change
Present Value of Assets	$104	$100	$80
Present Value of Liabilities	-99	-97	-78
NEV	5	3	2
NEV Ratio	4.8%	3.0%	2.5%
Minimum NEV Ratio Policy Minimum	2.0%	2.0%	2.0%

5. The policy must address limits and specific test parameters for the IRR simulation tests set forth in Section 704.8(d) which deals with rate shock analysis relating to NEV and the NEV ratio.

   These factors have already been addressed by 3 and 4 above. However, corporates are also required by Section 704.8(d)(2) to assess annually if it should conduct periodic additional tests to address market factors that may materially impact the corporate credit union's NEV. The factors should include, but are not limited to the following:

   1. Changes in the shape of the Treasury yield curve;
   2. Adjustments to prepayment projections used for amortizing securities to consider the impact of significantly faster/slower prepayment speeds;
   3. Adjustments to the market spread assumptions for non Treasury instruments to consider the impact of widening spreads;
   4. Adjustments to volatility assumptions to consider the impact that changing volatilities have on embedded option values.; and
   5. Changes in market spreads.

   The regulation does not establish specific targets or ranges for these extra tests. It is the responsibility of the board to: (1) decide how these tests should be conducted; (2) determine the frequency of the additional tests; and (3) place appropriate parameters and limits upon exposures to these particular market risks. Parallel, instantaneous and sustained shocks in the yield curve address a majority, but not all, potential market risks. Rate shocks do not capture the full spectrum of market risks and additional tests are intended to provide a more rigorous assessment. For example, a change in market volatility is not captured in a rate shock and significant value changes in options could therefore be missed.

The examination review of this area must consider the relevance and appropriate frequency of the additional tests and determine if the limits appear consistent with the overall board philosophy on risk. For example, if a corporate portfolio has no prepayment optionally to speak of, tests for prepayment changes would be meaningless. If, on the other hand, a corporate portfolio is heavily weighted in asset-backed securities (or some other non-Treasury "spread" product), the test for changes in market spreads will be essential.

Certain market indices (e.g., LIBOR, PRIME, COFI and CMT) serve as references for computing periodic interest payments on structured share certificates and securities. When buying instruments that contain interest coupon payment formulas tied to market indices, the corporate needs to obtain reasonable projections for future index levels. This is necessary to compute NEV for the various interest rate tests. Corporates are expected to place greater attention on projections of those indices which are not market determined rates (such as PRIME and COFI). Correlation analyses, which demonstrate the relationship between the non-market indices and market rates, is a major component of most index forecasts.

ALM Examination Objectives

The objectives of the ALM review are to:

1. Determine if policies, procedures, and strategic plans regarding cash flow and liquidity management adequately address safety and soundness, earnings, and compliance with laws and regulations.

2. Determine if the corporate has complied with the regulatory liquidity measurement and monitoring requirements of Part 704. Determine liquidity management evaluates: the potential liquidity needs of members; regularly monitors sources of internal and external liquidity; and sets accounting classification of securities consistent with potential liquidity demands.

3. Determine if the contingency funding plan adequately addresses alternative funding strategies in successively deteriorating liquidity scenarios, and assumptions utilized are reasonable and supportable.

4. Determine if reasonable parameters have been established for the corporate's NEV position, the corporate is operating within established parameters, and the parameters are reasonable.

5. Identify weaknesses in the IRR measurement systems, internal management reporting, or internal controls.

6. Evaluate plans for reducing excessive IRR, if applicable.

7. Evaluate management of the corporate's assets and liabilities.

8. Determine if internal management reports provide the necessary information for informed funds management decisions and for monitoring the results of those decisions.

9. Initiate corrective action when ALM policies, procedures, practices, and internal controls are deficient.

ALM Examination Procedures

See Corporate Examination Procedures - Asset/Liability Management (OCCU 202P and OCCU 202.1P).

Corporate Examination Questionnaire

See Corporate Examination Questionnaire - Asset/Liability Management (OCCU 202Q and OCCU 202.1Q).

References

1. NCUA Rules and Regulations (Section 704.8)
2. Regulatory Handbook, Thrift Activities (OTC) Volume II
3. Comptrollers Handbook, Interest Rate, Funds Management
   http://www.occ.gov/handbook/FundsMgt1.pdf
4. Comptrollers Handbook, Liquidity
   http://www.occ.gov/handbook/liquidity.pdf

Appendix 202A

MORTGAGE-BACKED SECURITIES AND MORTGAGE-DERIVATIVE PRODUCTS

Introduction

The advantages of selling mortgages in securities have attracted a large number of mortgage lenders who have a wide range of objectives. The result is a variety of mortgage security types and an uncertainty about the differences between the securities and how they impact an investment portfolio.

History of Mortgage Security

Mortgage securities are not recent innovations. High rates of default on mortgage bonds during the depression inhibited widespread use of these instrument until the introduction of the Government National Mortgage Association (GNMA) pass through security in 1970. Even with the federal government guarantee, there was considerable skepticism about accepting mortgage securities in the investment community when GNMA first issued its securities.

The mortgage-backed securities (MBS) that were first introduced by GNMA in 1970 were limited to Federal Housing Administration (FHA) and Veteran's Administration (VA) mortgages. Conventional lenders had indirect access to the capital markets only through the Federal Home Loan Mortgage Corporation (FHLMC) beginning in 1971. Originators could sell mortgages to FHLMC at which point FHLMC pooled and sold the resulting securities as Participation Certificates (PCs).

In 1981, FHLMC began a swap program that allowed lenders to exchange conventional mortgages for pass-through securities. In the first FHLMC swap of mortgages for securities, no cash exchanged hands. The seller received payment in the form of PCs representing ownership in the mortgages sold. The lender, in this exchange or swap of assets, believed that its low-rate mortgages could be sold more easily and at a higher price in security form than in mortgage form.

The restructuring of mortgage portfolios that began in the early 1980s was the major factor in the rapid growth of conventional mortgage securities. FHLMC formalized its program in 1981 with its first swap program, Guarantor I, and the Federal National Mortgage Association (FNMA) soon followed with its Mortgage-Backed Security program. FNMA, FHLMC, and GNMA all collect a small guarantee fee throughout the life of the mortgages for the service.

As the mortgage securities market grew, lenders recognized that the swap programs provided an attractive alternative for mortgage sales. In addition, many lenders began to securitize their portfolio mortgages to add value and liquidity to their mortgage investment portfolios.

Types of Mortgage Securities

The term mortgage security describes a variety of mortgage-related instruments. Although characteristics can vary widely, there are only two basic types of mortgage securities:

1. A certificate representing ownership of an undivided interest in a proportionate share of each mortgage in a pool, referred to as a mortgage pass-through security or a mortgage-backed security (MBS); or

2. A debt obligation secured by a specified pool of mortgages, referred to as a mortgage-derivative product (MDP).

Within each type, variations have been designed to appeal to certain investor classes or to reduce the cost of security financing. These variations may be categorized according to the manner and terms of payments made to security holders.

<u>Mortgage-Backed Securities (MBS)</u>

The MBS is attractive to investors because of its high value relative to individual or pools of mortgages and because of its ease of trading or liquidity. The price advantages for MBSs are due to the guarantees FNMA, FHLMC, and GNMA place on their mortgage securities. Investors are willing to pay for these guarantees, and the higher prices cover the seller's costs of converting the mortgages to securities and the guarantee fee.

The structure of an MBS is determined by the following characteristics:

1. types of mortgages in the pool;
2. weighted average coupon (WAC) on the pool of underlying mortgages;
3. pass-through rate on the MBSs;
4. weighted average maturities (WAM) of the mortgages;
5. number and size of the mortgages; and
6. geographic distribution of mortgages.

The Pass-Through Rate. - The pass-through rate is the net interest rate passed to investors. The WAC of the mortgage pool is an important factor in determining the speed at which prepayments will occur. In general, the higher the WAC in relation to current mortgage rates, the higher the prepayment rate since homeowners could refinance at lower interest rates. The lower the WAC to current mortgage rates, the lower the prepayment rate since homeowners could not readily refinance at lower rates.

Interest rates on the mortgages underlying an MBS are typically greater than the coupon rate, or pass-through rate, with any excess over the coupon, guarantee fee, and servicing fee going to the servicer. Each issuer can set limits on the permissible range of interest rates in a pool within the limits established by the guarantor of the MBSs for each specific program.

The Weighted Average Maturity. - The WAM determines the rate of the scheduled repayment of principal. The longer the maturity, the more time over which the principal is amortized and, therefore, the less principal is scheduled to be passed through in the early years of the security. The maturity date of an MBS is generally stated to be the date on which the last mortgage in the pool is due to be repaid in full, but all of the mortgages need not mature on the same date. Each guarantor of an MBS sets limits on the permissible range of maturities for each specific program.

Geographic Distribution. - This is the location of the properties securing the mortgages. The location of the mortgages comprising the pool is important because it affects the likelihood and predictability of prepayments. Different areas of the country prepay at much different rates. Geographical diversity results in greater predictability of cash flows, since the total of the mortgages pooled would be less subject to local disasters or other kinds of local influences. In addition, the greater the number of mortgages in a given pool, the more regular and predictable its cash flow is expected to be.

Payments to Investors. - The payments for MBSs are designed to resemble mortgage payments but without delinquencies. Principal and interest payments, less guarantee and servicing fees, are passed through to the investor whether or not they are collected. Delinquencies are advanced by the servicer to the investor until the mortgage either becomes current or foreclosure is completed. Prepayments are passed through to the investor as received.

The servicer collects mortgage payments on a monthly basis from the mortgagor and remits those funds less its servicing fee to a central collection point, or directly to the investors for GNMA I. FNMA, FHLMC, and GNMA II collect their guarantee fee either directly from the payments that are passed through them or from the servicer.

MBS Guarantee. - FNMA and GNMA have always guaranteed the timely payment of both principal and interest to investors for their MBSs, requiring the servicer to advance its own funds to the investor to make up for delinquencies. FHLMC only guaranteed the timely payment of principal until their Gold PC was developed and now they, too, guarantee the timely payment of both principal and interest. These organizations, however, do not generally become involved in the payment process unless the servicer fails to remit all scheduled principal and interest.

MBS Yields and Prices

Calculating yields for MBSs requires present value analysis, which discounts the future cash flows of the mortgages by the required rate of return. This process calculates an MBS's present value or estimated market value. Alternately, given a market price, it is possible to determine the rate of return or yield that would cause the sum of the discounted cash flows to be equal to the market price. Two common measures of yield are described below; the cash flow yield and the option adjusted yield.

Cash Flow Yield. - The cash flow yield (also referred to as static yield) of an MBS will discount the sum of all future cash flows back to the current market price. To calculate the cash flow yield, the current market price of the security must be obtained and future cash flows must be projected. Because homeowners have the right to prepay their mortgages before their contractual maturity, the timing of future cash flows is uncertain and must be estimated. A prepayment rate estimate is usually made on the basis of the prepayment experience of a similar MBS and incorporated into the analysis.

The cash flow yield assumes the cash flows will occur as estimated. Actual prepayments may be greater or less than projected depending on many factors, most importantly, the future course of interest rates. Falling interest rates would induce homeowners to prepay their mortgages and refinance them at the new lower rate. Increasing interest rates would influence homeowners to hold onto their mortgages, which would then have below-market rates. The cash flow yield, however, does not take this uncertainty concerning the future course of interest rates, and therefore, prepayment rates, into account. Although the cash flow yield may be an adequate yield measure for many purposes, it may not be as accurate as the option-adjusted yield method described below.

Option-Adjusted Yield. - The option-adjusted yield method can provide a better yield estimate on an MBS than the cash flow yield because it usually better estimates the cost of the embedded prepayment option. Instead of relying on a single prepayment estimate, the option-adjusted yield is calculated by solving the yield equation many times, each time assuming a different rate of prepayment. The resulting yields are averaged to obtain a single yield estimate. Because it relies on an entire distribution of possible estimated prepayment rates instead of a single estimate, the option-adjusted yield is usually a superior measure of the yield of financial instruments with embedded prepayment options.

Stripped Mortgage-Backed Securities (SMBSs)

In 1986, FNMA issued the first SMBS which created two new classes of investors or security holders. Each class was entitled to a percentage of the principal and interest payments from either the MBS or whole mortgages that served as the underlying collateral. For example, one class of the SMBS may receive 99 percent of the interest payments and 1 percent of the principal payments from the underlying MBS. Investors in different classes (tranches) of SMBSs have purchased a derivative mortgage instrument that has significantly different characteristics from the underlying mortgages or the MBSs.

In 1987, FNMA introduced an SMBS comprised of an interest only (IO) class and a principal only (PO) class. The holder of the IO was entitled to all of the interest payments from the underlying MBS while the holder of the PO was entitled to all of the principal payments. The I0s and POs quickly became the most widely used types of SMBSs and today represent the greatest percentage of the dollar value of SMBSs issued.

Investment bankers have also created their own version of SMBSs both through private placements and public offerings. The private placement is normally created through a participation agreement that entitles the holders to a certain predefined percentage of the principal and interest payments from the underlying mortgages or the MBS. These private placements are similar to the original FNMA SMBSs in that holders are entitled to varying percentages of the principal and interest payments rather than a percentage of all of the interest or principal. In addition, FHLMC issues its own version of I0s and POs using PCs rather than MBSs.

Mortgage-Backed Bonds

An earlier innovation that is not as prominent today are mortgage-backed bonds. A straight mortgage-backed bond is an obligation secured by a pool of mortgages. Similar to a secured corporate bond, the mortgage-backed bond has periodic interest payments and principal repayment at maturity. Bonds may also provide for sinking fund payments during the term to accumulate sufficient funds to pay off the bonds at maturity.

A standard mortgage-backed bond is secured by a lien against the mortgages in the pool. The holder looks first to the issuer for principal and interest payments and only to the collateral mortgages in the event of default. Because straight mortgage-backed bonds do not pay down like mortgages with a regular amortization of principal, but repay principal at maturity, the issuer is required to pledge collateral in excess of the face value of the bonds. This overcollateralization is necessary to protect against any decline in the market value of the mortgage collateral that may occur as a result of changing market conditions over the life of the bonds.

Pay-Through or Cash Flow Bonds

A pay-through or cash flow bond is a bond secured by the cash flows from a mortgage pool and, as such, does not represent an ownership interest in the mortgages. A pay-through bond may be viewed as a hybrid security, combining the features of a traditional mortgage-backed bond with those of a pass-through security. Pay-through bonds are designed to amortize in the same manner as mortgages, with principal and interest payments that mirror the actual collections on the collateral pool. The bonds mature as the mortgages in the pool repay unless the terms of the issue provide for a different maturity based on guarantees from the bond issuer.

A pay-through bond usually requires significantly less collateral per bond dollar than a straight mortgage-back bond because principal is paid to the investor as the underlying mortgages amortize. Pay-through bonds are structured so that the mortgage collateral will generate a sufficient cash flow to provide full and timely repayment of the bonds. Reliance on the cash flow of the collateral pool also substantially eliminates the need for the investor to look to the creditworthiness of the issuer. Pay-through bonds may be issued through limited purpose subsidiaries with no other significant assets apart from the pledged mortgages.

Collateralized Mortgage Obligations (CMOs)

Although standard pay-through bonds look much like pass-through securities in the schedule of payments, some variations have been developed to appeal to a broader range of investors. The most familiar type of pay-through bond is the CMO, first issued by FHLMC in 1983.

The CMO is actually a serial pay-through bond, combining a series of maximum bond maturities in a single issue. The advantage of a CMO is the prioritization of cash flows from the mortgage pool, which creates many classes of investors. This produces securities of several maturities and allows the issuer to attract investors who might not otherwise invest in a mortgage security.

Yield. - Like mortgage investors, CMO investors demand higher yields than other investments of similar quality and maturity because the actual life of the bond and, therefore, the actual yield to maturity is not accurately predictable. However, CMOs may offer more predictability of prepayments than mortgages or other types of mortgage-backed bonds because of the large collateral pools backing each type of issue and the prioritization of cash flows.

CMOs have large numbers of mortgages in each collateral pool and offer three or more investor classes, called tranches, of varying maturities and yields. Each investor class generally receives monthly interest payments on the outstanding principal balance of its class. In a “vanilla” sequential payment deal, principal payments are allocated to each investor class in the order of earliest maturity. The shortest outstanding maturity receives all principal payments until that class is fully retired, then holders of the second class begin to receive principal payments, and so forth. More complex deal structures, in which principal may be directed to one or more classes and in which payment priorities of tranches may change with changes in prepayment rates, are now common.

CMO yields and yield spreads over comparable Treasury securities are determined, in part, by the market’s assumption regarding the average life for each investor class. Thus, the weighted average term of the mortgages pooled significantly affects the assumed yield and the purchase price. As with mortgage investments, the actual prepayment of the mortgages will determine the actual yield to maturity.

Prepayment Rates. - Although CMOs are referred to as a generic group, the prepayment terms of CMO issues vary, as do the terms of other types of mortgage securities.

Most CMO issues have another feature that impacts the prioritization of cash flows. The compound interest or accrual class generally is the longest maturity and receives no interest or principal payments until all other investor classes have been retired. The accrual bond has a coupon rate that is compounded during the accrual phase and converts to an interest-paying instrument following retirement of all shorter maturity classes.

Planned Amortization Class. - A CMO innovation that became very popular in the late 1980s was the Planned Amortization Class (PAC). The PAC structure guarantees a pre-set payment stream. The increased certainty of these tranches causes other tranches in the issue to have more uncertain cash flows. The PAC class of tranche attracted many traditional bond investors into the mortgage security market.

Previous CMO Limitation. - A major initial drawback to widespread use of the CMO was the substantial size of the mortgage pool; $100 million or more, was necessary to support the cost of issuance. The advent of CMO conduits, however, made CMO issues feasible for smaller lenders. By pooling collateral supplied by a number of lenders, the conduit could achieve the economies of scale needed to make the issue cost effective for the lender. Only a few of the conduits have survived and, as a result, FNMA, FHLMC, GNMA, and investment bankers that all have access to large volumes of collateral dominate the list of issuers.

Issuers have become very innovative in designing new structures that respond to changing interest rate environments and cater to investor needs. CMOs are often a blend of the different maturities that characterize the traditional CMO with tranches that resemble stripped securities while other tranches create more bond-like classes.

Real Estate Mortgage Investment Conduits

Effective January 1, 1987, Real Estate Mortgage Investment Conduit (REMIC) legislation permitted various mortgage securities such as multiple class securities and regular pass-throughs to be treated as asset sales rather than as financing for accounting purposes. This allows issuers to show mortgage securities off the balance sheet which avoids the increasing financial statements normally caused by these securities. Thus, REMICs dramatically reduce capital needed to issue mortgage securities.

Adjustable-Rate MBSs

Issuing MBSs backed by adjustable-rate mortgages (ARMs) has provided an additional type of pass-through security in the secondary market. Normally, securities based on pools of ARMs have less interest-rate risk than securities based on fixed-rate mortgages. However, teaser rates and interest-rate and payment caps can make ARM securities less attractive for investors. Teaser rates are below-market interest rates that are offered to home buyers as an inducement to choose ARMs rather than fixed-rate mortgages.

ARMs often have periodic or lifetime interest-rate caps, or both. A typical ARM periodic cap with a coupon that adjusts annually would limit the increase or decrease in the coupon to no more than 2 percent per year. Lifetime caps are an upper limit to the level that an ARM coupon can reach at any time during the remaining life of the mortgage. In addition to interest rate caps, some ARMs have payment caps that limit the percentage change of mortgage payment changes at the reset date to no more than a given percentage.

Examiners should determine the extent to which corporates hold MBSs based on pools of ARMs with teaser rates, and interest-rate or payment caps resulting in below-market interest-rate loans. All future interest-rate adjustments are normally based upon the initial mortgage rate. If interest rates increase, an ARM would “cap out” (reach the maximum lifetime cap) at a lower interest rate than ARMs originated at current interest rates. For example, assume a 5 percent lifetime cap over the initial mortgage rate. If the market interest rate was 8 percent and loans were originated at 6 percent, the lifetime cap would be 11 percent rather than 13 percent. If a corporate has purchased a significant amount of adjustable-rate MBSs with teaser rates, profitability could be materially reduced.

To properly estimate the price sensitivity of adjustable-rate MBSs, the frequency of the interest-rate adjustment, the index, the initial interest rate, and the annual and lifetime caps must be considered. A corporate investing in adjustable-rate MBSs should determine the extent to which interest rates can increase before the cap is reached. Another consideration would be the index used. Cost of funds indexes tend to lag increases in interest rates. This lag could cause a serious decline in net interest income depending on how the securities were funded. For example, a corporate that had invested in adjustable-rate MBSs funded by reverse repurchase agreements would suffer in a rising rate environment, because the interest rates on the reverse repurchase agreements would adjust more rapidly that the interest rates on the adjustable-rate MBSs.

The prepayment experience of many adjustable-rate MBSs is high, since many mortgagors refinance into fixed rate mortgages with a small drop in interest rates. Prepayment is an especiallly important consideration when the securities were purchased at a premium (i.e., where a lagged adjustment of the index provides the investor with a yield higher than the current market yield).

Risks of Mortgage Securities

Each type of mortgage security allocates risk between issuer and investor in a different way. As a general rule, the more risk assumed by the investor, the closer the transaction is a transfer of ownership in the mortgage pool and the more compensation the investor will seek for the added risk. The more risk the issuer retains, the closer the security resembles debt financing.

The degree of market risk assumed by the issuer is directly related to the timing of principal remittances to investors. The more closely principal payments are tied to collections on the underlying mortgages, the less the issuer's reinvestment risk, while less frequent principal payments require the issuer to assume more reinvestment risk. Pass-through securities with minimal holding periods carry little reinvestment risk; however, straight bonds with principal payments at long intervals carry substantial reinvestment risk.

Pass-through securities transfer substantially all the risk and benefits of ownership of the underlying mortgages to the investor. Cash flows to the investor are advanced on virtually the same basis as collected, with minimal delays to allow for processing, reporting and related administrative functions. The investor is in substantially the same position as the mortgage holder with respect to uncertain prepayment rates.

The pass-through security carries an interest rate to the investor below the note rates in the underlying mortgage pool. The spread between the security rate and the mortgages provides the required fees to the servicer and to the agency that issues and guarantees the security. The issuer does not retain market interest-rate risk with pass-through securities because there are only small delays in the principal and interest cash flow to the investor. The risk of reinvestment passes to the investor of a pass-through security.

Under the terms of the FNMA and FHLMC mortgage swap programs and the GNMA II program, sellers can include mortgages with a specified range of note interest rates in a mortgage pool. Sellers can elect to pool mortgages with interest rates above the minimum required for the security and retain the excess as an additional monthly servicing fee. This additional servicing fee is called excess servicing. The servicer receives future excess servicing, but retains the corresponding risk that early prepayments will reduce its value.

Prepayment Risk

The most important characteristic in determining prepayment is the difference between the interest rates on the mortgages underlying the MBS and the prevailing mortgage interest rate. The more the underlying mortgage interest rate exceeds the prevailing mortgage interest rate, the greater the likelihood that refinancing will occur. If prepayments occur rapidly due to lower market rates, those declining market rates will make it harder for the investor to reinvest the prepaid principal at rates similar to the original mortgage interest rates.

Other factors affecting prepayments include the demographics of the area, the state of local economies, assumability of the underlying mortgages, and the time of year. A mobile population may result in significant prepayments as the houses are sold and the mortgages are repaid. If the local economy of a particular area is distressed, there may be a large number of foreclosures, which are equivalent to prepayments for the MBS. Prepayments are greater in the spring as individuals relocate. In the winter months, when housing sales decrease, prepayments are likely to be slower. Also, if the property is sold or destroyed by fire, flood, or some other disaster, the mortgage may be paid off early. Other factors, such as the relative age of the population, also affect prepayment rates.

Measuring Prepayments

The timing of principal repayment, or prepayment rate, is termed “speed.” There are a number of approaches to expressing prepayment speed estimates. Historically, Average Life Estimates or FHA Mortality Tables were used. Now, prepayment estimates are expressed in terms of constant prepayment rate or PSA speed.

Average Life Estimates. - The average life prepayment estimate assumes that all mortgages amortize exactly as scheduled with no prepayments for an average life (usually 12 or 10 years); and then all of the mortgages pay off at the same time. This approach was helpful in estimating yields, but not prepayments. The average life method of measuring prepayments has come to be viewed as extremely unrealistic and obsolete since the assumption of stable cash flows does not conform to the actual cash flows of the marketplace. Its use is generally discouraged.

FHA Mortality Tables. - The FHA experience method of measuring prepayment speed is based on the actual FHA prepayment experience. FHA Mortality Tables report the actual prepayments (both voluntary and as a result of foreclosure) during each year. Investors evaluate the performance of a particular pool relative to this FHA experience. The evaluation is expressed as a percentage of the FHA experience. For example, 0 percent FHA means no prepayments; 100 percent FHA means equal to FHA experience; and 200 percent FHA means the pool is paying twice as fast as FHA mortgages. The FHA experience for measuring prepayments works well for FHA and even VA mortgages; however, conventional mortgages prepay at different speeds and must be measured differently.

Constant Prepayment Rate (CPR)

The CPR was developed as a measurement that takes into account only principal payments in excess of those contractually required. The CPR method expresses annual prepayments as a ratio to the prior year’s outstanding principal balance. It includes only prepayments, not contractual amortization payments. Measurements of prepayments may also be expressed in terms of single monthly mortality (SMM), which reflects the percentage of outstanding principal balance prepaid each month.

Public Securities Association (PSA) Speed. The PSA formula is based on experience from conventional mortgages as tracked by the PSA. A 100 percent PSA speed means that prepayments are modeled as follows; .2 percent is prepaid in the first month of a mortgage, increasing by .2 CPR monthly to 6 percent CPR in month 30, and remaining at 6 percent thereafter through maturity. This is the basic PSA formula and prepayment speeds are expressed as a percent of PSA. Put differently, 100 percent PSA is substantially equivalent to 100 percent FHA experience or to 6 percent CPR (after the first 30 months), and 150 percent PSA is roughly equal to 9 percent CPR (after the first 30 months).

CMO Risks

CMOs, because they are structured to resemble either pass-through securities or pay-through bonds, may have risk characteristics similar to either, depending upon their particular terms. Generally, the CMO issuer assumes less interest-rate risk than the issuer of standard mortgage-backed bonds because remittance of both principal and interest payments is closely tied to the cash flows from the underlying mortgages.

The actual level of risk assumed by the issuer of a CMO will depend on two key characteristics of the security:

1. the frequency of principal and interest remittances to investors; and
2. guarantees, if any, as to the maximum maturity of each class of securities.

As with other pay-through bonds, delays in remittance to CMO investors subjects the issuer to reinvestment risk. To the extent earnings on the reinvested funds fall below expected yields, the overall cost to the issuer decreases. Guaranteed investment contracts can be arranged to lock in a reinvestment rate on the float income. This cash flow, since it is assured, can all be incorporated as interest to investors when structuring the CMO.

Maximum maturity guarantees for each investor class can establish shorter maturities for the bond than the underlying mortgages. This structure can result in the obligation to retire a class before its related mortgage principal is repaid. The issuer then must fund the retirement with new borrowings, which may be at a substantially higher rate than the CMO.

MBS portfolios can be managed by varying the composition of coupon rates as interest rates change. Investors which expect interest rates to increase may purchase an MBS with a coupon higher than the current coupon rate. This would result in paying a premium over the par value of the security. If interest rates increase, the prepayments on the underlying mortgages will slow, resulting in a slower write-off of the premium and a higher yield. Conversely, an investor may sell higher coupon rates and purchase lower coupon rate MBSs as interest rates decrease. Whenever the corporate acquires a significant dollar amount of lower coupon rate MBSs, this strategy should be closely reviewed to determine the interest-rate risk.

Some investors prefer to hold mostly current coupon rate MBSs in their portfolios. A current coupon MBS is one with a rate that is approximately 50 basis points less than the most prevalent interest rate quoted by lenders for fixed-rate mortgages. Current coupon MBSs are more actively traded and, therefore, more liquid. However, if the investor prefers to sell MBSs in its portfolio to acquire current coupon, the question of intent for investment versus trading may be raised. These strategies may add credence to the classification of a trading portfolio compared with an investment portfolio.

Mortgage Security Brokers

Corporates should solicit several price quotations for their transaction that involve brokers. This will help ensure that they are receiving market value for portfolio transactions. Some corporates may execute most or all of their transaction through a limited number of brokers. Should they not actively solicit comparable price quotes, corporates may be purchasing above or selling below the market. A substantial turnover in the portfolio could result in significant lost income. Therefore, corporates should actively solicit comparable market quotes from at least two brokers other than the broker through which transactions are executed. Even if a corporate does not have significant volume, comparable price quotes should be obtained.

Hedging MBS Portfolios

A number of approaches are available for hedging a portfolio of MBSs. Interest rate risk associated with holding MBSs can be reduce by entering into forward commitments to sell. The forward market allows for hedges customized by issuing organization, coupon, contract size, and settlement date. Management must have the requisite level of technical expertise and assess the risks of its hedging strategies prior to execution of the strategy. Derivative transactions are limited to corporates with Part IV Expanded Authority. More details on derivative activities are contained in Appendix 202B.

Monitoring Requirements

All documentation relating to the use of MDPs should be reviewed. In general, such documentation should include:

1. The policy, business plan, position limits, and internal controls and procedures applicable to MDPs.

2. The sensitivity or simulation analysis, performed prior to purchase and performed periodically thereafter.

3. The assumptions used in performing the sensitivity analysis;

4. Monthly updates of performance of the instruments showing actual versus projected performance; and

5. a list of personnel authorized to make investment decisions involving MDPs and a description of their qualifications.

The use of MDPs should commence only after the risks have been thoroughly evaluated and policies and procedures have been established and documented.

Chapter 203

LOAN REVIEW

Introduction

Corporate credit unions (corporates) were initially created to provide liquidity resources to the natural person credit union (credit union) industry. Over time corporates have come to offer a wider array of products and services; however, they are still the primary source of liquidity and wholesale funding for most credit unions. Historically, risk within corporate loan portfolios has been considered low due to the small percentage of overall assets loans represent, and due to the unique deposit structure of member credit unions where debt is considered senior to share deposits and is typically secured by assets of the credit union. However, given the key role corporates play as a liquidity resource to member credit unions, it is imperative corporates have effective policies and practices in place to ensure funding is available to the membership, and it can be provided in a manner that limits credit and liquidity risks to the corporate.

Lending activities of corporate credit unions are governed by Section 704.7 of the National Credit Union Administration (NCUA) Rules and Regulations (Regulations). Credit may be extended directly from the corporate to the borrower, or provided via pass-through and guaranteed loans from the Central Liquidity Facility (CLF) and the National Credit Union Share Insurance Fund (NCUSIF). In either circumstance, Section 704.7 sets forth specific limitations and responsibilities corporates must adhere to when making loans to member credit unions and other borrowers.

Regulatory Requirements

Section 704.7(a) requires all corporates operate according to a lending policy which addresses, at a minimum, the following items:

1. Loan types and limits;
2. Required documentation and collateral; and
3. Analysis and monitoring standards.

Loans granted by corporate credit unions to other credit unions are exempted by Section 107a(c)(1)(B)(v) of the Federal Credit Union Act from the statutory and regulatory requirements imposed on business loans. However, Section 704.7 of the Regulations sets forth the following other limitations regarding corporate lending:

1. Loans to Member Credit Unions - Section 704.7(c)(1). The maximum aggregate amount in unsecured loans and lines of credit to any one member credit union, excluding pass-through and guaranteed loans from the CLF and the NCUSIF, shall not exceed 50 percent of capital. The maximum aggregate amount in secured loans and lines of credit to any one member credit union, excluding those secured by shares or marketable securities and member reverse repurchase transactions, must not exceed 100 percent of capital.

2. Loans to Non-Member Credit Unions - Section 704.7(d)(1). A loan to a credit union that is not a member of the corporate, other than through a loan participation with another corporate, is only permissible if the loan is for an overdraft related to the providing of correspondent services pursuant to Section 704.12. Generally, such a loan would have a maturity of only one business day.

3. Loans to members that are not credit unions - Section 704.7(c)(3). The aggregate amount of loans and lines of credit to one member, other than a credit union or corporate CUSO, shall not exceed 15 percent of the corporate's capital plus pledged shares. Any loan or line of credit made to a member, other than a credit union or a corporate CUSO, unless exempted by Section 723.1(b), must be made in compliance with Part 723 of Regulations, which governs member business loans, unless such loan or line of credit is fully guaranteed by a credit union, or fully secured by U.S. Treasury or agency securities. Those guaranteed or secured loans must comply with the aggregate limits of Section 723.16, but are exempt from other requirements of Part 723.

4. Loans to Corporate CUSOs - Sections 704.7(c)(2), (d)(2), and (e)(2). Loans to corporate CUSOs, whether members or nonmembers, are governed by Section 704.11. The aggregate of all investments in and loans (including lines of credit) to member and non-member corporate CUSOs cannot exceed 30 percent of the corporate's capital. However, a corporate may loan to corporate CUSOs an additional 15 percent of capital if collateralized by assets in which the corporate has perfected a secured interest under state law. (See Section 704.11(b)). Note that while NCUA's Rules and Regulations Section 704.7(e)(2) states that corporate CUSOs are not subject to Part 723 of regulations, this statement is made relative to loan limitations in Part 723, which are superseded by limits imposed by Section 704.11. Loans to corporate CUSOs are still subject to the due diligence requirements imposed on business loans by Section 704.11(c), which incorporate selected subsections of Part 723 by reference.

5. Participation Loans with Other Corporates - Section 704.7(f). Corporates may enter into loan participations with other corporates, contingent that each corporate retains at least 5 percent interest in the face value of the loan. A master participation loan agreement must be in place before the purchase or sale of the participation, and each participating corporate must exercise the same due diligence as if it were the originating corporate credit union. Corporates are allowed to participate in loans with natural person credit unions, but only if they have been approved for Part V Expanded Authority, or have requested and received a waiver permitting this activity. The limits established by the OCCU Director will govern this activity, and can be determined from the approval paperwork.

6. An analysis of the financial and operational soundness of the borrower, and the borrower's ability to repay, must be performed prior to loan approval. A corporate may assess prepayment penalties, if these are called for by the loan contract. When loans are issued to a corporate's natural person members, all consumer lending regulations will apply.

Types of Corporate Lending

Corporates offer a variety of loan products to their membership, including, but not limited to: overnight settlement loans, term loans, and secured and unsecured line of credit loans. While underwriting procedures and limitations may differ for each individual type of loan product, in all instances it is imperative that loan policies, practices, and personnel are effective in managing credit and liquidity risks.

CLF Loans

Corporates act as agents of the CLF through U.S. Central Credit Union. In this capacity member credit unions can gain access to a stable source of liquidity without the need to make a direct investment in CLF stock. CLF loans are primarily liquidity loans, and by law cannot be used to expand the investment and loan portfolios of the member credit unions. Any loans made as an agent of the CLF must meet the CLF's lending criteria. The corporate should maintain appropriate documentation evidencing the fact the loan has been authorized and guaranteed by the CLF, and these lending criteria have been met.

NCUSIF Guaranteed Loans

In certain situations loans may be disbursed with guarantees from the NCUSIF. This generally occurs when a natural person credit union is being liquidated or is subject to some other administrative type action. In any event, NCUA will guarantee repayment of the loan to the corporate. The corporate should maintain the appropriate documentation on file to evidence the loan guarantee.

Settlement Loans and Short-Term Liquidity Loans

The most common types of loans offered by corporates are settlement loans, short-term liquidity loans, and reverse repurchase loans. Term financing is less common, but term loans are a product most corporates offer.

Normally, corporates will extend settlement lines of credit based upon the member's asset size, anticipated needs, and ability to repay (i.e. financial strength). The line of credit will normally be used for both settlement and short-term funding shortages. The line may be "committed" (guaranteed) or "advised." A committed line of credit is always available to the member, while an advised line of credit is available at the discretion of the lender (corporate) at the time of the request. Most lines of credit are typically advised because of the fees associated with obtaining a committed line. Normally, revolving lines of credit requiring no advance notice by the borrower will carry a higher rate of interest than a credit line where advances must be requested and approved. This is indicative of the fact the lender (corporate) will have the ability to decline the advised loan advance if, at the time of the request, a financial review indicates the borrower's financial condition has deteriorated to the point where ability to repay is in question.

The decision to discontinue a member's settlement funding can have material financial and reputation repercussions to the corporate, the member credit union, and natural person members of the member credit union involved. A corporate should have preexisting procedures in place which address how to proceed with the settlement funding process when a member credit union has overdrawn its settlement line or otherwise presents increasing levels of credit risk. Such procedures should address offset of the loan balance by the member's other deposit accounts at the corporate, requirements for additional loan collateral, and involvement of alternative funding resources, such as investment repurchase arrangements and the CLF.

Short-term credit line loans may be secured or unsecured. Normally, secured lines will be priced at a lower rate of interest than unsecured lines.

When evaluating the ability to repay a settlement or short-term line of credit obligation, the major evaluation criteria should be the strength of the borrower's balance sheet and ability to generate funds inflows and/or convert assets to meet cash flow needs. Normally, these loans will be repaid via the settlement of cash letters and ACH deposits in transit, as well as normal cash flows received from loan amortizations and maturing investment balances. Therefore, liquidity of the members' receivables is crucial to the satisfaction of the obligation. In most instances settlement loans should carry a maturity of one day, while short-term line of credit loans normally should be retired within 12 months of the initial advance. Settlement and line of credit balances that remain outstanding for periods longer than those stated could indicate serious funds management deficiencies on the part of the borrower, or a misuse of the proceeds of the advance (i.e. using line of credit loans to fund long term consumer and real estate lending).

Reverse Repurchase Agreements

Corporates often enter into repurchase agreements with member credit unions where investments are "purchased" from members in order to provide the members with short-term cash funding. These repurchase transactions are accounted for in a manner very similar to a secured loan. In a typical repurchase transaction the corporate will extend a loan advance to the member credit union. The loan is "secured" by investment securities owned by the member credit union.

The corporate receives a "fee" which is represented as the difference between the agreed upon price of the securities as of the day of the settlement date of the transaction and the agreed upon future repurchase price. Normally, a margin of at least 102 is required to adequately secure this type of lending transaction; however, this margin requirement should be increased if the securities taken as collateral exhibit high volatility or price risk. It is imperative the corporate have appropriate internal controls in place to determine the market value of collateral on a daily basis, and the collateral obtained is a legal investment for corporate credit unions pursuant to Section 704.5.

Term Loans

Term loans are normally used to fund long-term capital expenditures or product offerings for member credit unions and affiliated organizations. The repayment of term financing is heavily dependent upon the long-term financial strength of the borrower; therefore, the lender should not only focus upon the ability of the borrower to generate a short-term cash flow, but also review long-term earnings capability. Normally, term loan advances will be secured with specific fixed assets, investment securities, or loan receivables. The effective securitization, valuation, and monitoring of these assets is crucial in managing credit risk on a term loan advance.

Participation Loans

Participation lending is allowed under Section 704.7. Loan participation between corporates is increasing in frequency as corporates try to meet industry liquidity needs.

If a corporate is participating with other corporates, the examiner should ensure compliance with all the requirements of Section 704.7(f), and the same due diligence was required on the participation loan is required on all other loans originated by the corporate. The examiner should review the file, including the credit analysis process, security agreements, and participation agreement. If there is extensive activity in this area, the examiner should review a loan sampling of sufficient size and scope to determine the adequacy of the corporate's practices and procedures for each type of loan participation being entertained, and the level of risk each presents.

If the corporate has expanded authorities through Part V of the corporate rule or via a loan participation waiver, the examiner must ensure the corporate is complying with the terms of the expanded authorities or waiver. Additionally, the examiner must ensure the corporate has adequate policies, procedures, and practices to monitor and control credit risk based upon the type of collateral pledged.

Lending Risk Assessment

Since loans typically comprise a small percentage of a corporate's total assets, the extent of review of individual loan files will be determined by the EIC. The main focus of the loan review is to determine if the corporate has detailed policies and procedures for all types of loans offered, and they are being followed in actual practice.

If information developed during the review of policies and procedures reveals a serious problem, the examiner has the option of expanding the review of individual loans as necessary to identify the extent of the problem and the corrective actions required. Reasons for expanding or contracting the loan review will be discussed in the Corporate Examiner Memorandum for Lending and in the confidential section of the report. Regardless of the size of the loan review, serious problems will normally require development of a Document of Resolution to resolve them.

Written Lending Policies and Procedures

Section 704.7(a) requires that all corporates maintain written lending policies. Written policies and procedures should be commensurate with the volume and complexity of the corporate's lending program.

The board-approved policies should establish general risk limitations and authorizations regarding the corporate's lending function. Policies should also be specific as to collateral requirements, and procedures should be in place for valuing collateral taken as security on loans. Written procedures should detail the corporate's loan underwriting, monitoring, and reporting practices.

The examiner should review all written policies and procedures to determine that they adequately set forth restrictions, limitations, and appropriate internal controls over the lending function. The examiner should determine that written policies and procedures are periodically reviewed and revised as economic, competitive, and market changes dictate. The written policies and procedures should provide for sound credit risk and liquidity management, while also ensuring a competitive lending function for the corporate.

In general, the examiner should determine that the written policies and procedures:

1. Identify the types of loan products the corporate will offer. The policies and procedures should include the specific characteristics, limitations, and underwriting requirements for each loan product (e.g. security requirements, cash flow requirements, pricing).

2. Specify how the value of acceptable types of collateral (including for loan participations) will be determined and subsequently monitored, and identify the process needed to adequately perfect security interests in such collateral.

3. Identify the specific terms and maturities of different types of loan products. Repayment terms should ensure amortization of loans sufficient to meet the funding needs of the corporate. Repayment terms should also be related to any expected declines in collateral value, and the overall cash flows of the borrower.

4. Require that all loan terms be set in a written lending agreement between the corporate and the borrower, which, for loans other than lines of credit, should be sufficient to retire a note within 15 years.

5. Contain loan pricing strategies that comply with statutory interest rate limitations.

6. Identify management and staff members responsible for underwriting loan requests, and their approval authorizations.

7. Are consistent with the corporate's ALM and funds management objectives. Examiner staff should determine loans are being advanced with the profitability and liquidity needs of the corporate in mind.

8. Identify specific guidelines by which the borrower's credit worthiness will be assessed. This will include a listing of key financial ratios that will be evaluated. Policies and procedures need to specifically identify thresholds of acceptable financial and statistical data and trends.

9. Provide for periodic compliance reviews independent of the lending function. A periodic compliance review or audit of the lending policies and practices should be required in order to determine the effectiveness of the policies and procedures, as well as lending staff's adherence to the policy requirements and objectives. This requirement may be found in internal audit or other policies, if not specified in the lending policy.

10. Establish requirements for identifying delinquent loans, loan classifications, and "watch list" preparation and maintenance.

Loan Underwriting Procedures and Documentation

The corporate should make an assessment of the financial and capital strength of the borrower. Adequate procedures must also be in place to securitize and value assets taken as collateral on loans so they may be converted to appropriate cash flow in the event of a default.

The examiner must ascertain the corporate has performed the appropriate due diligence to determine the ability of the borrower to repay the debt, and the analysis is periodically updated throughout the life of the loan or line of credit.

As part of the lending review, the examiner should determine corporate management is taking adequate measures to continually assess the borrower's financial strength. The ability of loan officers to determine the financial strength of prospective borrowers is crucial in managing credit, interest rate, and liquidity risk on both secured and unsecured lending transactions.

Financial Analysis

The examiner should determine the loan officers are performing and documenting a sound financial analysis of borrowers. Financial ratios that may be used to determine the solvency, earnings potential, and liquidity of potential borrowers include, but are not limited to:

Solvency Ratios:

1. Capital/Total Assets;
2. Net Capital/Total Assets; and
3. Debt/Capital.

Earnings Ratios:

1. Net Income/Average Assets;
2. Operating Expenses/Average Assets;
3. Net Interest Margin/Average Assets;
4. Fee Income/Operating Expenses; and
5. Net Loan Losses/Average Loans.

Credit Quality Ratios:

1. Delinquency/Total Loans;
2. Charge-offs/Total Loans; and
3. Loan Growth Ratios.

Liquidity Ratios:

1. Current Assets/Current Liabilities;
2. Delinquent Loans/Total Loans;
3. Long Term Assets/Total Assets; and
4. Share and Loan Growth Ratios.

The examiner should determine the corporate is using proper financial analysis tools to evaluate specific types of loans. When evaluating a long-term secured loan, the loan officer must determine the member demonstrates adequate capital and long-term earnings ability. In addition, current and future value of collateral taken as security must be evaluated. The ability to convert collateral to cash must also be verified by the loan officer.

The examiner should determine the loan officer initially evaluated at least three years of the borrower's financial performance to estimate the credit union's or affiliated organization's financial strength and liquidity. This analysis should be updated periodically throughout the life of the loan (please refer to Ongoing Monitoring, below).

The examiner should ascertain the corporate has knowledge of the capabilities of the borrower's management team, and therefore, may be able to make subjective assessment of their skills in managing the financing of the credit union's assets. Any assessment should be detailed in the loan officer's credit review. Financial ratio and credit analysis should be undertaken on, at least, an annual basis, with more frequent reviews performed for active lines of credit, large concentrations, and "watch list" loans.

Review of Independent Audit Reports

A valuable tool in assessing the financial condition and internal control structure of the debtor is the independent audit report. Corporate loan policies should require a copy of each borrower's independent audit report, including any management letter, be obtained on an annual basis. The audit may often disclose internal control, management, and operational deficiencies that could be material in the decision to grant credit.

Collateral Analysis

Corporates often extend loans to member credit unions and other affiliated organizations that are secured by specific assets. In many cases corporates have required that a "blanket" lien be placed on all the assets of a credit union entering into a line of credit agreement with the corporate. When filing a blanket lien the corporate does perfect a security interest. However, without also making a determination as to specific assets to be secured, and determining lien position as to those assets, the corporate may not be gaining much collateral value.

When an examiner is making a determination as to the validity of security interests, it is important to ensure the corporate has practiced appropriate due diligence in perfecting a security interest, and ensuring a first position on assets identified as collateral. It is important to note the Federal Home Loan Bank will often require a corporate to subordinate its lien position regarding real estate loans taken as collateral in loan transactions previously consummated between the corporate and its member credit unions. If these aspects of collateralization cannot be confirmed, the loan should be considered unsecured.

In instances when a blanket lien is filed out of "an abundance of caution" in conjunction with a sound ability to repay on an unsecured transaction, the examiner should not be overly critical of the corporate's collateral interests. However, in instances when collateral is deemed critical to reducing credit risk on the loan, the examiner should determine the corporate has taken sufficient action to perfect a valid security interest in the collateral, and determine the value of collateral is sufficient to securitize the loan balance.

In most cases collateral on corporate loans falls into five different categories:

1. Member share deposits;
2. Members' investment securities;
3. Commercial real estate;
4. Interests in member credit union loan portfolios; and
5. Other tangible assets.

In order to perfect valid security interests in each type of asset, specific steps must be taken as to documentation, legal filings, and overall due diligence. The examiner may need to become familiar with state filing requirements and procedures to ensure security interests are properly perfected.

The three requirements for the creation of a security interest are stated in the Uniform Commercial Code (UCC) Section 9-203. Once the following requirements are met, the security interest attaches:

1. The collateral is in the possession of the secured party pursuant to agreement, or the debtor has signed a security agreement that contains a description of the collateral;
2. Value has been given to the debtor; and
3. The debtor has rights to the collateral.

Thus, unless collateral is in the possession of the secured party, there must be a written security agreement that describes the collateral. The description need not be very specific or detailed as long as it reasonably identifies the collateral. It is most important the creditor files appropriate documentation with applicable state authorities, and a lien search is performed to determine no other creditors have prior interest in the assets secured. The examiner may need to consult state laws regarding the perfection of security interests, determining the corporate has adequately secured its position in any assets collateralizing a loan. The corporate should maintain a written legal opinion regarding the legality of all forms used . The opinion should provide assurance the corporate's procedures for securing interests in collateral whether it be deposits, investment securities, real estate, loans, or other tangible assets, are adequate and legally binding.

In the instance where a loan is secured by shares deposited in the corporate, the perfection of the security interest is achieved via the security agreement entered into with the member and the Statutory Lien Provisions set forth in the Federal Credit Union Act. The corporate's possession of the cash accounts provides a "perfected" interest in the accounts according to the UCC provisions listed above.

In the event a corporate extends credit secured by cash not on deposit at the corporate, a lien search is recommended, and a UCC-1 filed with the appropriate state authorities identifying the cash accounts that are being encumbered as security on the loan. It is also recommended the institution holding the deposit acknowledge the corporate's interest in the collateral.

Ongoing Credit Review

A credit review should not end with the review of the initial credit application. Corporates issue commercial credit, repayment of which is heavily dependent upon the borrower's ability to maintain financial strength through changing economic and competitive conditions. The examiner should determine the corporate's lending policies and practices provide an effective program of ongoing credit analysis of borrowing members and affiliates.

Credit reviews, including an evaluation of financial, statistical, and organizational information, should be completed for each borrowing institution on at least an annual basis. More frequent reviews should be initiated depending upon the type of credit issued, fluctuation in value of collateral, amount of dollars outstanding, frequency of advances on credit lines, and the financial condition of the borrower.

All credit reviews should be documented, and evidenced by a loan officer's written assessment as to the financial and operational stability of the debtor. Many corporates enlist the services of third party data aggregators who compile various ratios based on NCUA 5300 Call Report information. Such analytical information can have value, but, standing alone, it is not sufficient to establish the corporate's due diligence. The credit review must establish the scope of the analysis, and loan officers should document in narrative format the rationale behind conclusions for increasing, decreasing, or merely maintaining an open credit line. If the examiner deems initial and ongoing credit reviews do not adequately verify the debtor's financial condition and ability to repay, then a finding and record of action should be provided in order to facilitate corrective action.

Examination Objectives

The objectives for reviewing a corporate's lending program are as follows:

1. Determine the degree of credit risk exposure inherent within the corporate's lending program, in relation to its capital position.

2. Determine the adequacy of policies, practices, procedures, and controls regarding loan portfolio management, in relation to current market and economic conditions.

3. Determine if corporate staff is processing loans within policies and procedures.

4. Determine compliance with applicable laws, rulings, and regulations.

5. Determine if members are treated equitably during the implementation of the corporate's lending policies, practices, and procedures.

6. Determine if timely corrective actions are initiated when policies, practices, procedures, or controls are deficient, or when violations of laws or regulations are noted.

7. Determine if the corporate is complying with its loan participation authorities.

Examination Procedures

See Corporate Examination Procedures - Loan Review (OCCU 203P).

Examination Questionnaire

See Corporate Examination Questionnaire - Loan Review (OCCU 203Q).

References

1. Commercial Bank Examination Manual, Board of Governors of the Federal Reserve

2. Regulatory Handbook, Thrift Activities, Office of Thrift Supervision

3. Examiner's Guide, National Credit Union Administration

4. Comptroller's Handbook for National Examiners

Chapter 204

CAPITAL

Introduction

Capital analysis is the primary method of determining the strength, not only of an individual corporate credit union (corporate), but also of the corporate credit union system (System). Capital levels must meet minimum regulatory requirements, but more importantly take into account the risk assumed by a corporate both on and off its balance sheet. Examiners and corporate management must realize that the capital regulatory requirements represent just a floor; the real goal is to accumulate adequate capital to protect the corporate from market and operational risks.

Section 704.3 requires that corporates maintain minimum capital levels. It also requires NCUA to evaluate, and possibly take action against any corporate which does not have adequate capital.

Capital is the quantitative culmination of management's efforts to develop and implement policies, procedures, and practices which result in a balance sheet that provides a reasonable return to members and protection against risk.

This chapter offers guidance for ascertaining whether a corporate has adequate policies, procedures, and practices to maintain a sufficient capital level.

Purpose of Capital

Capital performs a variety of functions.

<u>Promotes Credit Union Member and Public Confidence</u>

Capital provides a measure of assurance to natural person credit unions that a corporate will continue to honor its obligations and provide financial services. Confidence in the corporate then will be transferred to confidence in the entire credit union industry, by credit union members, the public and legislative leaders.

<u>Supports the Type, Volume, and Character of the Business Conducted</u>

The amount of capital necessary to protect a corporate depends, not only on the type of transactions in which it engages, but also the volume and character (the way business is conducted) of the transactions. The key is to evaluate the total risk to capital.

Provide for the Possibility of Inherent Losses

Capital will allow a corporate to continue as a "going concern" during periods when it experiences operating losses, declines in asset values, or other adverse financial results.

Control Excessive Growth

A corporate must continuously evaluate the size of its balance sheet to determine it operates within its capital limitations. Thus, it promotes prudent growth and restrains uncontrolled expansion of assets.

Provides Protection for Depositors, Investors, Creditors, and the NCUSIF

Corporate management has a fiduciary obligation to protect its depositors, investors, and creditors from losses. The building of capital not only acts as a cushion for those parties, but also the National Credit Union Share Insurance Fund (NCUSIF).

Increasing retained earnings has been a primary goal of regulatory initiatives for a decade. There is a very important distinction between internally generated capital, retained earnings, and other types of capital accounts. An adequate level of internally generated capital is essential to avoid erosion of member confidence in the event losses occur. NCUA believes an earnings retention requirement is the appropriate means of ensuring a minimal level of retained earnings on an ongoing basis.

The inclusion in 1998 of paid-in capital (PIC) as an alternative form of capital expanded corporates' options for raising additional capital. This concept was brought to fruition when well capitalized natural person credit unions indicated a willingness to commit a portion of their equity to support the System.

It was intended PIC, because of its implicit high cost, would be used by corporates as a bridge during short periods when they needed to increase capital adequacy. When that need diminishes, it is expected corporates would call in these high cost funds. The corporate rule facilitates this process.

Due to PIC's inherent risks to investors and attendant cost to the issuer, it is anticipated most corporates would use these instruments as a last resort to achieve specific goals, or during periods of unanticipated rapid growth. Corporates which plan to use PIC for long periods should adequately address this in their capital and strategic plans.

Definitions

Section 704.2 defines capital and other terms necessary to determine the make-up of capital.

Capital

Capital is the sum of a corporate credit union's retained earnings, paid-in capital, and membership capital.

Retained Earnings

Retained earnings includes the total of the corporate's undivided earnings, reserves, and any other appropriations designated by management or regulatory authorities. Retained earnings does not include the allowance for loan and lease losses account, accumulated unrealized gains and losses (UGL) on available for sale securities or other comprehensive income items. Valuation allowances established to meet full and fair disclosure requirements of Section 702.3 as well as UGLs are not included in retained earnings since they may distort capital levels and ratios during periods of steeply rising or falling interest rates.

Paid-In Capital

There are two types of paid-in capital authorized by Part 704: member paid-in capital and non member paid-in capital. Member paid-in capital is held by the corporate credit union's members. The following conditions apply to this obligation:

1. perpetual, non-cumulative dividend accounts;
2. a prohibition against a corporate from requiring membership, services, or prices of services as a condition for purchasing the instrument;
3. callable on a pro-rata basis across an issuance class only at the option of the corporate and only if the corporate meets its minimum level of required capital and Net Economic Value (NEV) ratios after the funds are called; and
4. the disclosure of the terms and conditions of the instrument when it is purchased.

Non member paid-in capital is sold on the market in accordance with conditions set by NCUA on a case-by-case basis.

Paid-in capital, regardless of the type, is

1. available to cover losses that exceed reserves and undivided earnings;
2. not insured by the NCUSIF or any other share or deposit insurers; and
3. callable only at the option of the corporate and only if the corporate meets its minimum level of required capital and NEV ratios after the funds are called.

Membership Capital

Membership capital is funds contributed by corporate members which:

1. May be issued as term certificates or as an adjusted balance account. Adjusted balance accounts may be adjusted based upon a measure that is established and disclosed by the corporate at the time the account is open. For instance, the required membership capital as of December 31 each year may be a percentage of a credit union's assets as of the preceding September 30. The percentage may change from year to year based upon a corporate's needs. Any reduction in the amount of the membership capital will not be considered a withdrawal if it occurs in conjunction with the periodic adjustment to all membership capital.

2. Have a three-year minimum withdrawal notification. Upon written notice of intent to withdraw membership capital, the balance of the account is frozen until the conclusion of the notice period, whether the account is a term certificate or an adjusted balance account. If the membership capital is in the form of an adjusted balance account, the frozen account may not be adjusted either up or down on the adjustment date. It remains the same until the end of the notice period. When notice is given, the amount of the account that can be considered membership capital (and thus a part of capital) must be reduced by a constant monthly amortization of the account until it is fully amortized at the end of the notice period.

3. Require disclosure of the terms and conditions to the recorded owner at the time the membership capital is issued and, at least, annually thereafter.

4. Are available to cover losses that exceed reserves and undivided earnings and paid-in capital. The full balance of membership capital, including the amortized portion, is available to absorb losses until the funds are released by the corporate at the end of the notice period.

5. Are not insured by NCUA or any other share or deposit insurers.

6. Cannot be pledged against borrowings.

7. May be sold to other members within the corporate's field of membership, subject to the corporate's approval.

Order of Payout

In the event of a corporate's liquidation, losses will be absorbed in the following order: current earnings, valuation allowances, undivided earnings, reserves, paid-in capital, membership capital, uninsured share obligations, NCUSIF, and liabilities.

Capital Ratio

The capital ratio is computed by dividing the corporate's capital by its moving daily average net assets (DANA). This is the ratio used in determining if base and base plus corporates are meeting the capital requirements of Section 704.3 (d); Part I corporates, Appendix B, Part I (c)(1),(2) and (3); and Part II corporates, Appendix B, Part II (c) (1), (2) and (3). It is also utilized for establishing concentration limits contained in Section 704.6(c), Credit Risk Management, Appendix B, Part I(b) and (d); Appendix B, Part II (a)(1), (b) and (d); Appendix B, Part III (b) (4) and (5); and Appendix B, Part V (a) as well as limiting changes in the NEV contained in Appendix B, Part I(c) (2) and (3) and Appendix B, Part II(c) (2) and (3).

Core Capital Ratio

The core capital ratio differs from the capital ratio in that it is computed by dividing the corporate's retained earnings (consistent with the definition of retained earnings on page 204-3, which does not include valuation allowances or UGL) and paid-in capital, if any, by its moving DANA. The core capital ratio does not include membership capital. This distinction was made to encourage corporates to build retained earnings and to limit risk to these accounts. The core capital ratio is considered when determining the earnings retention factor in conjunction with the calculation of earnings retention amounts.

Retained Earnings Ratio and Earnings Retention Requirement

The retained earnings ratio is computed by dividing the corporate's retained earnings by its moving DANA. A corporate must increase retained earnings if the prior month-end retained earnings ratio is less than 2 percent. Earnings retention requirements are contained in Section 704.3(i) and Section 704.19(b) for corporates and wholesale corporates, respectively.

Capital Requirements

All corporates operating as base or base plus must have 4 percent capital. Those operating under Part I or Part II authorities must have between 4 and 6 percent capital depending on the NEV volatility threshold established by the corporate.

Evaluating Capital Adequacy

Capital planning by corporates and regulatory analysis should include careful consideration of qualitative, as well as quantitative factors that may affect capital adequacy. Capital adequacy cannot be determined solely on the basis of a numeric formula or standard. Regulatory minimum requirements are not a proxy for analysis of the adequacy of an institution's capital position.

Risk Management - Qualitative Factors

The following factors should be viewed in conjunction with an overall analysis and understanding of a corporate, as well as the financial institution in general. The list is by no means all-inclusive.

<u>Quality of Management</u>

The quality, experience, depth, and sophistication of corporate management and officials are key in evaluating capital adequacy. Sound management entails developing procedures and practices, including reporting and auditing systems, which implement safe and sound policies. The corporate's board of directors must ensure it has competent managers. The board of directors and management should work together as a team, but they also must understand their distinct roles and responsibilities. The board ultimately remains responsible for the conduct of the corporate's affairs and provides independent checks and balances over management. Section 704.4 provides guidance to the board of directors on a wide range of areas for which the board of directors is responsible.

Inefficient or lax operations are costly. Shortcomings in systems, procedures, and controls expose corporates to losses through fraud, employee error, or miscalculation.

Capital Planning

Section 704.3(a) requires a corporate's board of directors to develop and ensure that written short- and long-term capital goals, objectives, and strategies are implemented. The combination of these should provide for building capital consistent with Part 704 and maintaining sufficient capital to support current and future risk exposures arising from the corporate's activities. The regulation also requires the periodic review and reassessment of the corporate's capital position.

Capital planning is a key aspect of managing a successful corporate. The board of directors, in conjunction with management and staff, should attempt to anticipate capital needs as well as maintain an adequate capital position. Although Part 704 stipulates minimum capital levels, management should not manage capital to the regulation. Rather, the board should target a minimum capital level consistent with its risk profile and future plans. Corporates undertaking significant expansion or exposed to high or unusual levels of risk are expected to maintain capital well above the minimum ratios.

Good capital planning is dynamic. The board of directors as well as management should be involved in formulating plans for the growth, mix, concentration, and effective management of assets and liabilities. A good plan sets forth specific strategies by which management intends to achieve established goals. Long- and short-term strategies should be developed. Long-term strategies should address the corporate's overall business plans including services intended for members. Strategies that may need to be used to increase capital and/or capital ratios (including NEV) are:

1. changing the mix of assets and liabilities to reduce the risk to asset portfolios;
2. reducing or slowing asset growth;
3. increasing earnings retention by changing the liability or deposit mix to reduce dividend payments;
4. streamlining operations or otherwise reducing the cost of operations; and
5. issuing paid-in or membership capital.

Funds Management

Section 704.8 provides the corporate with guidance in establishing effective asset-liability management policies. It is considered the core of sound planning and financial management and includes the supervision of the corporate's liquidity and interest rate sensitivity. Each corporate should have procedures minimizing the possibility of liquidity risk resulting in forced asset sales or interest rate risk resulting from asset maturities mismatched with source fund maturities. Policies and practices must include guidelines addressing off-balance sheet accounts if they exist.

Earnings Performance

The degree of profitability is a fundamental component of capital analysis, as it is a key indicator of the extent to which earnings can be relied upon as a source of new capital. Good earnings performance enables a corporate to remain competitive and even expand its operations. Included in that analysis is the payment of dividends. Dividends which are excessive can cause unnecessary growth which may reduce a corporate's capital position.

Credit Risk

Section 704.6 provides the corporate guidance in establishing policies that monitor and control credit risk in the corporate's various asset portfolios. Credit risk exists in a corporate's loan portfolio to members (although generally representing a small portion of overall assets) and its investment portfolio. Corporates that have Parts I, II, or III authorities generally can expand their capabilities to invest in instruments which have varying levels of credit risk.

The overall diversification in asset composition must be considered in determining capital adequacy. Likewise, the level of non-performing loans, securities ratings, and market value of securities are indicators of asset quality. Specific consideration should be given to the future effect on capital of continuing asset quality problems and the effectiveness of portfolio management.

Balance Sheet Diversification

The amount of capital required is a function of the risks associated with the composition and mix of assets and liabilities. Generally, a greater degree of asset and liability concentrations increases the need for capital. On- and off-balance sheet assets should be reviewed for concentrations in industries, product lines, customer types, and funding sources, as they apply to the corporate's strategic plan and its components.

Asset Growth

Growth in assets should be supported by growth in capital. Asset growth that outpaces the ability to maintain a sufficient level of capital is unsafe and unsound; however, determining the point and degree when growth negatively impacts capital is a more difficult task.

Traditionally, corporates have grown and contracted in response to the credit union industry's growth patterns. In the past, corporates were not concerned with the ratio of capital to assets, but relied on improving trends in the dollar amount of capital. Corporates are now looking for alternatives which enable them to meet their member needs without negatively impacting on their capital ratios. Examiners can expect corporates to utilize off-balance sheet transactions and CUSO operations as tools to control asset growth and thus the capital ratio.

Another method corporates may use to increase capital during periods of rapid growth will be membership capital and paid-in capital. While both are acceptable means to increase capital, an overall strategy for using each is a necessary element in capital adequacy.

Off-Balance Sheet Activities

Off-balance sheet activities should be examined to determine risk exposure and risk concentrations. Each source of risk must be viewed in light of its contribution to portfolio risk and the ability of management to administer it. It is important for management to be aware of these sources of risk, including the corporate's credit risk exposure under recourse obligations. Management must implement controls and procedures to identify, monitor, and manage the corresponding risks. Major off-balance sheet risks include credit, interest rate, and market risks, as well as pending litigation.

Field of Membership and Provided Services

The size and composition of a corporate's field of membership, combined with the philosophy of management are major contributors to the services provided to members. Some corporates which are limited in size are unable to provide some services to their members. Others, which have size have decided not to provide certain services. And others, without the size, still try to provide those services. The decision on what services to provide members rests with the board of directors.

In some institutions, services represent a significant portion of the corporate's income. The risks associated with services or the loss of income associated with the services must be clearly identified and addressed by the board of directors.

If services are provided through a CUSO, it should be capitalized commensurate with the industry standards for the activity in which it is engaged.

Financial Risk - Quantitative Factors

Financial ratio analysis should be used to supplement qualitative analysis of capital adequacy. In many financial institutions, the review of capital is often supplemented by comparing the ratio to peer groups or expanding the analysis to include a risk base capital standard. The unique nature of corporates may make these analyses difficult.

There are fewer than 30 corporates ranging in size from several million dollars to multi-billion dollars in assets; thus rendering a meaningful corporate-wide peer comparison impractical. Additionally, corporates vary significantly in the services they provide. The risk associated with these services adds another barrier in developing meaningful peer groups.

Corporates are primarily liquidity facilities. Their balance sheets are structured to respond to the liquidity needs of their members. As such, the balance sheets are generally comprised of short-term high quality investments which traditionally have little credit risk. Reliance on a risk based capital ratio as a forecaster of risk to corporates has proven to be unreliable in the past and does not appear to be an effective tool in the future.

Increasing leverage capital, while controlling the risk to a corporate's balance sheet by limiting changes to NEV and mitigating operational risks, is the most reasonable method of addressing capital adequacy in the System.

In lieu of comparing a corporate's capital ratio to a peer group, examiners, at the very minimum, should measure the empirical capital level against the minimum levels required in the regulation. However, it is more important to measure capital levels relative to the risk inherent in a corporate's balance sheet. This risk should be consistent with the corporate's own evaluation and be reflected in the goals the board sets. Thus, the examiner must ensure capital goals which corporates establish are adequate to meet these risks. This entails the quantitative review discussed previously.

More discussion of capital and the means to evaluate it are contained in the Empirical Capital Level and Capital Accumulation discussion in Chapter 401.

Additional Capital Requirement

Section 704.3(e) sets forth procedures by which the OCCU Director may determine the minimum capital requirements for an individual corporate are not appropriate. Examiners should be cognizant of any "significant circumstances or events" which might warrant either an increase or decrease in the capital levels established in the regulation. Since any action to adjust a corporate's minimum capital ratio must be taken to the OCCU Director, examiners will have to clearly document the case. Prior to taking any action to initiate a recommendation, the examiner should thoroughly discuss the issues with the corporate field supervisor and the OCCU Director.

Section 704.3(f) outlines the process by which a corporate must notify the OCCU Director it has failed to meet its capital requirement.

Section 704.3(g) describes the conditions that must be contained in a capital restoration plan submitted by a corporate.

Section 704.3(h) describes the process by which NCUA may direct a corporate to increase a capital ratio which does not meet the requirement of the regulation or take other actions to achieve adequate capitalization.

Examination Objectives

The objectives for reviewing capital adequacy are as follows:

1. Determine that the risk inherent in the corporate's balance sheet and operations, as well as off-balance sheet operations, are adequately supported by its capital position.

2. Determine that the corporate complies with the FCU Act, NCUA Rules and Regulations, NCUA issued Capital Directives and Generally Accepted Accounting Principles.

3. Determine if the corporate's capital policies, procedures, and practices, as well as internal controls are adequate to address the risk.

4. Determine corporate management and officials are adhering to established guidelines.

5. Evaluate the propriety and consistency of the corporate's present and planned level of capitalization policy, in the context of existing conditions and future plans.

6. Initiate corrective action when necessary.

Examination Procedures

See Corporate Examination Procedures - Capital (OCCU 204P).

Examination Questionnaire

See Corporate Examination Questionnaire - Capital (OCCU 204Q).

References

NCUA Rules and Regulations, Part 704, Corporate Credit Unions

Chapter 205

ACCOUNTING AND FINANCIAL REPORTING

Introduction

The purpose of the accounting and financial reporting review is to determine the corporate has appropriate processes in place to identify, measure, monitor, report, and control risk from its accounting and financial reporting activities.

Key issues surrounding these areas include: staff expertise/training, the level of separation of duties and internal controls, timeliness, staff turnover/cross-training, adequacy of policies/procedures, and the integrity of the financial statements/reports.

An in-depth review of a corporate's accounting and financial reporting area will be the exception, rather than the rule during annual examinations. This is primarily due to two factors as follows:

1. Corporates are required to have Certified Public Accounting (CPA) opinion audits which typically have unqualified (except for the classification of member shares as equity) opinions; and
2. Corporates have internal audit functions to address on-going internal control and accountability deficiencies.

Corporates are required to maintain accurate accounting records and financial reports based on Section 704.4(c)(4) of the NCUA Rules and Regulations and sound business practices. Additionally, Section 704.4(c)(3) requires the board of directors of a corporate credit union to ensure Generally Accepted Accounting Principles (GAAP) are followed.

The following accounting and financial reporting areas will undergo the most review during an examination:

1. Accounting and financial reporting policies, procedures, practices, and internal controls;
2. Federal Reserve, U.S. Central FCU, and other cash account reconciliation processes;
3. Suspense account reconciliation process; and

4. 5310 reporting process.

A more extensive or expanded review of the accounting and financial reporting area may be appropriate depending upon the circumstances existing prior to and during each examination. To help determine if a more extensive review is appropriate, examiners will complete the Corporate Examination Questionnaire - Accounting and Financial Reporting - OCCU 205Q.

EICs have the flexibility to reduce or expand the accounting and financial reporting review as deemed necessary. However, if the examination scope is changed subsequent to receiving the CFS’ approval, an EIC must justify why they plan to expand or reduce the scope and obtain CFS approval.

OCCU staff must be cognizant of situations that could be conducive to fraud and/or insider abuse. Examiners must determine adequate segregation of duties and internal controls are in place. Internal control weakness, poor documentation, improper internal audit relationships, inaccurate 5310s, un-reconciled accounts, and out-of-balance conditions are examples of significant accounting and financial reporting deficiencies most likely requiring corrective action. The degree and seriousness of these types of issues will help OCCU staff determine whether they are treated as a Document of Resolution (OCCU 102F) or Other Examiner’s Findings (OCCU 102G).

OCCU staff should not attempt to reconcile out-of-balance conditions. These types of concerns should be brought to the attention of the CFS prior to being discussed with corporate officials. OCCU staff should determine why the condition exists, whether management has adequate expertise/resources to resolve the problem, what steps will be taken to resolve the problem, and when the problem will be resolved.

Cash and Federal Reserve Accounts

A corporate’s cash and Federal Reserve Bank accounts are one of the most critical areas of the accounting and financial reporting review. It is imperative for OCCU staff to verify the Federal Reserve Bank account(s) are reconciled daily, adequate separation of duties exists, reconciling items are researched and cleared in a timely manner by corporate staff, and reconciliations are signed and dated by the reviewer and the preparer. To ensure this account is being properly reconciled, reconciliations as of the effective and current date must be reviewed. If the most current reconciliation has not been prepared for the last two business days, management must provide a reasonable explanation.

Examiners will perform a random sample review of the monthly cash account reconciliations, in addition to reviewing the reconciliations for the effective date of the examination. Related bank settlement and suspense accounts must also be closely reviewed. Reconciliation items should be traced to source documents along with any related correspondence, as deemed necessary.

Examiners must also perform a review of any overdrafts occurring with the Federal Reserve Bank during the examination period. If overdrafts have occurred, the examiner should ensure appropriate corrective action(s) has been taken by the corporate to minimize the likelihood of future overdrafts. Corrective actions vary but normally consist of policy and/or procedural changes, staff training, and/or increasing the minimum Federal Reserve Bank account balance.

Expenses

Normally, losses associated with the use of corporate credit cards and officials' expenses would not represent a significant risk to a corporate. However, if the examiner suspects or discovers abuses and/or expenses are excessive a review should be performed. When examining state chartered corporates, the EIC should coordinate the review of these areas with the SSA. EICs have the latitude to expand the review of the expense area as deemed necessary with the concurrence of the CFS.

Corporates involved in any type of shared expense arrangements with trade organizations or third parties will be reviewed for compliance with Section 704.16. Services, facilities, or equipment shared with any party must be supported by a written contract. Also, the contract must include the duties and responsibilities of each party specified, and the allocation of service fee/expenses must be fully supported and documented. Corporate staff should ensure it is not paying excessive fees by comparing fees charged to those of competitors in the marketplace. If OCCU staff perceives a problem, the CFS will be contacted prior to discussions with corporate management or the board. The consultation will help OCCU staff reach a supportable position regarding the extent of the problem, proper corrective action, and how it will be reported within the context of the examination report (Executive Summary, Document of Resolution, and/or Supplementary Facts).

Investments

Investment accounting is discussed in Chapter 201 of the Guide. The investment accounting review is normally performed by staff assigned to review the corporate's investment portfolio.

Future Dated ACH Transactions

For definition purposes, future-dated ACH transactions are debit and/or credit entry notices received by corporates from the Federal Reserve, which will post to a corporate's Fed account within a few days. The AICPA has concluded Generally Accepted Accounting Principles (GAAP) do not specifically address the accounting treatment of future-dated ACH transactions. In order to provide a consistent approach to reporting financial information within the corporate system, OCCU has instructed (Corporate Credit Union Guidance Letter No. 2007-04) all corporates to not record future-dated ACH transactions as assets and liabilities on financial statements for both regulatory and 5310 reporting purposes. Corporates, however, can report future-dated ACH transactions on their other external and internal financial statements based on the advice of their CPAs.

During regular supervision and examinations of corporates, it should be determined future-dated ACH transactions are reported as indicated above. A corporate, which incorrectly reports these transactions, may misstate their capital, NEV, and/or other financial ratios.

Examination Objectives

The objectives of the accounting and financial reporting review are to:

1. Determine policies, procedures, and internal controls for safeguarding assets, liabilities, and equity are adequate;

2. Determine corporate personnel operate in conformance with established policies, procedures, and internal controls;

3. Verify selected asset and liability account balances to ensure they are valid and are properly recorded;

4. Ensure cash and Federal Reserve Bank accounts are accurately reconciled in a timely fashion and reconciling items are researched and cleared in a timely manner;

5. Determine whether financial statements/reports generated by corporate staff are materially accurate;

6. Determine if the corporate complies with the FCU Act, NCUA Rules and Regulations, the Accounting Manual For Federal Credit Unions, and Generally Accepted Accounting Principles; and

7. Initiate corrective actions when material deficiencies or violations of policies, procedures, or internal controls are detected.

Examination Procedures

See Corporate Examination Procedures - Accounting and Financial Reporting (OCCU 205P).

Examination Questionnaire

See Corporate Examination Questionnaire - Accounting and Financial Reporting (OCCU205Q).

References

1. Federal Credit Union Act (Section 1756);

2. NCUA Rules and Regulations (Sections 704.3, 704.4, 704.15, and 704.16);

3. Accounting Manual for Federal Credit Unions;

4. NCUA Fraud Hotline - 1-800-827-9650 (703-518-6550 Washington, DC area);

5. Corporate Credit Union Guidance Letter No. 2007-04 Accounting for Future Dated Automated Clearing House (ACH) Transactions; and

6. Generally Accepted Accounting Principles.

Chapter 301

MANAGEMENT

Introduction

The quality of management is critical to the success of a corporate. Management consists of the board of directors (board), members of the various committees, and senior operational and executive management (senior management).

Together, the board and senior management are responsible for the ongoing management of the corporate's operations. Effective management entails the following:

- **Strategic planning**—A process to ensure current decisions consider the future operating environment, organizational goals, and performance measures.
- **Policy making**—The act or process of setting and directing the course of action to be pursued by an organization (e.g., government or business). Policies should be designed to implement strategic planning decisions.
- **Personnel administration**—The selection and retention of highly qualified management and staff. This includes appropriate recruiting, compensation, training, and personnel development activities.
- **Control systems**—The development or acquisition of systems to control and monitor delegated duties.
- **Management information systems**—The systems and reporting methodology which are designed to ensure relevant information is captured and delivered to decision-makers in a timely manner.

Since all corporate operations are unique and vary in degree of complexity, an examiner should not expect to find the same scope and documentation supporting the management process at each institution. However, there are minimum expectations at all institutions.

Board of Directors

The board has the ultimate responsibility for the corporate's strategic direction, policies and procedures, and risk management process. Recent trends have been toward a corporate governance structure whereby the board only develops regulatory and high level board governance policies. The board may delegate development of some operational policies to the corporate chief executive officer (CEO) and oversight of operations to senior management, but it remains responsible and liable for the consequences of unsound or imprudent polices and practices.

In today's environment, directors must have considerable knowledge and devote sufficient time to oversee a corporate's affairs. Although directors are usually credit union managers, their experience in these consumer financial organizations does not necessarily provide them with the experience needed to direct a liquidity facility and service organization such as a corporate. This can be true when the corporate has expanded authorities and/or engages in complex operations. In many cases, directors of corporate credit unions may need extensive training in the corporate's unique operations (i.e., complex investments, derivatives, and ALM). The information provided by management at board meetings may be extensive and complex. However, the information should be summarized in such a way as to provide directors with effective management tools. Directors must dedicate a significant amount of effort to become familiar with the subject matter.

Due to the emphasis placed on director duties, the evaluation of the board's effectiveness is an important examination function. When appropriate, regulators may facilitate this evaluation by direct contact with individual directors. The need to interview individual board members would be an exception rather than the rule and must be initiated by the examiner-in-charge (EIC). When this is done, it should be common courtesy to advise the board chair of the chosen course of action.

The determination of a board's effectiveness is based on evidence from various sources, including:

1. Review of written plans, policies, board and committee meeting minutes, and supervisory-related correspondence;
2. Interviews with board members and management; and
3. Assessment of the timeliness of board actions to address deficiencies and exceptions.

The board of directors should take appropriate actions to maximize strengths and to correct deficiencies discovered internally, or by regulators or independent auditors. Efforts to supervise an institution will be improved when the examiner correctly assesses the philosophy, degree of involvement, and capabilities of the board. Further, the performance of the board is often a useful indicator of future operating results and may reveal the need to revise the corporate's one-year supervision plan.

General Considerations

There must be an adequate system of checks and balances between senior management and the board. It is essential the board is promptly and fully informed of serious problems within the corporate. If directors are unaware of serious problems they will be unable to take adequate and timely corrective action to address risk or prevent large losses or even failure. Therefore, it is imperative management develop appropriate information and management reporting systems.

Board members are ultimately responsible for ensuring the corporate complies with all applicable laws, regulations, and rulings, as well as maintaining the safety and soundness of the corporate. The board is expected to exercise reasonable care and due diligence in carrying out these duties.

If directors fail to perform their responsibilities in an appropriate manner, they may be subject to various actions, including letters of understanding and agreement, cease and desist orders, orders of removal and prohibition, lawsuits by member, civil money penalties, and suspicious activity report filings.

Problems in financial institutions are usually attributed to a combination of the following items: self-dealing or other conflicts of interest, unsafe and unsound practices carried out by employees or management, unqualified management, lack of director participation, domination by one director or officer, or a disregard for the regulatory process. It is the responsibility of the board to prevent these situations from occurring through the development of sound strategies, internal controls, and policies.

Duties and Responsibilities of Directors

Section 704.4, and applicable state laws and regulations, delineate the duties and responsibilities of directors and limit certain types of activities. Statute and common law also assign broad fiduciary responsibilities to directors.

Assessing Board Performance

An assessment of board members' abilities to fulfill their responsibilities is essential. Although an assessment of the board is primarily qualitative, the following general considerations can be useful:

1. Focus analysis and discussion on the goal of continuous improvement and strengthening of risk management practices;
2. Concentrate on issues rather than on personal criticism. A critique of the board is a sensitive process that requires focusing on problem solving, not fault finding. Except where criminal violations might be cited, board member and/or employee names should not be used in the examination report; and
3. Determine accountability. Board members should demonstrate they are aware of and meeting their responsibilities.

Specific criteria should be considered in the examiner's analysis of the performance and effectiveness of the board. The directors should:

1. Operate independently from management;
2. Be informed of activities in which the institution is engaged;
3. Supervise activities by establishing policies, goals, and objectives;
4. Make strategic operating decisions;
5. Provide guidance for management;
6. Provide general business expertise;
7. Attest to reports of condition;
8. Maintain capital adequate for balance sheet and operational risks;
9. Avoid self-serving practices; and
10. Ensure the institution appropriately serves its members.

Although examiners are involved in ensuring corporates appropriately manage their risk activities, examiners do not manage their risk activities (i.e., this is the board's responsibility). Except where safety and soundness is at risk, examiners should refrain from expressing personal preferences or views.

Board Minutes

Significant financial, operational, risk management and strategic issues are discussed at the board and/or committee level, and should be documented in the board and/or applicable committee minutes. Minutes should be reviewed for:

1. Adequacy of reports. Reports submitted by senior management should be thorough and accurate. They should cover all aspects of the corporate's operations including capital, financial performance, and major operating reports. Reports should be provided in advance, allowing board review prior to the meeting, leaving time during the meetings for discussion;
2. Supervision of senior management's activities. Minutes should reflect the board's discussion and approval of any major strategic or operating decisions, as well as review and approval of all major operating policies. The board should ascertain senior management has developed procedures for all operational areas;
3. Attendance and participation by directors. Directors' attendance is usually outlined in the corporate's bylaws. Additionally, a corporate may have a board/committee attendance policy. Regular attendance is the only way directors can fulfill their fiduciary responsibilities. Minutes should also identify members who actively participate in discussions. Another indication of board involvement is participation on committees;
4. Evaluations of performance of executive management. Minutes should reflect review of senior management's performance and compensation package determinations. Note: This may occur in executive session and the examiner may have to request these minutes separately; and
5. Senior management's compliance with the board's directives. Systems should be in place to ensure senior management's actions conform to the policies and direction established by the board.

Executive Management

One of the most important decisions of a board in exercising its responsibilities is the selection of the corporate's CEO. The board should define in writing the CEO's duties and responsibilities as well as an adequate management succession plan. Additionally, the board should establish an appropriate compensation package given the size and complexity of the corporate and prevailing compensation for similar positions.

Compensation

In determining the compensation of senior management, the board of directors should consider the following:

1. The qualifications and experience of the individuals;
2. The compensation paid to other members of senior management;
3. The compensation paid to persons having similar duties and responsibilities in other institutions;
4. The size and complexity of the corporate and its operations;
5. The financial condition, especially capital position and income level, of the corporate; and
6. The value of the total compensation package provided to the employee (e.g., automobiles, club memberships, retirement plans, expense accounts, hospitalization and medical coverage, vacation, holidays, sick leave, life insurance, deferred compensation, etc.).

A competitive compensation program is essential in the recruiting and retention of highly qualified staff. The process for determining compensation may be based on market surveys provided by third party vendors or other sources. In any case, there must be an effective process to ensure compensation remains competitive with the passage of time and changes in the job markets.

Employment Contracts

Upon specific approval of the board of directors, a corporate may enter into employment contracts with its senior management and/or other employees. Contracts should clearly delineate performance standards and compensation. They should clearly define what actions or conditions may result in the termination of the employee(s). The board should review employment contracts and compensation arrangements, including renewals and extensions, for senior management, annually and shall document and justify its approval in the board minutes. This is generally performed as part of the annual performance appraisal process.

Sound Policies and Procedures

The directors must provide a clear framework of policies and procedures within which the CEO is to operate and administer the corporate's affairs. At a minimum such policies and procedures should cover all areas required by regulation, including but not limited to investments, credit risk, asset-liability management, OFAC, BSA, conflict of interests, and the Privacy Act. Other policies appropriate for board development and approval are code of conduct, membership, dividends, and personnel. The board may delegate approval of other operating policies to the CEO.

Policies are established guidelines for a corporate's activities based upon its strategic direction. Procedures represent the methodology for implementing an activity. Operating policies and procedures are necessary to establish management's strategy and to provide a basis for gauging performance. Properly developed policies and procedures generally result in effective and efficient operating performance.

The corporate's policies and procedures should:

1. Be tailored to operations;
2. Exist for all major operational areas;
3. Provide direction for activities;
4. Establish operational guidelines; and
5. Promote controlled and efficient operating practices.

Management's implementation of policies and procedures and adherence to operating standards may be an indication of the effectiveness of the board of directors. Positive indications of board effectiveness include:

1. Knowledgeable key personnel;

2. Clear strategic goals with established benchmarks for measuring performance;
3. Current, up-to-date policies and procedures;
4. Annual policy and procedure reviews;
5. Established internal controls to ensure adherence to plans;
6. Operations achieve stated objectives;
7. Personnel actions conform with policies and procedures; and
8. Monitoring of critical financial and operational functions.

Strategic and Business Planning

Planning is an organized and continuous process of ensuring projections of the future operating environment influence current decisions. Planning can be divided into two classifications: strategic (developing a strategy) and operational. Strategic planning focuses on the long-term deployment of resources to achieve corporate goals. Operational planning concentrates on short-term actions, which should flow logically from the strategic plan and be revised periodically.

The board should review and revise the corporate's strategic plan as necessary. A common practice is to update the strategic plan every three years.

Annually, the board is responsible for establishing a business plan that documents major financial goals and objectives designed to achieve the longer-term goals identified in the strategic plan. While management may develop such policies at the board's direction, the directors must thoroughly review and give final approval to each contemplated action. The board must also approve the budget and ensure it is realistic (in relationship to the corporate's operating environment) and provides for adequate capital.

Board and Committee Reports

To provide adequate oversight of corporate operations, the board must receive comprehensive, accurate financial and risk management reports from senior management and applicable committees. Reliance on only a few indicators such as benchmark financial statistics may result in erroneous evaluations of the corporate's condition. Key ratios are useful, but can be misleading without supplemental information or adequate explanation. The examiner should confirm the directors are receiving complete, understandable, and accurate reports for all significant financial and operational areas.

Each regular board meeting should include a review of financial reports. Directors should not simply accept questionable report figures at face value, but should question and verify them when necessary.

Committees

To carry out its functions, the board of directors may appoint and authorize committees to perform specific tasks and supervise certain phases of operations. Utilization of a committee does not relieve the board of its fundamental responsibilities. However, committees can assist the board in operating a safe and sound institution.

Contracts

The board has several major responsibilities in the area of contracts. Each contract must be legal and enforceable. Legal counsel should be well informed on credit union related issues and review all material corporate contracts. Once counsel reviews the contract, there should be no need to review it again unless there has been a significant change in a related law or the operations surrounding the contract. It is not necessary for the examiner to recommend that a board review its contracts periodically for legal purposes, unless changes in the law or operations have occurred.

Contracts need not be reviewed for legal considerations, solely because some or all of the board who signed the contract are no longer in office. The fact the current board is not aware of the financial impact on the corporate may be a reason for a board review, but not a legal review.

The contract must be beneficial to the corporate. The board has a fiduciary responsibility to protect the assets of the corporate. It must establish policies and require procedures that address the use, bidding, and awarding of contracts. Normally, a board will require that all contracts, over a certain amount considered to be reasonable, must go through the bidding and legal review process. Additionally, the board may require its own approval of contracts that commit the corporate to a significant level of expense.

Contracts that may require a bid or legal review include: employment contracts, purchase of computer hardware and software, leases on facilities and vehicles, insurance policies, and service contracts such as for audits, special reports, and operational evaluations.

The board is responsible for setting the bidding criteria, including the maximum amount of the contract. The contract need not be to the lowest bidder, but if not, other criteria must be clearly established and documented. The examiner should not take exception if the board has established clear policies and followed those policies.

Senior Management

Management includes senior management such as the CEO, chief financial officer, chief operations officer, chief risk officer, chief investment officer, controller, and any persons including division managers, who have the ability with or without explicit authority to implement and interpret a corporate's policies and procedures.

A major examination objective is to evaluate the quality and effectiveness of senior management. The success or failure of operations may relate directly to senior management. Senior management develops operational procedures and strategies and makes decisions within board policies, guidelines, and strategic plans.

In evaluating senior management's performance, examiners should consider the knowledge, skills, and abilities of the individuals, the results of their decisions, and the institution's regulatory compliance, financial soundness, and the adequacy of risk management processes. To assist examiners in this evaluation the following areas should be reviewed:

1. Strategic planning;
2. Policy and procedural compliance;
3. Personnel administration;
4. Adequacy of internal controls;

5. Investment review;
6. Asset-Liability Management;
7. Auditing;
8. Maintenance of management information systems; and
9. Loan review.

The major responsibilities of senior management are:

1. Proactive oversight of daily operations;
2. Developing procedures and processes to implement board policies and objectives;
3. Providing the board with accurate and timely information;
4. Filling staff positions with qualified individuals;
5. Ensuring there is adequate depth of staff (backup personnel) for all key areas;
6. Establishing sound and effective cross-training procedures; and
7. Identifying, measuring, monitoring, reporting, and controlling risks.

Planning

As noted previously, planning can either be strategic or operational. In either case, sound planning is fundamental to effective management and is key to anticipating and dealing with change. Management and the board should inventory the corporate's resources, examine changes in its operations, and determine its responses to those changes. Planning should be dynamic, carefully monitored, and well supported. Projections must periodically be revised as circumstances change and when new strategies are formulated.

Planning requires the collection and coordination of large amounts of information and the thoughtful efforts of all members of the management team. Written plans help ensure the board, executive officers, and all division managers share the same goals, objectives, and strategies. A common, shared perception of future strategic actions is critical to execution of a successful plan.

Examiners should note in the examination report management's failure to have a satisfactory planning process, to properly monitor and control adherence to a plan, or to adjust existing plans or risk management systems to address external factors such as economic cycles, interest rates, capital markets, and event risk. Examiners also should be alert for any deviations to strategic or operational plans that potentially may be detrimental to the corporate's financial and/or risk management soundness.

The Planning Process

As noted previously, strategic planning focuses upon the long-term, vision, direction, and allocation of resources to achieve goals and objectives. Operational planning, (e.g., the business plan), concentrates on shorter-term actions designed to implement the goals and strategies outlined in the strategic planning process. For an effective planning process, the operational plans must flow logically from the strategic plan.

The examiner must treat a corporate's strategic, operational, and business plans with maximum confidentiality. They contain sensitive and proprietary information that directly affect the corporate's market position and financial condition.

Human Resource Management

Human resource management includes establishing procedures for recruiting, selecting, promoting, replacing, appraising performance, devising a compensation system, and selecting staff for further development.

The following areas warrant attention in evaluating personnel management, as they are important indicators of an institution's viability:

1. Well developed personnel policies and employee handbooks;
2. Detailed position descriptions and performance standards;
3. Carefully planned recruiting and proper screening, including background checks, of new employees;
4. Appropriate training and cross-training;
5. Performance review and comparison to standards;
6. Salary and benefits administration; and
7. Employee turnover rates.

Management Succession

The examiner should evaluate the corporate's plans to maintain its present and improve its future condition. This should include an evaluation of the board and senior management's efforts to provide for succession of senior staff. The corporate should have an established succession plan for each key member of management.

Senior management and the board must anticipate the organizational knowledge, skills, and abilities needed to meet the corporate's strategic goals. Subsequently, internal staff may need to be developed and/or staff possessing the necessary skills must be acquired from external sources.

Response to Supervision

The examiner must determine an institution's compliance with findings and records of action. OCCU looks to management to implement corrective actions in response to regulatory requirements as well as safety and soundness issues. Management should establish policies and procedures to ensure continuing compliance. Corrective actions must be responsive to the cited weakness and implemented within agreed upon timeframes. If management disagrees with areas of concern and/or plans for corrective action, documentation supporting this position should be developed and provided to NCUA and the SSA (if applicable).

Conflicts of Interest

Avoidance of Conflicts of Interest

The phrase “conflict of interest” refers to any situation in which the safety and soundness or an opportunity for a corporate is in conflict with the personal interest of board members, committee members, management, the credit unions represented by board or committee members, or other persons with influence over the corporate's policies, procedures, and actions.

Conflicts of interest (and even the appearance of such) can adversely affect an institution's profitability, reputation and undermine public confidence in the corporate credit union system. A conflict could cause a financial loss if the individual involved considers self-interest and personal gain more important than the corporate's interests. Management has a fiduciary responsibility to avoid any conflicts of interest or appearance of conflicts of interest (see Section 704.5(i)).

Policies should address areas in which conflicts of interest could arise, including transactions involving the institution and parties related to directors or officers. It should also address controls to avoid abuses and establish procedures for dealing with policy violations. Some corporates cover such issues in code of conduct policy but it may also be covered in the personnel policy.

The examiner should comment on and specify appropriate actions on any actual or apparent conflicts of interest adversely affecting the corporate. Any conflicts of interest should be discussed with the EIC and the corporate field supervisor before being discussed with management.

Internal Controls

The board, senior management, and supervisory committee have important roles in an institution's programs of internal control and internal audit. Although the board has overall responsibility, senior management is charged with the duty of developing and maintaining a strong system of internal controls. Relying solely on the independence of auditors to establish the institution's internal controls is inappropriate. Senior management is responsible for the design and implementation of effective controls to prevent and detect errors, conflict of interest situations, and fraud. In addition, a strong internal audit and compliance function helps provide additional assurance regarding the effectiveness of such controls.

Meetings

Meetings with the Board of Directors

Meetings between examiners and the board provide an opportunity to discuss:

1. The examination process and findings;

2. The institution, its functions, and plans;
3. The general financial environment;
4. Industry-related concerns; and
5. Commitments for corrective action.

Exit conferences are held with members of the executive management team (and possibly the chair , other interested board members and supervisory committee members) to review technical and overall examination findings and to obtain commitments for corrective action. At this time the EIC should notify management of all examination related items slated for discussion with the board of directors.

Joint conferences may result from a regular or follow-up examination or a supervisory contact. Their primary purposes are to present and discuss examination findings and reach agreements on plans for corrective action. A secondary purpose may be to gather information regarding a new function or plans for the corporate. These meetings also may be used to enhance the board's understanding of the regulatory process and to establish and build lines of communication between the examiner and the board.

Joint conferences normally should be held in conjunction with the board's next regularly scheduled meeting or at another mutually agreed upon date. However, to ensure the timely delivery of the examination report, they should not be held later than 45 days after the conclusion of the examination's on-site fieldwork. The EIC should contact the board chair prior to the start of the examination to schedule the joint conference. When scheduling the meeting, the EIC should consider the time necessary to complete the examination report after the on-site contact is completed.

Ideally, the examiner and corporate management will have developed a mutually acceptable plan for correcting areas of concern during the examination. This plan will be discussed at the exit meeting. If that was not accomplished, it should be the major objective of the joint conference. If there are no major areas of concern to discuss, the examiner should use this opportunity to discuss with the board the general condition of the corporate and the board's view on its future operations. The board should be encouraged to discuss any matters of interest.

Meeting Preparation, Presentation, and Documentation

To ensure a successful meeting, the examiner should be thoroughly prepared, have adequate documentation to support the report's findings, and conduct the meeting in a professional manner. PowerPoint presentations are strongly suggested. The following are items to consider when preparing for a joint conference:

1. Determine a time and location;
2. Develop an agenda;
3. Ensure all participants (including ARDP of respective region) are informed of the meeting;
4. Meet with other examiners (if any) who are attending to discuss the agenda and their roles;
5. Prepare and organize supporting data, to illustrate significant points or trends; and
6. Prepare PowerPoint presentation and any handouts.

The following should be considered when making a presentation:

1. Conduct the meeting in a dignified, professional, and objective manner;
2. Present the agenda and follow it within reason;
3. Encourage board member involvement and questions;
4. Wait for the complete question to be asked and check for understanding before responding;
5. Do not attempt to answer questions without being able to offer complete and accurate information; and
6. Obtain commitments for corrective action from the board.

The effectiveness of the meeting is directly related to the extent communications is established and credibility maintained.

Meetings should be held with the entire board to ensure all directors are aware of regulatory findings and commitments to correct areas of concern. Any person or organization connected with the institution, such as an auditor or attorney, may attend a meeting subject to board approval. The confidentiality of the meeting should be stressed. If the examiner believes an individual present should not be at the meeting, those concerns should be addressed to the board chair. If the board wishes the individual to attend, the examiner should advise the board it is the board's responsibility to ensure the individual in question maintains the confidentiality of the issues discussed.

The examiner should prepare a detailed outline of the topics for discussion (PowerPoint presentations are one method.). Some of the issues that should be covered include:

1. Introductions;
2. Confidential nature of meeting;
3. Sign-in sheet;
4. Taping of meeting (NCUA would like a copy within a reasonable agreed upon time frame, if applicable);
5. Type of examination, scope, and other limitations;
6. Executive summary;
7. Document of Resolution;
8. Agreements;
9. Summary;
10. Other matters;
11. Questions from the board; and
12. Overall conclusions.

Examination Objectives

The objectives for reviewing management are to determine if senior management and the board:

1. Understand and adequately manage the corporate's operational and balance sheet risks;
2. Are qualified and understand their duties and responsibilities;
3. Carry out their duties and responsibilities in compliance with the FCU Act, NCUA Rules and Regulations, state laws, other federal regulatory agency rules and generally accepted business practices;
4. Develop and implement adequate policies and procedures for all financial and operational areas;
5. Implement a sound planning and decision-making process;
6. Address operational, examination, and audit deficiencies timely; and
7. Protect the assets of the corporate by sound contract administration.

Examination Procedures

See Corporate Examination Procedures – Management (OCCU 301P).

Examination Questionnaire

See Corporate Examination Questionnaire – Management (OCCU 301Q).

References

1. The Federal Credit Union Act;
2. Part 704 of NCUA's Rules and Regulations;
3. Section 701.14 of NCUA's Rules and Regulations;
4. Federal Corporate Credit Union Bylaws;
5. Corporate Credit Union Guidance Letter, No. 2003-05 Investing to Fund Employee Benefit Plans
6. Comptrollers Handbook – Management and Board Processes. http://www.occ.treas.gov/handbook/ss.htm

Chapter 302

PROFITABILITY

Introduction

The adequacy of a corporate credit union's (corporate) earnings relative to its capital accumulation strategies is a critical area of evaluation during the ongoing supervisory process. Each corporate's earnings performance must be evaluated in regard to its current capital position, financial and operational risk exposures, complexity of operations, and its strategies and business plans. The ongoing accumulation and maintenance of adequate capital should be the examiner's major focus when making an assessment as to the adequacy of a corporate's earnings performance.

The review of the corporate's earnings and financial condition is a continuing process. The pre-examination analysis and scoping process should identify any existing or potential problem areas requiring attention. A comprehensive on-site analysis substantiates and assesses current and prospective earnings. A well-performed analysis not only provides an understanding of the corporate's operations and earnings capability, but also identifies matters of existing or potential concern. Thus, the analysis can be used to facilitate corrective action that may avert problems or prevent existing problems from deteriorating.

The examiner should maintain a sense of balance when analyzing financial statements, avoiding undue precision or spending excessive time on immaterial amounts and/or items. Most importantly, the examiner should constantly maintain a sense of the examination objectives. Since earnings, over time, reflect the corporate's overall financial condition, the examiner should know the extent of existing or potential problems outside the purview of the earnings/profitability analysis. The examiner must maintain a constant flow of communication with individuals working on other examination areas in order to affect a cohesive and comprehensive review.

Finally, reporting errors, incomplete information, and deficient accounting information may hinder or prevent an accurate evaluation of the corporate's operations. A thorough analysis depends on accurate, reliable information and is an extension of reviews of the corporate's financial records and reports (i.e., financial statements, call reports, budget variance reports and board reports).

Relationship of Earnings to Capital Accumulation and Risk

Profitability must be evaluated in relation to each corporate's overall capital accumulation needs and risk exposures. Corporates that exhibit adequate levels of capital in relation to risk exposure and risk management practices will not necessarily require the same earnings performance as those corporates which have a low capital level in relation to regulatory requirements and risk activities. The examiner must keep this relationship in mind when evaluating the adequacy of earnings performance.

Each corporate's earnings must be evaluated with the following objectives in mind:

1. Determine earnings are sufficient to accumulate adequate capital levels; and
2. Determine whether the stability and mix of earnings components is appropriate to continue to accumulate or maintain adequate capital levels.

Components of Earnings

In order to obtain a complete and accurate understanding of a corporate's operations, it is essential to know the operating strategy of the institution. The operating strategy is identified in the corporate's strategic business plans and can be identified by determining major revenue and funding sources. Earnings components include interest income and expense, fee income, operating expenses, other income and expenses (operating or non-operating), etc.

<u>Interest Income</u> - Interest income consists of interest earned on loans and investments. The major contributor to interest income within a corporate is normally the investment portfolio.

<u>Interest Expense</u> - Interest expense is the corporate's cost of funding operations. Interest expense in a corporate includes dividends on shares, share certificates, member capital accounts, and interest on

borrowings (i.e., loans, reverse repos, commercial paper). For GAAP and regulatory reporting, dividends on paid-in capital accounts are not included in interest expense, but rather as a distribution of equity.

Net Interest Income (NII) - NII is interest income minus interest expense. NII is normally the primary source of income for a corporate and a key indicator of earnings performance and stability. This measure makes no adjustment for non-earning assets or liabilities that incur no explicit interest earnings or costs.

Net Interest Margin (NIM) - NII is called the NIM when expressed as an annualized percent of moving daily average net assets (DANA). A corporate can maximize its NIM by effectively allocating resources among earning and non-earning assets, maintaining low levels of non-performing assets, providing adequate funding through the lowest cost mix of funds, and maintaining a strong capital position. In a volatile interest rate environment, large changes in NIM are associated with high interest rate risk exposures and possibly weak risk management.

Net Interest Position (NIP) - A corporate's NIP is the difference between interest earning assets and interest paying liabilities. A shrinking NIP may indicate a weakening balance sheet and greater reliance on margins on products and investments for continued profitability. A negative NIP is considered a more serious weakness since it indicates interest-costing liabilities are financing non-interest-earning assets. Generally, corporates have sound NIPs due to low levels of non-earning assets. Shrinking NIPs should be reviewed by the examiner using a cost/benefit analysis of non-earning asset expenditures (i.e., will fee income and member service be enhanced).

Net Interest Spread - Net interest spread is the weighted interest rate received on average earning assets less the weighted interest rate paid on average liabilities.

Non-Interest Income - All other income.

Non-Interest Expense - Non-interest expenses are the costs of operating the corporate (i.e., operating expenses). A reduction in non-interest expenses will increase core earnings, net income, and market value. A well-managed level of operating expenses also allows the corporate greater flexibility with respect to managing net interest margin and levels of credit and interest rate risk.

Return on Assets and Equity

Return on Assets - Return on assets is net income divided by average assets. Traditionally, return on assets is the primary measure of a corporate's profitability. The examiner should review the level and trend of this ratio in relation to capital strength as well as financial and operational risks.

Return on Equity - Return on equity is net income divided by average equity. The return on equity is normally a ratio used by investors in the capital markets to evaluate investment options. Return on equity can be used to measure management's effectiveness in utilizing and accumulating capital to ensure strong net economic value and the long-term viability of the institution.

Evaluation of Earnings

An aggregate evaluation of all earnings components should be performed in relation to stability and trends.

Stability - The quality, composition, and consistency of income and expense flows should be evaluated relative to internal factors such as credit, interest rate, and operational risks, as well as external factors (i.e., general economic or competitive forces). The stability of earnings under different economic and competitive scenarios is critical in setting, attaining, and maintaining the capital accumulation objectives of the corporate.

Some corporates have positioned themselves as major providers of "back office" and correspondent services. The stability of service fees depends upon the proper management and promotion of these products.

Earning Trends - The general direction of a corporate's earnings relative to previous time periods should be considered during the analysis of profitability.

Through trend analysis the examiner should identify and investigate both adverse and positive trends within the corporate's earnings. Earnings trends must be viewed in relation to the capital accumulation and risk management objectives of the corporate. Trends must also be viewed in conjunction with macro-economic conditions within the financial markets as these conditions affect the entire System.

Analytical Techniques

Earnings analysis involves the review of financial data on a period-to-period basis in an effort to substantiate the reasonableness of financial performance without requiring a systematic review of transactions.

There are three primary components to performing a thorough trend analysis. These components are:

1. Twelve to twenty-four months of financial information for analysis;
2. Sound judgment in determining the materiality of variances; and
3. Volume-to-rate variance analysis.

The use of twelve or more months of data provides an understanding of what will likely be normal changes in the data. Given the seasonal funds flow inherent in corporates, at least twelve months of data must be observed in order to make an assessment as to any irregular changes or trends. By comparing variances over several accounting periods, patterns of change emerge that can be used to identify any unusual changes in current periods. Another benefit is an examiner can identify a change warranting further review.

The use of sound judgment in assessing the materiality of a variance in the data cannot be stressed enough. Examiners must use professional judgment when evaluating the change, but must also remember business is dynamic and change is inevitable. Only those variances that are not reasonable or are of a sufficient magnitude to justify additional review should be pursued. Such variances include cyclical and seasonal factors, changes in accounting practices and operating strategies. Positive or adverse trends should be identified and explained, so the findings support the overall evaluation.

Ratio Analysis - Ratio analysis is the method of comparing a figure or group of figures in a set of financial statements to another figure or group of figures within the same financial statements. It is predicated on the assumption there are meaningful relationships between different asset, liability, net worth, net income, and expense accounts.

Numerous standardized ratios have been developed for analyzing financial statements. The more commonly used ratios include:

1. Capital divided by moving DANA (Capital Ratio);
2. Reserves and undivided earnings divided by moving DANA (Retained Earnings Ratio);
3. Gross interest income divided by moving DANA;
4. Cost of funds divided by moving DANA;
5. Net interest income divided by moving DANA;
6. Operating expenses divided by moving DANA; and
7. Net income divided by moving DANA.

For additional discussion on analytical techniques, refer to Chapter 3, Total Analysis Process, found in the Examiner's Guide.

Budgeting and Performance Monitoring

The examiner should obtain a copy of the budget including projected revenues, expenses, and underlying assumptions (i.e., asset growth, sensitivity). An evaluation of this budget should include comparing:

1. Projections with prior period results;
2. Projections with actual results for the same period;
3. Projected return on assets and return on equity with prior period results;
4. Projected yields for major earning assets with prior period yields;
5. Projected operating expenses as a percentage of assets as well as revenues as a percentage of assets with prior period data; and
6. Projected goals and assumptions with trends and market conditions.

The key to evaluating the budget is to understand the validity of the underlying assumptions and the probability of projected goals. Prior data does not provide meaningful information if the entire focus of the corporate is changing.

Controlling business risks is one of the primary responsibilities of management. The types of risk assumed by the corporate, and how well management controls those risks, is reflected in the balance sheet and income statement. By analyzing the balance sheet and operating results in relation to projected goals, the examiner can determine whether management's policies benefit or adversely impact the corporate.

The examiner must determine the effectiveness of management's profit planning and control function. The examiner should not only make an assessment as to the reasonableness of the results of operations and budgeted goals and objectives, but should also determine management has an effective budget review and reporting process in place.

Product Line Profitability

In addition to making an assessment as to the corporate's overall earnings performance, the examiner should also determine management has effective processes in place to monitor the profitability of individual product offerings. Management should be performing a risk/return evaluation on each major product offering.

Periodic product profitability monitoring and reporting will provide management with valuable information regarding the effectiveness with which products are being offered to their members, and the competitive demand for those products. Maintaining and monitoring the results of individual product lines in relation to projected goals will provide a clear depiction as to where improvements may need to be made in order to benefit the overall earnings and competitive position of the corporate.

The examiner should determine an effective cost accounting process is in place that segregates revenue and expense by individual product line. The system should provide a reasonable allocation method for corporate overhead and shared expenditures. Individual product profitability reporting should be completed on at least a quarterly basis, with formal reports made to the ALCO or board at least annually.

Recordkeeping and Reporting

Complete and accurate records and reports are essential for a corporate's board and management in making informed decisions and in clearly understanding and supporting transactions. The corporate must also have appropriate policies, procedures, and controls to ensure financial reports and records are properly maintained. Inaccurate, incomplete, or unreliable information jeopardizes the safety and soundness of the corporate in that unidentified or undisclosed problems could prevent or delay corrective action and undermine the viability of the corporate.

NCUA must have reliable data so it can assess and monitor a corporate's financial condition and activities. It is imperative the corporate has adequate procedures and controls in place regarding the compilation of data used to prepare the NCUA 5310 Call Report (5310). Examiners will discuss these controls with management. The integrity of the corporate's books and records, internal reports, and 5310 data is essential if NCUA is to rely on the corporate's records for information throughout the examination, supervision, and monitoring process.

Examination Objectives

The examiner will address the following main examination objectives during the review of the corporate's earnings performance and profit planning process:

1. Determine and evaluate the corporate's policies, procedures, and controls for maintaining accurate income and expense reports and records;

2. Test the accuracy of balance sheet and income and expense data reported on monthly 5310 reports;

3. Evaluate the corporate's capital and earnings objectives and strategies;

4. Identify, evaluate and explain positive and negative income and expense trends;

5. Assess the prospective effect on earnings as a result of any changes in the activities or strategies of the corporate; and

6. Evaluate management's budgeting and reporting process to determine profit planning and control is being administered in an effective fashion to identify and achieve earnings and capital accumulation objectives.

Examination Procedures

See Corporate Examination Procedures - Profitability (OCCU 302P)

Examination Questionnaire

See Corporate Examination Questionnaire - Profitability (OCCU 302Q)

References

1. Office of Thrift Supervision, Examination Handbook - Earnings Section; and

2. National Credit Union Administration, Examiner's Guide, Chapter 3, Total Analysis Process.

Chapter 303

INFORMATION SYSTEMS AND TECHNOLOGY

Introduction

A corporate credit union's (corporate) information systems and technology (IST) program provides information services needed to effectively manage the organization. The board of directors and senior management have the responsibility to determine what information is needed to make informed decisions in line with business objectives and to monitor activities of the corporate. Additionally, the board and senior management are responsible for properly securing information systems. Part 748 of the NCUA Rules and Regulation requires a corporate to establish a written information security program to protect the institution's information systems. A written information security program will have at least the following four essential parts:

1. *Risk Assessment* – A rigorous ongoing process to identify risks to information assets. There are various risk assessment models available for reference (e.g., National Institute of Standards and Technology [NIST] Special Publication 800-30, OCTAVE [Operationally Critical Threat, Asset and Vulnerability Evaluation] and ISO [International Electrotechnical Commission] 17799). The following list taken from the NIST method is an example of what steps are necessary to perform an information security risk assessment. These steps would be applied to each asset to determine the level of risk exposure.

   - System Characterization
   - Threat Identification
   - Vulnerability Identification
   - Control Analysis
   - Likelihood Determination
   - Impact Analysis
   - Risk Determination
   - Control Recommendations
   - Results Documentation

2. *Policy* – Creates and governs controls deemed necessary to mitigate information security risks identified as a result of risk assessments.

3. *Controls* – Administrative or technical efforts to manage, monitor or protect systems.

4. *Testing* – Various procedures such as audits, penetration tests and vulnerability assessments. The frequency and nature of these tests should be based on the results of the risk assessment.

Corporate Role

As corporates fill the role of service providers for credit unions, the information security risks facing the corporate network also represent a systemic risk for the industry. Problems with information systems at the corporate level can have a downstream effect on the security**,** reputation and well being of credit unions.

Corporate Objectives

There are a number of objectives a corporate must address to ensure the security of its information systems. They are as follows:

- *Availability*—The ongoing availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users access to information or systems.

- *Integrity of Data or Systems*—System and data integrity relate to the processes, policies, and controls used to ensure information has not been altered in an unauthorized manner and systems are free from unauthorized manipulation that will compromise accuracy, completeness, and reliability.

- *Confidentiality of Data or Systems*—Confidentiality covers the processes, policies, and controls employed to protect information of customers and the institution against unauthorized access or use.

- *Accountability*—Clear accountability involves the processes, policies, and controls necessary to trace actions to their source. Accountability directly supports non-repudiation, deterrence, intrusion prevention, security monitoring, recovery, and legal admissibility of records.

- *Assurance*—Assurance addresses the processes, policies, and controls used to develop confidence technical and operational security measures work as intended. Assurance levels are part of the system design and include availability, integrity, confidentiality, and accountability. Assurance highlights the importance secure systems provide the intended functionality while preventing undesired actions.

Focus Areas

Examiners will review and assess information systems using four primary focus areas.

1. *Audit* - A well-planned, properly structured audit program is essential to evaluate risk management practices, control systems, and compliance with corporate policies.

2. *Management* - Management of (information technology) IT is critical to the performance and success of an institution. Sound management of technology involves aligning its IT infrastructure to support its business strategy. The board of directors and executive management should understand and take responsibility for IT management as a critical component of overall corporate governance efforts.

3. *Development and Acquisition* – The development, acquisition, and maintenance process includes numerous risks in today's dynamic and changing technology environment. Effective project management in development and acquisition will help reduce the possibility of loss resulting from inadequate processes, personnel, or systems.

4. *Support and Delivery (Operations)* - Effective support and delivery from IT operations is vital to the performance of most critical business lines in the institution. The risks, however, involve more than just IT technology and controls. They also include processes and staff.

The review of each of the four areas will help the examiner assess the adequacy and effectiveness of the controls put in place by management.

The following provides a narrative to be utilized in evaluating the four functional areas.

Audit

In order to determine the adequacy of the audit function an examiner will want to evaluate how well the risk assessment process feeds into the audit function. The results of risk assessments likely will call for mitigation strategies which will lead into additional controls to improve security. Those controls should be governed by policy. The audit function itself should be governed by formal policy as well.

When looking at the audit type, frequency and scope the examiner will determine if it is adequate given the technology employed by the corporate. Audit reports should be submitted to the board of directors or designated audit committee for review and proper follow-up on exceptions. Audit staff must be technically qualified to perform the reviews. Other considerations include separation of duties, potential conflicts of interest and audit staff involvement in the software development life cycle.

Management

Board Oversight

In order to determine the adequacy of board and senior management oversight there are several areas to evaluate. The examiner will want to look at whether the board approved an adequate framework to govern the IT function. Strategic planning should be coordinated with the corporate's business objectives. Significant changes planned for business processes, technology employed, key personnel, service providers or software development should be reviewed by the examiner. Management is responsible to adequately resolve IT deficiencies noted in internal and external reviews. Of primary importance is management's compliance with Part 748 of the Rules and Regulations requiring the development of an information security program. This requirement is discussed below. All corporates develop and/or acquire software so management must provide adequate oversight of software development and acquisition. Additionally, management is required to adequately plan for business continuity as well as mitigating business disruptions.

Outsourcing

The examiner will consider several items to determine the adequacy of the board's and senior management's oversight relating to outsourced technology services. A vendor management program should be governed by adequate formal policies and procedures. These would include proper due diligence completed prior to outsourcing technology services. (i.e. financial stability, GLBA, security, BCP, etc.) Adequate contracts will include confidentiality requirements and other important clauses and should be reviewed by the legal department. The vendor management program should include periodic review of critical service providers to ensure financial stability, adequate control environment, and adequate performance of service level agreements. Outsourced services should be included in the risk assessment and risk mitigation process as well.

Security Program

The security program has become the primary mechanism to protect a corporate's information assets as well as non-public personal information addressed by the Gramm, Leach, Bliley Act (GLBA). In order to determine the adequacy of the information security program the examiner will review and assess the critical risk assessment process. As with all functional areas the essential security program will be governed by policy. The risk assessment process should be governed by a board-approved framework with a methodology robust enough to identify risks to the corporate. Essentially the methodology should include a characterization of its systems and an assessment of the risks to information assets. (Refer to the introduction section of this chapter for examples of risk assessment methodologies).

In reviewing the risk assessment process the examiner should determine whether the corporate has:

- Identified and ranked information assets (e.g., data, systems, physical locations) according to a rigorous and consistent methodology that considers the risks to member non-public information as well as the risks to the institution;
- Identified all reasonably foreseeable threats to the financial institution assets;
- Analyzed its technical and organizational vulnerabilities; and
- Considered the potential effect of a security breach on members as well as the institution.

The examiner will also evaluate the risk assessment process for the effectiveness of the following key practices:

- Multidisciplinary and Knowledge Based Approach—A consensus evaluation of the risks and risk mitigation practices requires the involvement of users with a broad range of expertise and business knowledge. Not all users may have the same opinion of the severity of various attacks, the importance of various controls, and the importance of various data elements and information system components. Management should apply a sufficient level of expertise to the assessment.
- Systematic and Central Control—Defined procedures and central control and coordination help to ensure standardization, consistency, and completeness of risk assessment policies and procedures, as well as coordination in planning and

performance. Central control and coordination will also facilitate an organizational view of risks and lessons learned from the risk assessment process.

- Integrated Process—A risk assessment provides a foundation for the remainder of the security process by guiding the selection and implementation of security controls and the timing and nature of testing those controls. Testing results, in turn, provide evidence to the risk assessment process that the controls selected and implemented are achieving their intended purpose. Testing can also validate the basis for accepting risks.
- Accountable Activities—The responsibility for performing risk assessments should reside primarily with members of management in the best position to determine the scope of the assessment and the effectiveness of risk reduction techniques. For a mid-sized or large institution, those managers will likely be in the business unit. The information security officer(s) is (are) responsible for overseeing the performance of each risk assessment and the integration of the risk assessments into a cohesive whole. Senior management is accountable for abiding by the board of directors' guidance for risk acceptance and mitigation decisions.
- Documentation—Documentation of the risk assessment process and procedures assists in ensuring consistency and completeness as well as accountability. This documentation provides a useful starting point for subsequent assessments, potentially reducing the effort required in those assessments. Decisions to mitigate or accept risk should be documented in order to achieve accountability for risk decisions.
- Enhanced Knowledge—Risk assessment increases management's knowledge of the institution's mechanisms for storing, processing, and communicating information, as well as the importance of those mechanisms to the achievement of the institution's objectives. Increased knowledge allows management to respond more rapidly to changes in the environment. Those changes can range from new technologies as well as threats to regulatory requirements.
- Regular Updates—Risk assessments should be updated as new information affecting information security risks are identified (e.g., a new threat, vulnerability, adverse test result, hardware change, software change, or configuration change). At least once a year, senior management should review the entire risk assessment to ensure relevant information is appropriately considered.

As weaknesses are identified by the risk assessment the corporate may need to implement new or additional mitigation strategies. The examiner should test specific areas of the risk assessment to validate it against industry best practices. Once mitigation strategies are determined they should be addressed in governing documents. (i.e., policy, procedures, baselines) Following both the risk assessment as well as the policy and control formulation parts of the security program, management must provide an adequate audit function to validate those mitigation strategies.

In evaluating the risk assessment process the examiner will want to make sure it includes such areas as outsourced services and software development and acquisition. As the risk assessment is a key part of the security program it should provide adequate support for the security strategy, controls, and monitoring the financial institution has implemented.

Timing of risk assessments is very important. The institution should update the risk assessment prior to making significant system changes, implementing new products or services, or confronting new external conditions affecting the risk analysis. If these conditions do not apply, the risk assessment must be reviewed at least once a year.

An important part of the security program is the incident response program. This should be board-approved and, as with any control, it should be tested periodically. This can be done with simulations and walk-through exercises. The examiner should review and evaluate the corporate's incident response program pursuant to the requirements of Appendix B, II, A of Part 748 of the NCUA Rules and Regulations.

A yearly security program report is required by Appendix A, III, F of Part 748 of the NCUA Rules and Regulations. The appendix delineates specific items that should be included in the annual reporting to the board or an appropriate committee of the board. This report describes the overall status of the information security program and the corporate's compliance with the program's guidelines.

Development and Acquisition

Corporates engage in varying levels of development and/or acquisition efforts. In order to determine the adequacy of oversight relating to software development and acquisition an examiner will evaluate several items. The development and acquisition area should be governed by formal policies and procedures. As with any project management effort or strategic planning proposal, the software development project initiatives should also be aligned with business objectives. Adequate due diligence should be performed prior to software development. In reviewing this area the examiner will determine if the software development initiative is meeting project objectives (i.e., schedules, budgets, functionality). As noted, a risk assessment should be performed before any significant project is undertaken. Security and code reviews should be part of the software development life cycle used by the corporate.

Support and Delivery [Operations]

Network Architecture

All network designs should adequately address security through the use of firewalls and other devices. The examiner will review the network diagram for reasonableness based on the size and complexity of the network. The arrangement known as a demilitarized zone (DMZ) isolates incoming network traffic for evaluation before forwarding to the internal network. A DMZ should be used for publicly accessible servers such as web servers. Remote access from untrusted sources; that is, those not controlled by the corporate, should also terminate in a DMZ. The development area of a network should be segmented from production. The network design should adequately meet business objectives. With the majority of programs being accessed through the internet, robust perimeter security is of primary importance.

Intrusion Detection and Response

Intrusion detection and response is an important component for security of information assets. There must be a formal incident response plan as required by Part 748 of the Rules and Regulations in the event of a breach of data or systems. This should be governed by policy and tested periodically.

From a technical standpoint, in order for a network intrusion to be detected and mitigated timely, the corporate must have adequate intrusion monitoring. There are several methods and levels of intrusion detection. Intrusion Detection System (IDS) devices can be placed at various points within the network to protect internal areas of the network. Software can be placed on hosts to protect critical systems. The method or levels chosen by the corporate should be based on its risk assessment. The examiner will verify the intrusion detection method and response also includes outsourced services.

Physical Access to Critical Equipment

Access to critical equipment should be limited to personnel with a need to access the equipment to perform their daily duties. The equipment must be physically secured from unauthorized access. Locks with keypad or card access are common for most data centers.

There should be a level of monitoring to track who has accessed the data center. Often this is accomplished with keypad or card access software and/or sign-in forms.

System Access Levels

All computer equipment should be set up with access levels based on the user's job function and "least privilege" concept. The concept requires limiting access only to the systems and services actually needed by the user. The corporate should have a process in place to periodically review access levels. There should be an adequate and timely process in place to assure access is removed when an employee is terminated or when employees are absent for an extended period. The examiner will want to evaluate whether access level change procedures are appropriate. Administrative access to systems should be adequately restricted. Management should maintain an administrative access account and password offline in case of emergency.

Computer Systems Security

The security of computer systems should be adequately governed by formal policy and procedures. The patch management process must be sufficient to keep pace with the increasing threats to information assets. Management should also establish appropriate baselines for critical equipment. These baselines should have been addressed in a risk assessment to determine the level of risk and mitigation needs. Malware in the form of viruses, worms, Trojan horses, and key loggers are an ever present and changing threat. All institutions must have adequate malware protection.

Change Management Processes

The corporate should have a formal change management process that includes governing documents and procedures. No significant changes should be made to critical systems without formal management approval. Change management includes all hardware and software in the organization. Management should establish adequate baselines for change management.

Environmental Hazards

All critical equipment must be adequately protected by an uninterruptible power supply. The environment housing critical data processing equipment should be adequately controlled by an HVAC system. All critical equipment should be covered by a fire detection and suppression system, preferably a chemical based system as opposed to water. The computer room should be uncluttered and free from hazards.

Business Continuity Planning

Management is responsible for developing and testing a business continuity plan (BCP) to be invoked when various levels of interruptions occur to critical information systems. The portion of the IS BCP will be integral to the enterprise-wide BCP and should be coordinated appropriately.

Examination Objectives

The objectives for reviewing the information system processing are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control data processing risk.

2. Determine that the corporate complies with the FCU Act, NCUA Rules and Regulations, NCUA issued Directives, the Accounting Manual for Federally Insured Credit Unions, and GAAP, as they directly or indirectly apply to information system processing.

3. Evaluate the adequacy of security policies relative to the risk to the institution.

4. Evaluate vendor management related security controls.

5. Assess the adequacy of the corporate's security controls.

6. Initiate corrective action when the corporate's internal IST controls, policies, procedures, and practices are deficient.

Examination Procedures

See Corporate Examination Procedures - Information Systems Processing (OCCU 303P).

Examination Questionnaire

See Corporate Examination Questionnaire - Information Systems Processing (OCCU 303Q).

References

1. NCUA Rules and Regulations
2. FFIEC Information Technology Examination Handbooks
3. FFIEC Information Security Booklet of July 2006
4. OCCU Guidance Letters

APPENDIX 303A
IST Term Listing

This glossary of terms is not intended to be a comprehensive list. It focuses primarily on terms that relate to networks, network security, communications, and communication devices used on the Internet. An additional source of definitions can be found at http://whatis.techtarget.com/.

Term	Discussion
Access Control List	An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Windows NT, Novell's Netware, Digital's OpenVMS, and UNIX-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.
Account Lockout	This feature is available in most current network operating systems. After a specified number of logon attempts, the account is locked out and it usually requires a network administrator to unlock the account.
Administrator Account	This account manages the workstation’s user account, policies and resources. This account cannot be locked out or disabled. The Administrator account also controls files owned by other users.
Alpha Test	The first stage of testing a new software product, carried out by the developer’s staff.
Anonymous FTP	Using the Internet's File Transfer Protocol (FTP), anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available. If someone tells you to use anonymous FTP and gives you the server name, just remember to use the word "anonymous" for your user ID. Usually, you can enter anything as a password.
API -Application Programming Interface	Software that allows a specific front-end program development platform to communicate with a particular back-end database engine, even when the front end and back end were not built to be compatible.
Applet	An applet is a little application program. Prior to the World Wide Web, the built-in writing and drawing programs that came with Windows were sometimes called "applets." On the Web, using Java, the object-oriented programming language, an applet is a small program that can be sent along with a Web page to a user. Java applets can perform interactive animations, immediate calculations, or other simple tasks without having to send a user request back to the server.
Application	A computer program or set of programs that perform the processing of records for a specific function.

APPENDIX 303A
IST Term Listing

Archie	Archie is a program that allows you to search the files of all the Internet FTP servers that offer anonymous FTP access for a particular search string. Archie is actually an indexing spider that visits each anonymous FTP site, reads the entire directory and file names, and then indexes them in one large index. A user can then query Archie, which checks the query against its index. To use Archie, you can Telnet to a server that you know has Archie on it and then enter Archie search commands. However, it's easier to use a forms interface on the Web called ArchiePlex.
Auditing policies	A critical component of security monitoring controls. Auditing measures the system status against a pre-determined system setting and either will not permit a change or audit and send notifications of the change.
Authentication	The process of proving the claimed identity of an individual user, machine, software component or any other entity.
Bandwidth	The transmission capacity of a computer channel or communications line.
Bastion Host	A computer system that must be highly secured because it is vulnerable to attack, usually because it is exposed to the Internet and is a main point of contact for users of Internal networks. A web page server is an example of a bastion host. It gets its name from the highly fortified projections on the outer walls of medieval castles.
BDC - Back Up Domain Controllers	After a domain has been created, the entire account database is mirrored on each BDC. The PDC (see definition of PDC – primary domain controller) updates a BDC with changes usually at a minimum of every 5 minutes.
Callback security	A feature of remote access servers or software. When a user dials into a remote access facility, the server disconnects the session, and then calls the client back at a preset telephone number or at a number provided during the initial call.
CHAP – Challenge Handshake Authentication Protocol	CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works: After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it to its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.
Communications Protocol	A convention—a set of rules and procedures—for completing a communications systems task.
Corporate Security Policy	Defines the assets of a corporation, risks to those assets, owners of these assets and how to protect those assets. It includes creating security awareness among employees and having senior management support. It also defines the framework under which the entire corporation treats and reacts to attacks on its resources.

APPENDIX 303A
IST Term Listing

CRC – Cyclic Redundancy Check	An error-checking procedure for data transmission. The sending device performs a complex calculation, generating a number based upon the data being transmitted, and sends that number to the receiving device. The receiving device performs the same calculation after transmission. If the results match, the transmission succeeds. If the numbers don't match, it means the message was received in an altered state, and the data may be incorrect.
De-militarized Zone	In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the war in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.
Denial of service attack	A denial of service attack is aimed at preventing owners of a computer system from using it. It attempts to prevent the use of a system either by using all available processor resources, memory resources, network resources or by shutting down the system. A typical denial of service attack is to send a flood of e-mail messages to a mail server. If the mail server is inside a critical network, the traffic will either close down or severely slow it down.
DES - Data encryption Standard	A standardized encryption method widely used on the Internet.
Digital certificate	A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys.
Digital Signature	A digital signature (not to be confused with a digital certificate) is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.
Directory Replication	Any process that utilizes directory replication makes an exact copy of a file contents and places it on another server.
DNS – Domain name system	The DNS is a static, hierarchical name service used with TCP/IP hosts, and is housed on a number of servers on the Internet. Basically, it maintains a database for figuring out and finding (or resolving) host names and IP addresses on the Internet. This allows users to specify remote computers by host names rather than numerical IP addresses. The advantage of the DNS is that you don't have to remember numerical IP addresses for all the Internet

sites you want to access.

Domain	A group of computers containing domain controllers that share account information and have one centralized accounts database. The four domain models – single domain, complete trust, master domain, and multiple-master domain-represent various stages of growth and decentralization.
Domain controller	Authenticates users and grants them access to other resources within the network.
Encryption	The process of enciphering or encoding data so that it is inaccessible to unauthorized users.
Ethernet	A standard and probably the most popular connection type for LANs. It was first developed by Xerox, and later refined by Digital, Intel and Xerox (see also "DIX"). In an Ethernet configuration, computers are connected by coaxial or twisted-pair cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm.
Event Log	Network operating system services that records system, security, and applications events in the Event Log files.
Event Viewer	A tool used to review logged and audited events. It can be a tool within the operating system or an application designed to do this.
Extranet	The part of a company or organization’s internal computer network that is available to outside users, for example, information services for customers.
Finger	Finger is a program that tells you the name associated with an e-mail address. It may also tell you whether they are currently logged on at their system or their most recent logon session and possibly other information, depending on the data that is maintained about users on that computer. Finger originated as part of BSD UNIX. To finger another Internet user, you need to have the finger program on your computer or you can go to a finger gateway on the Web and enter the e-mail address. The server at the other end must be set up to handle finger requests. A ".plan" file can be created for any user that can be fingered. Commonly, colleges, universities, and large corporations set up a finger facility.
Firewall	A combination of devices and software that form a barrier between a secure network and an open environment. Firewalls examine incoming and outgoing communications on a network and determine if the traffic is permissible. Unauthorized communications are not permitted.
FTP - (file transfer protocol)	FTP is a method of transferring files over any network. It is used extensively over the Internet. Typical FTP servers are established for the purpose of giving open access to information. Critical files should never be installed on an FTP server. FTP servers typically should be placed outside a critical network.

Gopher	Gopher is an Internet application protocol in which hierarchically-organized file structures are maintained on servers that themselves are part of an overall information structure. Gopher provided a way to bring text files from all over the world to a viewer on your computer. Popular for several years, especially in universities, Gopher was a step toward the World Wide Web's Hypertext Transfer Protocol (HTTP). With hypertext links, the Hypertext Markup Language (HTML), and the arrival of a graphical browser, Mosaic, the Web quickly transcended Gopher. Many of the original file structures, especially those in universities, still exist and can be accessed through most Web browsers (because they also support the Gopher protocol). Gopher was developed at the University of Minnesota, whose sports teams are called "the Golden Gophers."
Group accounts	Accounts used for grouping together users who perform the same task or require access to the same resources. Group accounts eliminate the administrative headaches that would be created by granting resources to users on a per user basis.
Groups (Global)	Created on domain controllers and used to assign local permissions to domain users. The sole purpose of a global group is to gather users together at the domain level so that they can be placed in appropriate local groups. (see also local groups).
Groups (Local)	Local groups are defined on each machine and may have both user accounts and global groups as members but cannot contain other local groups.
Guest Account	Typically, this account is built into the operating system. It is designed for one time or occasional users. The problem with guest accounts is that they provide no audit trail or user accountability. They should rarely, if ever, be enabled.
HTML - Hyper Text Markup Language	The language in which World Wide Web documents are formatted. It defines fonts, graphics, hypertext links, and other details.
HTTP - Hypertext Transfer Protocol	The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol.
IMAP – Internet message Access Protocol	A standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail.
Intranet	A private network that uses Internet software (Web browsers, gophers, etc.) and standards (TCP/IP, FTP, HTML, etc.).
IP - Internet Packet	The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.
IPX/SPX	(Internet work Packet Exchange/Sequenced Packet Exchange) Protocol used to connect Novell networks.

ISDN - Integrated Service Digital Network	A communications service that encodes voice, data, facsimile, image, and video communications digitally so that they can be transmitted through a single set of standardized interfaces.
Land Attack	A denial of service attack in which the source and destination SYN (see definition of SYN) packets have the same address and the same port. This attack forces the computer to operate more slowly while trying to respond to packets sent to itself.
Latency	In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.
Logon scripts	Scripts are used to start applications or send environment variables for specific users or computers upon logon.
Nbstat	Tool used to display the contents of a remote computer's Net BIOS name table. The information listed in the Net BIOS name table can be used to determine the Domain name or workgroup the machine is in and the currently connected users. The information may also be used to uncover the Administrator's account due to the fact that account Station IDS are displayed in the name cache.
Net BIOS	Protocol used when Microsoft networking is required in a large multi-segment network. Net BIOS has many similarities to NetBEUI except for the fact that it can be routed with either the TCP/IP or NWLink protocols in a form known as an encapsulated protocol.
NetBEUI - (Net BIOS Extended User Interface)	The built-in protocol of Microsoft networking supports communication in a Microsoft-only environment when the network is small and composed of a single network segment. NetBEUI is a non-routable protocol, meaning that its packets contain no routing information and cannot pass through routers into other network segments.
Netstat	Tool used to display the status of the TCP/IP stack including what ports are open and what connections are active.
Network DDE	Service that provides a network transport as well as secured for DDE (Dynamic Data Exchange) Conversations.
NOS – Network Operating System	Software that controls the execution of network programs and modules.
NTFS - (New Technology File System)	The file system exclusive to Windows NT 4.0 Utilizes Windows NT File and Directory Security features so it is more secure than the File allocation Table File System (FAT) found in Windows 98, 95 and DOS systems.
Nwlink	Microsoft's implementation of the IPX protocol that allows connectivity between the Windows NT and the Novell NetWare Environment.
OFX - Open Financial Exchange	Open Financial Exchange is a unified specification for the electronic exchange of financial data between financial institutions, business and consumers via the Internet. Open Financial

	Exchange, which supports transactional Web sites, thin clients and personal financial software, streamlines the process financial institutions need to connect to multiple customer interfaces, processors and systems integrators. By making it more compelling for financial institutions to implement online financial services, Open Financial Exchange will help accelerate the adoption of online financial services by financial institutions and their customers.
OLE – Object Linking and Embedding	A Microsoft Windows capability in which an object from one application can be referenced from within another application.
OSI - Open Systems Interconnection	Standards for the exchange of information among systems that are "open" to one another by virtue of incorporating International Organization for Standardization (ISO) standards. The OSI reference model segments communications functions into seven layers. Each layer relies on the next lower layer to provide more primitive functions and, in turn, provides services to support the next higher layer.
Out of-Band Attacks	Service attacks where data is sent out the normal expected band that has been shown to affect Windows NT. This attack may cause Windows NT to have trouble handling any network operations.
Packet Filtering	The action a device takes to selectively control the flow of data to and from a network. Pack filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network or vice versa). To accomplish packet filtering, you set up a set of rules that specify what types of packets (for example, those to or from a particular IP address or port) are to be allowed and what types are to be blocked. Packet filtering may occur in a router, in a bridge or on an individual host computer.
PAP – Password Authentication Protocol	One of the many authentication methods that can be used when connecting to an ISP. PAP allows you to login automatically, without having to use a terminal window to type in your username and password. One warning about PAP: passwords are sent over the connection in text format, which means there is no protection if someone is "listening-in" on your connection.
PDC - Primary Domain Controller	The central server in the network that maintains the security database for that domain.
Performance Monitor	Tools configured to monitor system performance in Windows NT. It gathers vital information on system statistics and provides the information graphically. It can also be configured to send alerts when a hacker may be attempting to compromise security.
PING - (Packet InterNet Groper)	A standard TCP/IP network utility that sends packets from one machine to another in order to determine if there is a valid network route between them.
Ping-of- Death 2 attack	A variation on the original Ping-of -Death whereby multiple packets of either greater than 64 K in size or multiple 64 K fragmented packets are sent, crashing the receiving system.
Ping-of-Death attack	A security attack involving Ping. Issuing a Ping pack of larger than normal size set at 64 Kbytes causes the Ping-of-Death. This attack effectively takes the system off-line until it is rebooted.

POP3 – Post Office Protocol 3	The most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail.
Port	On computer and telecommunication devices, a *port* (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. The serial port supports sequential, one bit-at-a-time transmission to peripheral devices such as scanners and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers. 2) In programming, a port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, HTTP, have ports with pre-assigned numbers. These are known as "well-known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA). Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number. Port numbers are from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default and it does not have to be specified in the Uniform Resource Locator (URL). 3) In programming, to port (verb) is to move an application program from an operating system environment in which it was developed to another operating system environment so it can be run there. Porting implies some work, but not nearly as much as redeveloping the program in the new environment. Open standard programming interfaces (such as those specified in X/Open's UNIX 95 C language specification and Sun Microsystems's Java programming language) minimize or eliminate the work required to port a program. Also see portability.
PPP - Point-to-Point Protocol	Enables links between two points with no devices in between.
PPPMP - Point-to-Point Protocol Multilink Protocol.	An Internet standard allowing multiple protocols, such as NETBUI and IPX to be encapsulated within IP data grams and transmitted over public backbones such as the Internet.
PPTP - Point-to Point Tunneling Protocol	A Microsoft protocol under which remote users can connect to corporate networks through secure channels creating connections commonly referred to as Virtual Private Networks (VPNS). There are two implementations of PPTP today. One is a North American version featuring 128-bit encryption and the other is an exportable version with 40-bit encryption. (See also Virtual Private Networks).
Protocols	Languages used by computers. In order for two computers to talk to each other, they must use the same protocol.

APPENDIX 303A
IST Term Listing

Proxy server	A server between a client workstation on a network and the Internet. A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.
Public Key cryptography	Public key cryptography consists of a public key and a private key. The public key is given freely to anyone that needs it. The private key is kept secret by the owner of the key and is stored in the user's security file.
Public Key Infrastructure	Public Key Infrastructure (PKI) provides an encryption scheme offering privacy and user authentication. The concept uses a public key accessible by anyone, a private key for decrypting data encoded with your public key, and a pass code to protect your private key. Some experts believe PKI, when implemented properly, is more secure than your own signature.
PVC – Permanent virtual circuit	A software-defined logical connection in a frame relay network. A feature of frame relay, making it a highly flexible network technology is that users (companies or clients of network providers) can define logical connections and required bandwidths between end points and let the frame relay network technology worry about how the physical network is used to achieve the defined connections and manage the traffic.
Query language	A set of commands through which users can update, ask questions, and retrieve data from computer files.
RAID **-** (Redundant Array of inexpensive disks)	Enables a system to segment data and store pieces of it on several different drives, using a process known as data striping. The principal reason for implementing RAID is for fault tolerance.
RDB – Relational Database	A database in the form of tables which have rows and columns to show the relationships between items, and in which information can be cross-referenced between two or more tables to generate a third table. A query language is used to search for data. If data is changed in one table, it will be changed in all related tables. A database that has only one table is called a flat file database.
Registry	This is the database for windows NT. It contains all the system and program configuration parameters. It also contains the Security Access Manager and configuration data for applications, hardware and device drivers. It also houses data on user-specific profiles, desktop settings, software configurations and network settings.
Remote Access Service	A default service that enables users to connect over a phone line to a network and access resources as if they were at a computer connected directly to the network.
Replication	Creating and maintaining a duplicate copy of a database or file system on a different computer, typically a server. The term usually implies the intelligent copying of parts of the source database which have changed since the last replication with the destination. Replication may be one-way or two-way. Two-way replication is much more complicated because of the possibility that a replicated object may have been updated differently in the

	two locations in which case some method is needed to reconcile the different versions.
Rlogin	Rlogin is very similar to telnet and is available on many Unix and Non-Unix machines. Rlogin allows you to be on a local machine and to sign on to a remote machine (just like telnet). Rlogin may also require a password to allow system access. However, if it was set up in its default mode, chances are high that a password is not required.
Router	On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.
SAM - Security Access Manager	A data base that maintains all user, group, and workstation accounts in a secure database.
Server Alerts	Used to send notification messages to users or computers. Server alerts are generated by the system, and relate to server and resources use. They warn about security and access problems and server shutdown because of power loss when the UPS service is available.
Share	Created by granting a particular resource a share name. This name is what other users or devices recognize as the entity with which they have permission to access. Shares can be set up on files, folders, directors or server services, such as printing.
Share-level security	Used to give other users access to a local hard drive via the network. The four types of share permissions are No Access, Read, Change, and Full Control.
SLIP - serial line Internet Protocol	An older protocol used to carry TCP/IP over low-speed serial lines.
SMB - Server Message Block	Services that form the backbone of Microsoft networking in the Windows NT environment. All file and printer sharing in Windows NT operate using the SMB services.
SMTP – Simple Mail Transfer Protocol	A TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server.
SNMP - Simple Network Management Protocol	An Internet standard for monitoring and configuring network devices. An SNMP network is composed of management systems and agents.
SPAMMING	An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn't ask for it.

APPENDIX 303A
IST Term Listing

SSL - Secure Sockets Layer	SSL (Secure Sockets Layer) is a program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. Netscape's SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. This standard was offered free to the Internet community and is now widely used as part of the protocol for transmitting confidential data over the Internet.
SYN	A segment used in the start of a TCP connection to enable both devices to exchange information defining characteristics about the session. It is also used to synchronize the target and destination devices.
SYN flood attack	A SYN is a TCP request that can be sent to a server. When a flood of SYN requests are sent to a single server, the server can only respond with a reset to all further connection requests.
System Alerts	Critical security controls that help perform real-time monitoring of system resources, administrator and user activities. Alerts are configured in the network operating system typically the network administrator.
T1	A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T-1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet.
TCP/IP (Transmission Control Protocol/Internet Protocol)	An industry-standard suite of protocols designed for local and wide-area networking. Widely used for Internet communications.
Telnet	The Internet standard protocol to connect to remote terminals. Telnet clients are available for most platforms. When you Telnet to a UNIX site, for example, you can issue commands at the prompt as if you were directly at the machine.
Trojan Horse	In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse can be considered a virus if it is widely redistributed. The term comes from Homer's Iliad. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.
Trust relationship	A secure communications channel is established between domain controllers. Only servers with proper access rights can send and receive information across this channel. There are two types of trust relationships. The trusting domain which allows another domain to access its resources and the trusted domain-users in the trusted domain can access resources in a trusting domain.

APPENDIX 303A
IST Term Listing

UNIX	A Multitasking Operating System developed in 1969. There are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.
Untrusted Network	Any network in which secure communications have not been established between domain controllers. The largest untrusted network is the Internet.
UPS Uninterruptible power supply	A power system that provides short term power to critical computers so that in the event of a full power outage, the equipment can continue to operate until it can be safely shut down.
VPN - Virtual Private Network	A combination of software and hardware components that use public networks to create what appears to be a private network. A VPN-based remote access connection typically begins with a data connection to an Internet Service Point of Presence Server. From there, the data flows through a VPN session over the Internet (or other IP network) and ends at the corporate network gateway. All of the data that traverses the Internet is encrypted and authenticated providing the necessary security.
WAIS	Wide-area information servers (WAIS) is an Internet system in which specialized subject databases are created at multiple server locations, kept track of by a directory of servers at one location, and made accessible for searching by users with WAIS client programs. The user of WAIS is provided with or obtains a list of distributed databases. The user enters a search argument for a selected database and the client then accesses all the servers on which the database is distributed. The results provide a description of each text that meets the search requirements. The user can then retrieve the full text.
Whois	An Internet program (related to Finger) that lets you enter an Internet entity (such as domains, networks, and hosts) and display information such as a person's company name, address, phone number and email address.

Chapter 304

ITEM PROCESSING SERVICE CENTERS

Introduction

Item processing is the conversion of source documents, checks, and other transaction tickets to machine readable form, then processing and distributing this information in a manner that results in the ultimate settlement (payment or collection) through the Federal Reserve Bank (FRB) or another correspondent financial institution. Larger natural-person credit unions, corporate credit unions (corporates), credit union service organizations (CUSOs), leagues, banks, and national or regional check processing service centers typically perform item processing services.

The landscape of item processing services is and will continue to change. With the advent of Check 21, the increase in electronic funds transfer, the use of ACH and internet bill payment, the utilization of paper checks is declining. The FRB continues to consolidate its check processing units at a number of its facilities throughout the country. This restructuring will create additional opportunities as well as increased competitive pressures for corporates.

During the last several years, many corporate credit unions offering item processing services have streamlined their services by deploying full electronic image capture and presentment strategies. At some point in the future, traditional item processing of paper checks will be eliminated. To identify the risks associated with electronic capture and processing, it is important to understand the differences between paper and electronic check processing services. Discussion of both processing services is included.

Item processing is a term used to encompass all aspects of the check processing path from deposit to clearing of an item. Appendix A of this chapter is a glossary of commonly used item processing terms included to assist the reader. For ease of understanding, the following discussion on item processing begins with the initial depositing of a check.

Proof of Deposit Transit

Proof of Deposit (POD) transit (collection) is a common item processing service performed by corporates. This occurs when a corporate receives and processes checks, which have been deposited at a member credit union for credit to the individual member's account. The basic process is as follows:

1. A member or member business deposits the share draft(s) at its credit union (the corporate's member).

2. The credit union processes and balances the daily check deposits. Check encoding may be performed by the credit union or corporate, depending on the arrangement.

3. The credit union sends the day's check deposits with its cash letter (by courier) to the corporate.

4. The corporate processes, images, sorts, and sends the checks to the appropriate clearing agent (for sake of discussion it is assumed to be the FRB) for credit.

5. The FRB receives the check deposits (in the form of a cash letter) and then processes the checks.

6. The corporate's FRB account is credited. At the same time the accounts for the banks paying the deposited checks are charged for the payments and the checks are sent to those banks or their designated processor.

7. The corporate in turn credits its member credit unions the amount of deposits processed on their behalf.

Direct Presentment Arrangements

Direct presentment arrangements occur when two or more financial institutions, in a defined geographical area, agree to present their checks (deposits and payments in the form of cash letters) directly to each other, bypassing the FRB. These arrangements, in some cases, may involve formation of a local clearing association, with its own procedures and restrictions on joining the association. Direct presentment arrangements can exist for both deposits and share drafts.

Share Draft Clearing via Direct Presentment includes the following steps:

1. A vendor or consumer deposits a share draft at their financial institution.

2. The financial institution processes and sorts the checks which are encoded with the corporate credit union's routing and transit number.

3. The financial institution sends the checks and a cash letter directly to the corporate for settlement the same day.

4. The corporate sorts, images, and proofs the direct presentment checks to confirm the payment amount on the cash letter and creates an electronic file for posting (debiting) the payment amounts to the member share draft clearing accounts. A second electronic file is created with check data the member credit union needs to post against its members' accounts. Electronic check files are made available for the member credit union to download. For more information, refer to "Share Draft Inclearing."

5. The corporate then pays the local bank (by Fedline wire) for the member share draft deposits made at the bank.

Deposit Settlement via Direct Presentment includes the following steps:

1. The member credit union or participating bank sends a cash letter and the checks deposited that day to the corporate.

2. The corporate sorts the checks by routing and transit number to determine settlement paths. Checks identified for direct presentment are separated and bundled by participating bank. Each participating local bank receives a cash letter and a bundle of checks issued by that bank with a demand for payment to the corporate credit union.

3. The bank processes the checks and wires an amount to the corporate to settle payment for its cleared checks.

Share Draft Inclearing

Share draft inclearing is another common item processing service. This refers to the corporate's processing of member credit union share drafts. A corporate can receive its members' share drafts through a variety of intermediaries (from the FRB, via direct presentment arrangement, from a local clearinghouse, from other member credit unions, etc) The FRB is used as the intermediary in the following example of this process:

1. A credit union member pays a vendor with a share draft, which the vendor deposits into its bank account.

2. The bank processes this deposit internally by encoding and sending the share draft to the clearing agent (FRB, clearinghouse, direct presentment arrangement) for credit.

3. The FRB processes the share draft, credits the local bank's account at the FRB and charges the credit union's payable account through the corporate's account at the FRB.

4. The FRB sends the corporate (by courier) the cleared member share draft.

5. The corporate sorts and images the member share draft and posts the inclearing transaction from the FRB to the member share draft account.

6. The corporate makes an electronic file available of the drafts presented for clearing to the member credit union. The member credit union receives the file (via FTP or download from internet site) for processing against its members' accounts. Any checks unable to be paid by the credit union's members are listed on a share draft exception report, which identifies the reason the check was not paid.

7. The next morning, the member credit union uses the share draft exception report to identify any accounts with insufficient funds, closed or non-existent accounts, or other criteria preventing the draft from being paid. The credit union identifies share drafts to be returned, with the appropriate return reason code, and initiates the returns to the corporate.

8. The corporate physically pulls the item and sends it back to the FRB for return to the local bank and gives the member credit union immediate credit.

Item Processing Center Facilities

The most common equipment and related components of the item processing operation are:

1. encoding stations;
2. reader/sorter(s) (includes imaging process);

3. power encoders;
4. computer terminals for both the item processor controller and member credit union data systems;
5. reject/re-entry stations;
6. correspondence and/or adjustment desks used for resolving and researching differences with members, other financial institutions, and the FRB;
7. check storage areas both on-site and off-site; and
8. microfilming equipment.

Facilities should be organized in a manner resulting in an efficient, one-way workflow. The space allocated to item processing operations and related functions must be adequate to assure proper physical segregation of equipment and personnel. The following physical security controls are common:

1. controlled access, via card key or combination locks;
2. fire suppression systems;
3. water detection equipment below the floors;
4. hand-held fire extinguisher(s);
5. switches to activate an alarm when an electrical circuit is broken; and
6. sound and/or motion detection equipment.

In addition to physical controls over the item processing equipment, all negotiable instruments (checks, cash letters, deposits in transit, etc.) should be in a secure area from their initial receipt throughout processing, imaging or filming, storage and destruction.

Document Management and Data Backup

Properly stored and maintained microfilm imaging is essential for all item processing operations. Controls must be in place to safeguard the microfilm imaging stored on-site, and for maintaining at least one full copy off-site. Procedures must be in place to ensure all images are legible prior to placing it in storage. Processed data must be backed up daily. Adequate generations of backed-up data must be maintained both on- and off-site.

Written contracts must be in place documenting agreements for the satisfactory destruction of physical checks, cash letters, and reconciliation support. Items should be shred on-site and witnessed by a staff member, or transported in secured containers to a vendor location for shredding. Management must provide a sufficient record of the process, adequately documenting the destruction of items.

Contingency Planning

Management must ensure plans are in place to resume operations in a timely manner in the event of damage to the facilities and/or equipment. The item processing operation should be included in the corporate-wide contingency plan.

Management must:

1. establish legal agreements for the use of alternate sites and equipment;
2. develop procedures for all item processing operations under full disaster recovery situations; and
3. test fully item processing operations with alternate site equipment. The test must be realistic, comprehensive, and well- documented. Item processing functions must be fully restorable within hours of the impairment of item processing operations.

Item processing contingency testing should employ sufficient volumes of work to ensure operational staff can maintain the alternate processing function until standard operations resume. If there is limited equipment at the back-up site, management should consider temporarily obtaining available resources so comparable volumes of work can be tested, ensuring the adequacy of the backup function.

Transaction Volume and Trends

Supporting item processing operations requires significant investments in hardware, software, and human resources. High volume operations may require more than one reader/sorter. Backup equipment or backup capabilities at alternate sites should be in place or be contracted with third parties.

Potential Losses

Human error, fraud, failure to remain competitive, operational disruption, or catastrophic damage to the facility and/or items in transit can cause losses in an item processing operation.

The examiner should review lawsuits, pending litigation, and write-offs. Excessive legal problems and losses stemming from the operation could indicate deficiencies in management, internal controls, and/or contractual agreements.

Policies and Procedures

Comprehensive policies and procedures addressing services and day-to-day operations are needed to manage the risks inherent in item processing. The board-level policy or board-directed procedures should address the following, at a minimum:

1. specific services offered;
2. fee structure;
3. periodic cost analysis;
4. market factors, including market penetration studies, assessment of direct competition, and changes in technology (image processing, remote capture, proof of deposit, etc.); and
5. charge-off policies.

The examiner should review workflow procedures, which address operational functions in detail. These include but are not limited to:

1. departmental internal control structure;
2. operational deadlines and computer run schedules;
3. accounting procedures and requirements;
4. reject/re-entry and return procedures;
5. timely research and clearing of suspense items;
6. disaster recovery procedures;
7. personnel management, including cross-training and back-up schedules;
8. records maintenance and destruction procedures;
9. security measures; and
10. equipment care and maintenance.

Management must routinely review and update procedures, as well as staff's compliance with policies and procedures.

On an ongoing basis, management must monitor item processing operations, accounting reconciliations, clearing of adjustments, and compliance with deadlines. The board of directors should review monthly financial and operational reports regarding the item processing operations. Plans for resolving accounting and adjustment backlogs or problems in operations must be developed and implemented on a timely basis.

Management should develop flowcharts and/or narratives discussing the flow of items (deposits or payments) through the system. Tracing the flow of items through the system should document:

1. timely and accurate settlement occurs through the FRB or another correspondent bank; and
2. transactions post accurately to individual members' share accounts.

Contracts with Third Parties

The examiner should review all contracts for item processing services to ensure the following matters are addressed:

1. Settlement line of credit agreements between corporates and credit unions - These are needed to ensure the coverage of check clearing settlements if a member credit union's account balance is insufficient to cover clearings on a given day.

2. Disaster recovery agreements for alternate site and processing equipment - This is essential to ensure continuation of operations in the event of disaster.

3. Maintenance agreements - These are necessary to ensure appropriate software and hardware support. Maintenance contracts should include minimum service level agreements as well as maintenance response times for the vendor responsible for maintaining the equipment or software.

4. Agreements with the FRB and other exchange networks.

5. Agreements with any other hardware and communication vendors for funds settlement and electronic transmission activity.

6. Contract with document destruction company or certification of destruction.

Management and Staff Experience

The manager of the item processing department should exhibit a thorough knowledge of each functional area of the operation, as well as possessing management experience. Without a thorough understanding of each function, the manager cannot ensure the overall operation remains as efficient as possible. The manager should also exhibit awareness of new technology, and how to leverage it to increase the efficiency and/or profitability of the operation.

Cross training is critical in small and medium operations. Even in larger operations, management must have appropriate cross training and backup plans in place to cover unexpected absences and/or staff turnover.

Staffing levels must be adequate to maintain sufficient internal controls and separation of duties. Computer access controls and security measures must be in place.

Imaging systems can change or eliminate traditional controls, inherent in a paper-based system. Management should evaluate internal controls before implementing an image presentment system to ensure risks are appropriately mitigated. Internal audit procedures may also need redesigning to ensure a comprehensive evaluation and review of the image process. Institutions following best practices for project management normally include internal audit from the project planning stages forward.

Profitability Management

The costs of starting and maintaining an item processing operation are significant. A business or strategic plan must include item processing operations. Business plans should identify the services being provided and the resources needed to operate this area. Departmental cost, revenue projections, and analysis of the impact item processing operations will have on the corporate's financial performance must be properly documented. The business plan should include:

1. A description of the corporate’s operations, internal controls, management, staffing, training, hardware, software, disaster recovery, accounting support, and volume projections.

2. Long- and short-term financial and operational goals.

3. Marketing studies and plans, including analysis of competitors’ prices and services, and determination that existing demand and volume are sufficient to support the operation as an ongoing concern.

4. A detailed budget identifying the total expected cost and revenue of the item processing operations under varying volume scenarios. It is recommended examiners verify projected data volume for reasonableness regarding any corporate considering entering this business on its own or through the purchase of an existing processor.

In support of the business plan, management should complete a department profitability analysis at least annually. Management should ensure all costs of operating the department (e.g. facilities, human resources, internal and external audit, contingency planning, write-offs) are appropriately allocated to the operation. In that way, the true cost and profitability of the operation are determined and communicated to management and other users of the analysis. When analyzing profitability, it is important to ensure stable item processing revenues are not based on a combination of increasing clients and declining volume. The trend of declining volume can reasonably be expected to continue, while the increase in clients can not. If volumes are declining either on an absolute or per member (credit union) basis, the examiner should determine management has established a stop-loss threshold at which point services are phased-out and/or appropriately curtailed.

Effective management of an item processing operation includes continually reviewing the operation for areas where efficiency can be increased, and/or operating costs reduced, while maintaining reasonable internal controls and segregation of duties throughout the operation.

Document Imaging

Optical imaging systems provide a method of capturing, storing, displaying, printing, and transmitting data. Such systems offer the opportunity to streamline the item processing department workflow, reduce storage and retrieval costs, as well as improve customer service through automation. The following must be considered when installing document imaging in an item processing operation:

1. Planning - Poor planning can result in excessive installation costs, loss or accidental destruction of original documents, and failure to achieve expected benefits.

Issues for consideration in the planning stages include:

a. conversion of existing paper storage files;
b. integrating imaging into the organizational workflow; and
c. backup and recovery procedures.

2. Scanning Devices - Good quality scanning equipment is critical, as these devices are the entry point for all transactions. Workflow can be affected if scanning equipment cannot handle the volume, has frequent break downs, or does not meet image quality standards. Poor controls over the scanning process can result in poor quality images, improper indexing, duplicate item scans, as well as incomplete or forged documents being entered into the system.

3. Indexing - Proper indexing of documents is critical to future retrieval and limiting access to files. The integrity of the indexing must be carefully maintained in order to ensure and control access, as well as protect documents from unauthorized modification. The indexing method also can affect the security administrator's ability to restrict access based on the user's needs.

4. Software Security - System security controls over imaged documents are critical to protect the corporate and its members from unauthorized access and/or modifications to documents. Software security and security administrator functions are essential to prevent unauthorized alterations to stored documents.

5. Contingency Planning – A multitude of documents may be stored on a single optical disk; therefore, the loss of storage files or media can severely impact business if electronic backup or paper files are not maintained. The overall contingency plan should be modified to address the use of imaging in the item processing operation.

6. Training - Failure to properly train personnel responsible for operating scanning equipment can result in poor quality document images and indices as well as the premature destruction of original documents.

7. Legal Issues - Corporates installing imaging systems should carefully evaluate the legal implications of converting original documents to image, and the subsequent destruction of the original documents. Existing contracts should be reviewed to determine procedural changes are consistent with contract language and requirements.

Remote Capture

Remote capture is a sophisticated method of processing checks that a corporate's member credit union takes in from its membership. The check information is captured at the credit union location by a scanning device. The scanning device captures an image copy of the front and back of the check for automated processing. Typically, the software associated with the remote capture program automatically reads the MICR encoded information from the check as well as the legal amount line to populate the correlating fields in the software program. The image of the check or item and its encoding information is then transmitted to the corporate for further processing. The original checks can be truncated or maintained at the member credit union location. Credit unions no longer need to send the physical items by courier to the corporate. The corporate can print the images as a substitute check or transfer them electronically depending on the agreements in place. National networks exchange large volumes of images between financial institutions. Financial institutions are also collaborating to directly exchange images.

Remote capture technology also allows corporates to better serve their members with proof of deposit services. Typically, once the credit union scans its deposits and transmits the information electronically, it receives immediate credit that evening or the next morning for the deposit. This results in increased funds availability for the credit union member.

The corporate's item processing remains basically the same regarding remote capture. The primary benefit is items processed through remote capture are transferred electronically, reducing the paper being processed through the reader/sorter. The software and hardware (scanners and data storage) are expensive, which emphasizes the importance of the corporate having a realistic business plan to address costs, pricing and volumes.

It is important the process and controls involved with the electronic transfer and storage of images are reviewed during the information systems review. Protection of member data is essential for corporate credit unions and the credit union network.

Problem Areas

Common problems found in item processing operations include the following:

1. high staff turnover;
2. inadequately trained personnel;
3. inadequate staffing levels for proper internal control, accounting, and adjustment clearing;
4. changes in settlement patterns or procedures;
5. inadequate communication, hardware, and/or software may result in incorrect postings and reconciliations;
6. rapidly growing volume, added to existing inadequate staffing and inappropriate accounting systems;
7. weak internal controls and accounting procedures; and
8. backlog of reconciling and adjusting items.

Corporates exhibiting difficulties in new or established item processing operations may benefit from a third party review. A full third party review involves an evaluation of the accounting system controls and day-to-day operations of the department. Large public accounting firms usually have the expertise to review both functions of the department. Weaknesses in operations, management, and accounting identified during a review should result in the development of plans for prompt corrective action.

Regulatory Considerations

The following are two laws significantly impacting item processing and the security of personal information.

Check Clearing for the 21st Century Act

This law is commonly referred to as Check 21. Check 21 went into effect on October 28, 2004. The purpose of this law is to:

- Facilitate check truncation by creation of a new negotiable instrument known as a "substitute check;"
- Foster innovation in the check collection system without mandating receipt of checks in electronic form; and
- Improve the overall efficiency of the nation's payment systems.

The act does not mandate image exchange, provide any legal coverage for image exchange, or determine what constitutes legal presentment.

Gramm-Leach-Bliley Act (GLBA)

This act is also known as the Financial Services Modernization Act of 1999. The GLBA's privacy protections only regulate financial institutions. Financial institutions, whether they wish to disclose personal information or not, must:

- Develop precautions to ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Examination Objectives

The objectives for reviewing item processing service centers are to:

1. Obtain an understanding of the item processing operations environment.
2. Determine the quality of the item processing operations oversight and support provided by the board of directors and senior management.
3. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control the risk in its item processing operations (i.e., internal controls including physical and logical security, inclearing, exception and adjustment processing, account controls, etc).
4. Determine the reasonableness of business recovery strategies, data storage and backup methodologies.
5. Determine if item processing imaging systems and technology have an adequate control environment.
6. Determine corporate staff, management and officials are adhering to established guidelines.
7. Initiate corrective action when the corporate's item processing policies, procedures, practices, and controls are deficient.

Examination Procedures

See Corporate Examination Procedures - Item Processing Service Center (OCCU 304P).

Examination Questionnaire

See Corporate Examination Questionnaire - Item Processing Service Center (OCCU 304Q).

References

1. FFIEC Information Systems Examination Handbook
2. NCUA Examiners' Guide, Appendix C of Chapter 9 Item Processing
3. FFIEC Information Technology Examination Handbook: Operations

Appendices

304A Common Item Processing Terms
304B Item Processing Schematics

Appendix 304A

C0MMON ITEM PROCESSING TERMS

Adjustment - An entry requested by the corporate, member credit union, other financial institution, or Federal Reserve Bank because another institution has lost an item or cash letter, encoded an item incorrectly, etc.

Bank of First Deposit – The credit union where a member deposits a share draft. Also referred to as the BOFD**.**

Batch Processing - A group of transactions**,** deposits, or check clearings assembled for proving or processing purposes. A batch may consist of 100-300 items. Each batch is accompanied by a batch control ticket which records the batch number, control totals, and routing information.

Cash Letter – Bundles of items deposited or received together based on work type. They are accompanied by a cash letter form summarizing the enclosed bundle amounts and the total.

Clear on Tickets - An action initiated by a clearing house bank to debit the corporate for an adjustment.

Fine Sort - A term used to describe sorting transaction media into numerical or alphabetical order.

ICR or Intelligent Character Recognition – This usually refers to the machine reading of handwriting.

Imaging – A term referring to the process of capturing a digital image of share drafts.

Incoming Return Items - Items being returned to the bank of first deposit (also referred to as the BOFD).

Inclearing - A process whereby items are captured, imaged, sorted, and then presented to credit unions for posting to member accounts. Inclearing items include but are not limited to the following:

1. **Convenience Draft** - A draft against a credit card account.
2. **Corporate Draft** - A draft written by a credit union against its own account.
3. **Pre-authorized Draft** - An item initiated by a third party, with authorization by the account holder, to debit the share draft account for payment. Examples of pre-authorized drafts include health club dues, electric bills, and insurance premiums.
4. **Share Draft** - A written draft on a deposit account by a credit union member.

5. **Sight Draft** - An item initiated by a financial institution with an ATM, to debit a credit union for an error that occurred at that ATM, or a return item.

Infirmity - Any known act, or omission, that would invalidate an instrument (share draft). Common examples of infirmities that would cause a financial institution to refuse payment are missing endorsements, missing signatures, conflicting amounts in written and numerical figures, alterations, or forgeries.

IRD or Image Replacement Document – A reproduction of a share draft or the image of a digital share draft.

Item - Any media, excluding coin or currency, handled daily by a financial institution, which will be posted in total or in detail, as a debit or a credit, to an institution's account. Items are generally referred to by type, such as "cash items," "transit items," "on-us items," clearing items," "general ledger items," etc.

MICR - Magnetic Ink Character Recognition. Process used for encoding checks and/or other types of items to be processed. The MICR-line, which contains check routing account number and dollar amount information, is read to capture (read) the item and then sort it.

Mis-sent Item - An item which has been sent in error to another financial institution.

Mis-sort - An item sorted into the wrong account. A mis-sent item leaves the financial institution, while a mis-sorted item remains in the financial institution's possession, but causes a control problem.

Proof Machine - A machine with multiple pockets designed to balance and encode debit and credit transactions, accumulate pocket and grand totals, and sort the source documents according to type.

Reader/Sorter - A high speed document handler that reads MICR encoded information on documents for transmission to a computer and sorts the MICR documents on digits selected either at the unit console (off-line) or by the computer program (on-line).

Raised Check - A check on which the dollar amount has been illegally increased.

Reject - An item rejected from the reader sorter which has to be processed manually. Reasons for rejection include incomplete or unreadable MICR lines, or invalid check digits/account types.

Return Item - An item the member credit union returns rather than posting to the member's account. Examples of return items include insufficient funds, stop payments, account closed, unauthorized drawer signature, and uncollected funds. Items must be returned within 24 hours of presentment.

Routing and Transit Number - The numbers printed on checks to identify the specific institution on which a check is drawn and to which the check must be sent for payment by the Federal Reserve.

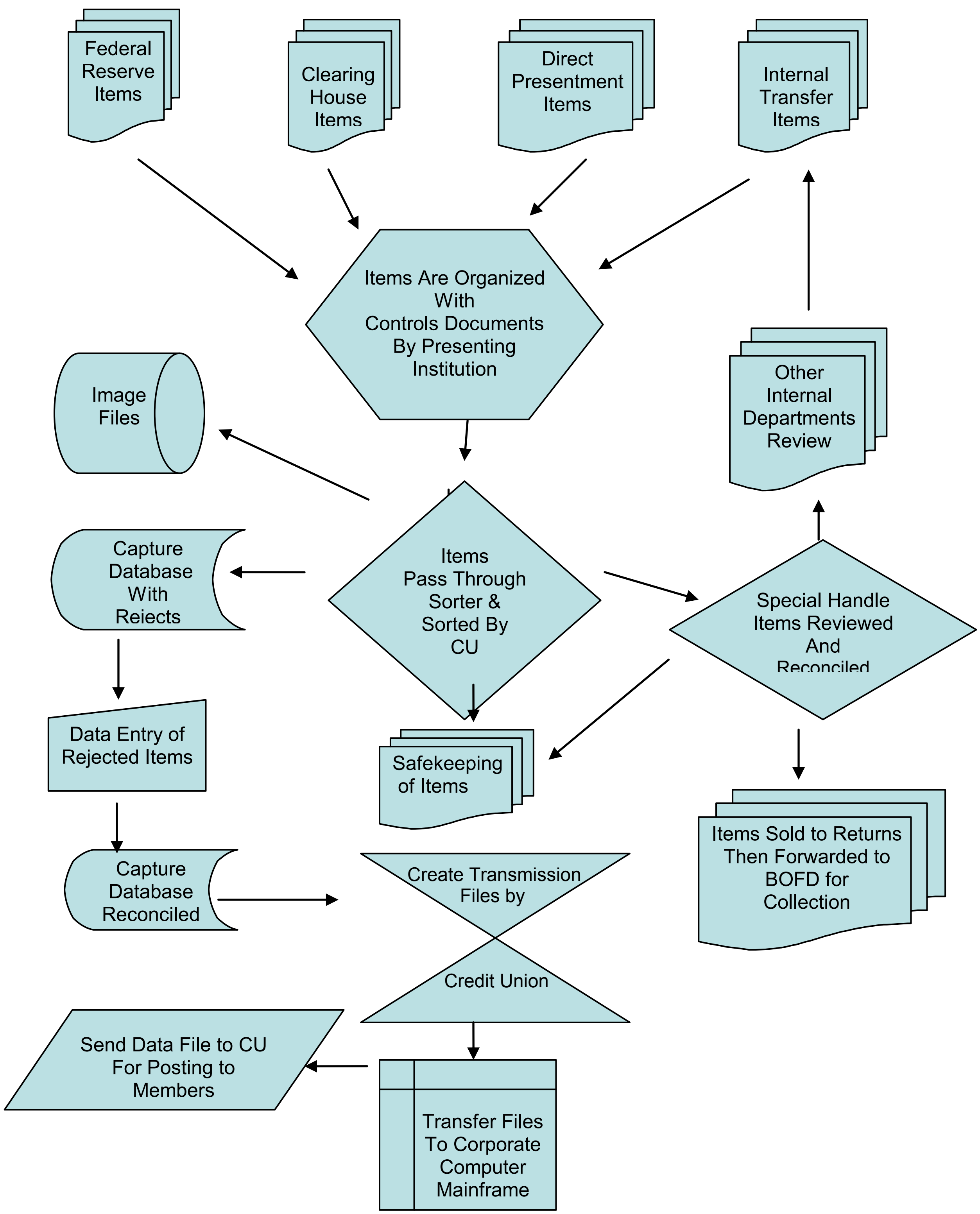
Substitute Check – This is a paper copy of the front and back of the original check. It is slightly larger than a standard personal check so it can contain a picture of the original check. A substitute check must be printed in accordance with very specific standards so it can be used in the same way (legal equivalent) as the original check.

Transit Item - A cash item drawn on a financial institution outside the immediate exchange area. Transit items are processed and sent to the Federal Reserve Bank(s), correspondent financial institutions, etc., for collection and remittance to the financial institution that originally received the items.

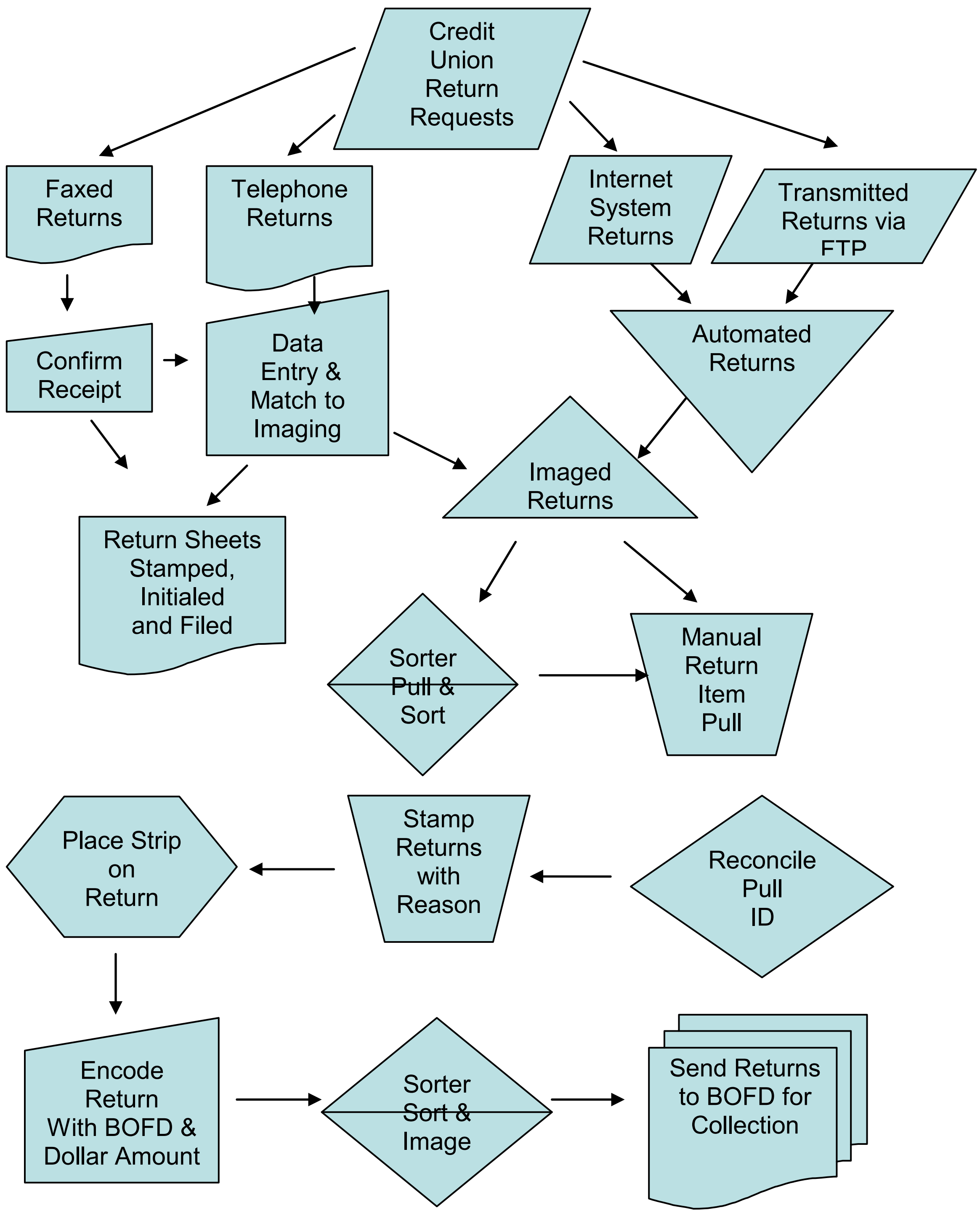
Transit Letter - A deposit form or remittance instruction slip that describes and gives totals of items to be collected and paid, enclosed with the checks and other cash items. The term “cash letter” refers to transit items sent to a financial institution where the remitting institution maintains an account. A “remittance letter” is sent when payment must be made (usually by draft) for the items sent.

Truncation - The process of distributing the original copies of cleared share drafts. In truncated processed drafts are stored for a prescribed number of days (usually 60-90), then confidentially shredded. Non-truncated processed items are returned to the member credit union and distributed to the members in monthly account statements.

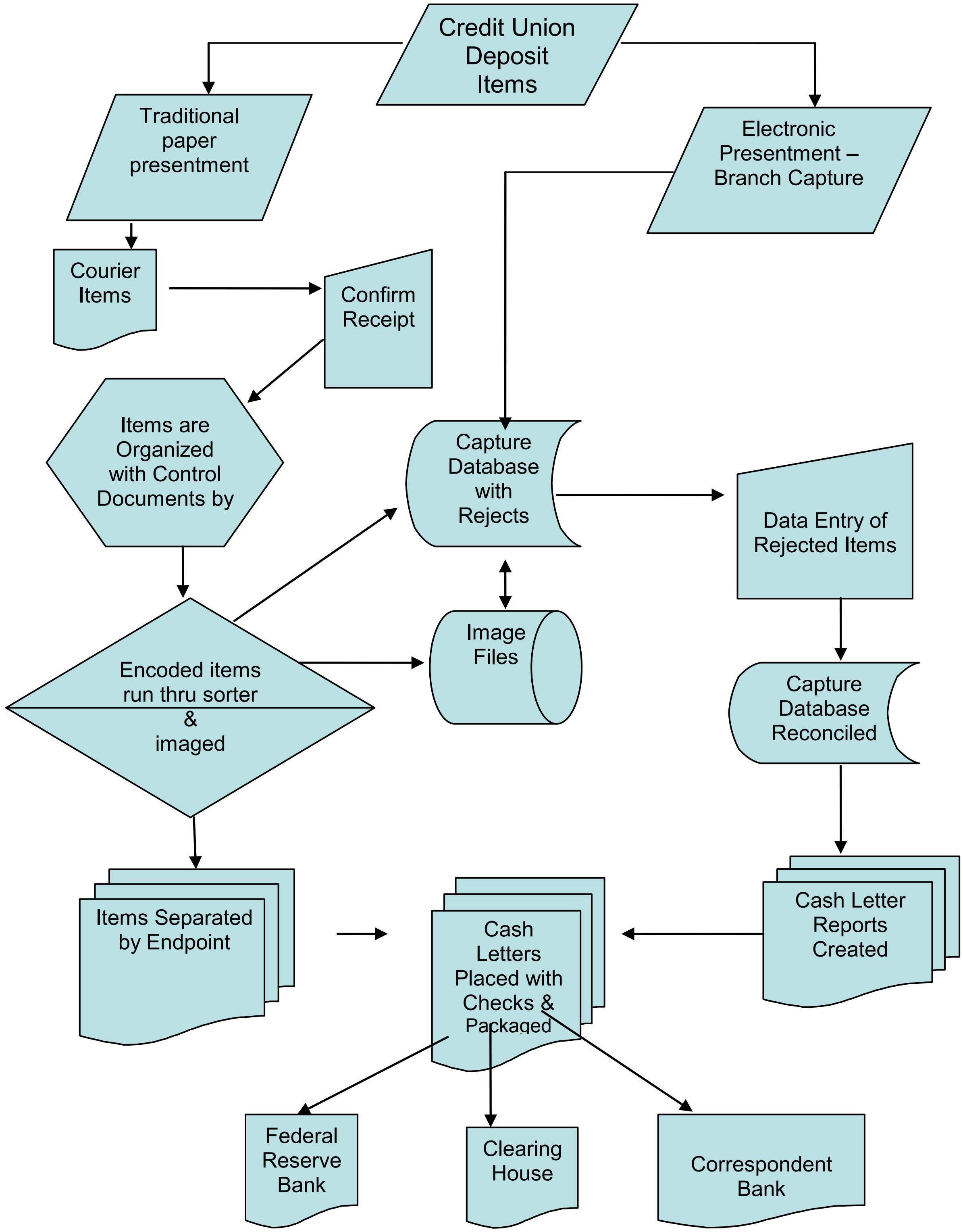
Inclearing Processing



Return Item Processing



Deposit Processing



FUNDS TRANSFER

Introduction

The funds transfer operation can present a high degree of risk to a corporate credit union (corporate), its members, and the credit union industry as a whole. In light of the potential for material losses through error, inadequate controls, or fraud, it is imperative the corporate establish a strong internal control environment over funds transfer activities.

Security measures are for the benefit of the members, as well as the corporate. A corporate operating under the impression its own internal security measures can be lowered simply because legal liability can be shifted from the corporate to the member is incorrect in its approach. If a corporate's inadequate procedures cause a member credit union to suffer a loss, the resulting adverse publicity could prove detrimental to the corporate credit union system (System) and credit union industry as a whole. Additionally, lax controls at any one corporate can simultaneously place many natural person credit unions at risk.

Methods of Affecting a Funds Transfer

Most corporates use the FedLine system to transfer funds into and out of their Federal Reserve Bank (FRB) account. Other methods include:

1. Sending funds through U.S. Central or another correspondent financial institution;
2. Sending funds through Open Door (see Appendix C for further discussion);
3. Manually communicating the request to the FRB by telephone;
4. Using Telex systems, such as Western Union; and
5. Using alternative software (such as YOJNA, IntraNet, FedPlu$, etc.) to access the FRB.

This discussion will address general controls over all funds transfer systems, including FedLine. Regardless of whether the corporate uses FedLine or other methods and systems for effecting funds transfers, the scope of the examination will include a review of policies and operating procedures, internal controls, logical and system controls, as well as segregation of duties surrounding the use of those systems and methods.

Whenever possible, and as software changes occur, the examiner should request the system user's manual from the corporate. The basic controls outlined in this chapter are applicable across all funds transfer software systems (e.g., dual controls, user IDs, security administration, physical security, transaction controls, and segregation of duties).

Managing the FRB Account

It is extremely important to ensure:

1. Funds transferred are frequently balanced to the corporate's FRB account (at least twice a day for smaller corporates; more frequently for larger corporates); and
2. A detailed reconciliation of the FRB account is accomplished daily by an individual not otherwise involved in the funds transfer process.

A daylight overdraft occurs if the corporate's FRB account is in a negative position any time during the business day. An overnight overdraft occurs if the corporate has a negative balance at the close of the business day. Items settle throughout the day into the corporate's FRB account, resulting in fluctuating daily balances. If the corporate does not carefully monitor its account activity throughout the day, and reconcile the account at the end of the day, overdrafts can occur. Examiners will ensure the corporate has procedures in place to adequately monitor and maintain its FRB account balance. Overdrafts in the FRB account can indicate the corporate is having difficulties in meeting one of its primary roles, that of a liquidity facility.

If a corporate has incurred overdrafts during the examination period, the reasons for the occurrences should be determined. Most corporates are considered Banker's Banks under the Federal Reserve's Payment Systems Risk Policy. This policy states a Banker's Banks should refrain from incurring overdrafts. They are usually required to post collateral to cover overdrafts if they do occur. The no-overdraft policy for Banker's Banks is primarily because these institutions are not required to maintain Regulation D reserves, and therefore, do not have access to the Fed discount window. Examiners should be aware if a corporate waives its Banker's Bank status, it then has the option of establishing overdraft cap limits as allowed by the Payments System Risk Policy.

Methods of Receiving Funds Transfer Requests

The payment order is the corporate's authorization to act on behalf of its member. As such, there must be controls in place to establish the authenticity and time of receipt of the funds transfer payment order. These two elements are the primary components cited by the Uniform Commercial Code Article 4A (UCC-4A) in establishing responsibility for executing the order. Most states have adopted variations of the UCC-4A and it is incorporated into the Federal Reserve System's Regulation J. It establishes responsibility for improper or untimely processing of a payment order, or cancellation, from initiation to final execution of an originator's orders. UCC-4A also requires establishing reasonable, commercially acceptable security procedures for both the corporate and the member.

The most indispensable and sensitive components of funds transfer activities are the messaging systems employed to generate payment orders. Payment orders may be made in a number of ways ranging from manual (e.g., memorandum, letter, telephone, FAX, or standing instruction) to internet and online telecommunications systems.

Telephone Requests

Corporates may receive their funds transfer requests by telephone. It is extremely important the corporate take appropriate steps to ensure telephonic requests for funds transfers are made only by an authorized individual.

Voice recognition is not an acceptable method for corporates to identify telephone callers requesting funds transfers. It is not reasonable to assume a corporate's employees are able to recognize the voices of many different employees from different member credit unions. Even the smallest corporates have multiple members using its funds transfer service, and most of those members have more than one individual authorized to make telephone requests to the corporate. Therefore, examiners will always take exception to this practice. The corporate should have an alternative means of verification or authentication.

Most corporates require the employee taking a funds transfer request audibly to repeat the information back to the member's employee making the request. This is done to ensure all details of the transfer are understood and accurate. All corporates should implement this procedure.

Recording Funds Transfer Requests

Most corporates use recording equipment to document telephone funds transfer requests. This security procedure is useful because recordings can be used to settle disputes between the corporate and member credit unions. Additionally, it deters initiation of unauthorized or fraudulent funds transfer requests on the part of corporate and/or member credit union staff.

Recording equipment generally is capable of recording several lines simultaneously. The cost of these systems can reach hundreds of thousands of dollars. However, since recording greatly reduces the risks associated with the funds transfer operation, this cost is usually justified.

Some corporates use desktop telephone recorders to reduce costs. They are not recommended as an employee can deactivate most systems, recording media must be changed more frequently, and they require more maintenance.

Corporates should have written procedures and strict controls over access to the recording equipment including the following:

1. Physical security over the digital recording equipment or tapes;
2. Designation of the person responsible for managing the digital system, electronic storage, or changing and storing of tapes;
3. Person(s) authorized to access and listen to recordings;
4. Requirements for periodically checking the quality of recordings;
5. Retention period for recordings (six to nine months is normal, but the corporate should review applicable laws and regulations); and
6. Procedures clearly prohibiting deactivation of desktop recorders, if used.

Electronic Delivery

Most large corporates use software systems or programs to move wire information via electronic receipt/delivery. Typically, corporates have modules in their online banking systems, which support domestic, international, and telex fund transfer requests. An interface between the online banking system and funds transfer software program allows messages to flow between the two systems. It is extremely important the corporate take appropriate steps to ensure the accuracy of these transactions. Examiners must review these systems for system and logical controls, user access, internal controls, and adequate written procedures. The systems should also be reviewed on the information system side to verify adequate network and data security is in place and information is protected (e.g., firewalls, encryption, authentication, etc.).

Telex

Examples of larger companies providing telex services for funds transfers are Western Union, RCA Globe, ITT World Communications, and Money Gram. Telex systems do not include built-in security features. It is the responsibility of the sending institution to incorporate a test key in all instructions to a receiver to execute a payment order. If corporates operate terminals for any company using telex services for funds transfers, the surrounding controls will be closely reviewed. Controls over origination, data entry, release, and balancing should be the same or similar to controls over regular funds transfers.

Written (e.g., by mail or in person)

Mail and in-person funds transfer requests are not an expeditious method of communicating a funds transfer order, so these types of requests are seldom used. However, if a corporate accepts such requests, the signatures on all requests should be compared to signature cards on file prior to processing the funds transfer. For written requests, a callback to verify the authenticity of the request also should be performed. For accepting in-person requests, the corporate should require the individual sign a request form and compare the signature card to the signature on file.

FAX

Faxing funds transfer requests is not recommended for the following reasons:

1. It is difficult, if not impossible, to determine whether the signature on a FAX request is original or has been cut and pasted onto the document;
2. It is impossible to positively authenticate the source of the request, as FAX machines can be programmed to put a false identification line on the FAX message; and
3. The requester's password is compromised if the message is intercepted, or if unauthorized personnel view the FAX message after receipt.

Some corporates insist FAX requests are necessary because members want to expedite a transfer, but have difficulty in reaching the corporate due to busy phone lines. The examiner will always discourage any use of FAX machines to receive funds transfer requests. However, if the corporate is willing to implement stringent additional controls over FAX funds transfer requests, exceptions may be considered. The following supplementary controls must be in place:

1. Call back all FAX requests, including those for "pre-authorized" funds transfers, to the original requester and a second authorized employee of the member credit union;
2. Prohibit the writing of passwords, PIN numbers, or test keys on the Faxed documents; and
3. Ensure written funds transfer agreements of those members that send requests by FAX on a frequent basis clearly describe the limitations of the corporate's liability for accepting these requests.

Telegram or Telex

Telegram and telex messages should not be allowed for receipt of funds transfer requests for the same reasons FAX messages should not be allowed. Except for requests originating from some remote foreign location, use of the telephone for requests is just as expeditious, and it allows the corporate to use the security procedures previously described.

Electronic Mail (E-mail)

E-mail funds requests are acceptable as long as the corporate ensures proper internal controls and security procedures are in place. Procedures must be designed to prevent the receipt of unauthorized messages, and to prevent interception and possible manipulation of authorized messages. At a minimum:

1. Passwords and controls should be on whatever system is used, both at point of origination and at the corporate;
2. Incoming messages must be accessible only by authorized corporate employees from the moment they are received (i.e., passwords and other machine-enforced controls);
3. A return message, confirming receipt of the request, should be sent to the member. This should be done in a manner which will ensure the return message is being sent to the member, even if the original message originated elsewhere; and

4. Missing required data should be resolved by telephone contact with the member.

Internally Generated Funds Transfer Requests

In addition to member funds transfers, corporates must move their own funds from institution to institution. Transfers for those corporates investing solely in U.S. Central are usually limited to a small number of destinations, such as the corporate's FRB account, commercial bank checking accounts, or U.S. Central. Since these requests are repetitive, they are likely to be established as pre-authorized (card or recurring template) funds transfer requests. As long as controls are in place over the creation of templates for the pre-authorized transfers, risk exposure is minimal. (See section on preauthorized transfers).

When a corporate transfers its own funds to a non-repetitive destination (e.g., investment transfers), greater controls are required, as follows:

1. Requests should be signed by or electronically authorized by two individuals in the investment department, or as designated by policy; and
2. The funds transfer department should perform a callback to the broker/dealer to verify the accuracy of the account number, amount, and other vital information before transmitting the funds. The telephone number and contact names should be from the funds transfer room’s existing records, not from information supplied by investment department personnel. (See section on callback criteria)

If either of these controls is not in place, the examiner will require their immediate implementation and document the deficiency as an examiner's finding.

Receiving Funds Transfer Requests from Foreign Countries

Due to complex security problems associated with foreign communications, acceptance of funds transfer requests directly from foreign countries is discouraged. Rather, the member credit union will be required to have its overseas branch relay the request to one of its offices within the United States, which should then contact the corporate.

If a corporate does accept foreign requests from a remote location (i.e., some third world countries), it may be received via telegram or telex, as that may be the only expeditious method of communication. Such messages should be received on a secured or "tested" telex system.

Controls over Passwords/PIN Numbers/Test Keys

The best way to identify callers and authenticate requests is by use of carefully controlled user IDs, passwords, PIN numbers, or test keys. The user ID, password and PIN refer to a word or string of characters or numbers, which must be supplied by the user (requester) in order to make the request. A test key refers to the association of a code with the individual funds transfer request. The code is based on a sequential number, calculation, or algorithm, which is tied to the previous message (request), which has been sent. The use of a "test key" is usually considered to be the most secure, since it is not as easily compromised.

Unless otherwise noted, the remainder of this discussion will use the term "password" to also include PIN numbers and test keys.

Allowing the same password to be shared by all employees of a member credit union is unacceptable. This practice increases the likelihood of controls being compromised and makes it more difficult to identify an individual and hold them accountable for their actions.

Some corporates assert written funds transfer agreements place legal responsibility for security problems, resulting from the sharing of passwords among the member's employees, solely on the member. Individual credit unions sometimes resist requests by the corporate to require separate passwords for each employee. Their typical objection is the inconvenience of assigning and maintaining a larger number of passwords. Such a position by the member credit union undermines the philosophy of the corporate that requires a high level of responsibility for security of passwords.

The method of assigning and communicating passwords to users must be properly controlled. The corporate should have written procedures for rectifying compromised password security by canceling the password and assigning a new one.

The password assignment and communication process must be independent of, and confidential from, operational staff who process funds transfers. The corporate must have security procedures over the process of communicating new passwords to or from individual users, as follows:

1. Passwords should be sealed individually in privacy envelopes which are sent to the member credit union's CEO, manager, or other board authorized individual;
2. A separate verification form should be inside each envelope, which is signed by the user and returned directly to the corporate;
3. There should be controls in place at the corporate to ensure no passwords are activated until the verification is received from the original user; and
4. All forms should be destroyed under dual control after their receipt has been recorded.

If the users at member credit unions are allowed to select their own passwords, controls must be in place over the communication of passwords. In addition, the corporate should require use of alphanumeric passwords instead of words found in the dictionary or commonly used. Users tend to select easily remembered words, or characters in a pattern, which increases the likelihood of passwords being compromised.

The corporate's funds transfer polices and procedures must require changing user passwords periodically, but not less than semiannually. In the case of an actual or suspected breach of security, passwords must be changed immediately.

Compromise of a password can occur in a number of ways. For example, an unauthorized individual may obtain a password from a rolodex file left exposed on a desk, or by looking over an employee's shoulder, and reading it off a computer screen. Taking specific precautionary measures can minimize risks. For example, Rolodex files should not be used for maintaining passwords. Corporate staff should never record passwords on paper funds transfer request forms, although there should be a notation area on the form where staff signifies the password was verified. Most corporates will enter phoned in requests directly into the wire transfer module, which usually has the ability to electronically verify the password.

Passwords can also be compromised if employees discuss them in places were they may be overheard. Policies and procedures should require employees not discuss funds transfer operational information outside the funds transfer area. Furthermore, the use of speakerphones to take funds transfer requests from member credit unions is not acceptable.

Passwords may also be stored electronically, either on the corporate credit union network (CCUN) system, a LAN (local area network), or within a fund transfer system. Some corporates use the "DCME" screen on the CCUN system to store member passwords. If passwords are stored on the DCME, access to this screen must be limited to those employees who receive or verify funds transfer requests.

There are also a number of computer applications, which are designed to generate and store passwords. If such systems are located on the LAN or some other system, security controls and network policies should limit access to the applications and directories to only those personnel needing access. Regardless of where the passwords are stored, access to this information should be restricted.

Passwords will be stored in some form (hard copy or electronic media) at the corporate's contingency site. These should be controlled appropriately, and there should be procedures in place to ensure a current set of passwords is maintained at the contingency site when passwords are changed.

Confirming Funds Transfer Requests

After a funds transfer request is received, but before the funds are actually transferred, the corporate should verify the authenticity and accuracy of the request. This is normally done by telephone callback; however, it can also be accomplished by E-mail or other secure means.

The most common method of confirming funds transfer requests is to make a telephone "callback" to the member credit union. Telephones "callbacks" serve to:

1. Confirm the accuracy of the request;
2. Confirm the request is originating from an authorized individual, from an authorized location; and
3. Reduce the risk of errors or fraud.

Since passwords and telephone callbacks have somewhat different purposes, they are not substitutes for one another. Telephone callbacks should be performed by a different corporate employee than the one who took the request (telephone call) from the member. Preferably, the callback will be made to an employee at the member credit union other than the employee who originated the request. This is sometimes difficult in small credit unions with limited staff. If the corporate does not require the callback to go to a second employee of the member credit union, the examiner will determine whether the corporate has taken appropriate alternative actions to protect its own interests (i.e., a liability disclaimer in the funds transfer agreement, lower wire transfer thresholds, etc.).

The corporate's procedures should require callbacks be made to the member's telephone number as listed in the corporate's official records. A "speed dialer" used during the callback process is unacceptable.

Employees may attempt to deviate from established callback procedures to save time. For example, callbacks should not be performed by having the employee who received the funds transfer request placing the caller on hold, then having another employee confirm the information. This greatly reduces the effectiveness of the procedure, since this method does not ensure an authorized user was calling from a member credit union.

Callback Criteria

There should be defined criteria in the corporate's procedures, outlining when callbacks are required. Common call-back criteria include:

1. All third-party funds transfers. The final recipient of a third party transfer is a party other than the member credit union or the corporate. The risk of loss is greater for third party transfers since the chance of recovering funds sent to a third party is less than recovering from the account of a member credit union;
2. All requests for establishing pre-authorized (card) transfers;
3. All funds transfers over a specified dollar amount; and
4. All investment funds transfers, which are not set up as a pre-authorized (card) wire transfer.

The criteria the corporate uses to determine which requests will be subject to callback should be maintained as confidential information. Knowledge of when a callback is performed would assist fraud perpetrators in evading the corporate’s security procedures. If the corporate has publicized the criteria, the examiner will recommend that it be changed, and the criteria be kept confidential.

The corporate should also perform random callbacks on requests falling outside normal callback criteria. This will deter attempts by both outsiders and corporate employees to circumvent established controls.

Electronic Mail Confirmation of Funds Transfer Requests

Funds transfer requests may be confirmed using electronic mail ("E-mail"), instead of telephone callbacks. Although use of E-mail to communicate with members is not common, this will change rapidly as corporates seek to further automate the funds transfer process.

If the corporate uses E-mail for confirming funds transfer requests, it must take steps to ensure integrity and control over the process, by determining that:

1. The system and its software have adequate security safeguards in place, both at the corporate and the member credit union; and
2. Any confirmation messages are transmitted to the system "address" listed in the corporate's records, and not sent to the address in the request message.

When other methods of confirming funds transfer requests are used, the examiner must use judgment in reviewing the controls surrounding these methods. The corporate must implement controls to minimize the risk of loss due to inadequate controls for confirming the accuracy and authenticity of a funds transfer request.

Post Telephone Audit of Funds Transfer Transactions

Some corporates have implemented an internal control procedure known as a "post telephone audit." In this procedure, an employee independent of the funds transfer operation telephones the member after completion of the transmissions of funds to confirm the authenticity and accuracy of the transaction.

Since the telephone audit is performed after the funds have been sent, it does not prevent errors or fraud from being detected before the funds are released. As such, the post telephone audit is not a substitute for telephone callbacks. The main purpose of the post telephone audit is to detect fraud. These telephone audits are usually performed on a sample basis, with the larger and more risky transactions (such as third party transfers) more likely to be included in the sample.

Pre-authorized (Card) Transfers

Many funds transfer requests processed by corporates are repetitive transfers, such as when a member credit union transfers funds to an investment account at another institution. Once established, the wiring instructions for repetitive transfers stay the same, except for the dollar amount. These transfers are called pre-authorized transfers, and most often, a template is prepared and utilized for recurring transfers. Pre-authorized transfers are also commonly referred to as "card" transfers because originally, institutions kept records of pre-authorized instructions on index cards.

Corporates usually handle repetitive transfers by establishing a template screen within the wire transfer system. Once established, a template reference, password or PIN number is associated with the wiring instructions. When a card transfer request is received, the caller must supply the template number, password or PIN number, and state a transfer for a certain dollar amount is needed to the credit union's account at "ABC Bank."

The caller does not have to give an account number or the bank's ABA number, thus saving time and allowing the transfer to be sent more quickly and efficiently.

The corporate must have additional controls over the creation of card transfers, as follows:

1. Creation or editing of the templates should be performed by someone other than the employees who perform the "initiation" and "verification" functions on the terminal; and
2. If the template screen is for an investment transfer for the corporate's own funds, then creation or editing of those screens should be performed by someone other than a corporate employee with investment authority.

Posting Funds Transfer Transactions

After the authenticity and accuracy of the request has been determined, the corporate is ready to post the transaction to the member's account. This should be done before the actual transmission, to ensure funds (or sufficient credit on a line of credit) are available.

Transmission of Funds

Funds transfer messages sent to the FRB must go through a two step process before the message is transmitted:

1. <u>Initiation</u> involves entering or uploading the message(s) into FedLine; and
2. <u>Verification</u> involves visually verifying file item counts and totals, or reentering all or part of the message into FedLine. Once the

verification process is complete, FedLine Advantage automatically transmits the message, and the funds are transferred.

If the data entered during verification does not agree exactly with the data entered during initiation, an error will occur, and the message must be correctly edited before it will transmit. (The verifier also has the option of canceling the message completely.) Since the data entered during verification must be exactly the same as entered during initiation, normally only numeric fields are verified. Critical numeric fields include:

1. The dollar amount;
2. The ABA number of the receiving institution; and
3. The receiving account number.

The accuracy of the transmission is dependent upon these numeric fields, not upon the words and names in the message.

The corporate's operating procedures must require two different employees to perform the initiation and verification processes. This should be reflected in the corporate's written policies as well as mandated by the machine controls set up for the funds transfer operating system.

Audit Copy of Funds Transfer System Messages

Messages on FedLine or any other funds transfer system should be retained either in printed or electronic format. Normally, messages are retained in three basic categories:

1. Outgoing transactions;
2. Incoming transactions; and
3. Miscellaneous messages.

FedLine Advantage and other funds transfer systems assign a sequence number to each message and each of the three message types has its own numbering sequence. Previously, corporates used multiple-part paper on the printers to record transactions. FedLine Advantage allows corporates to retain message data in electronic format. Whether in paper or electronic format, one copy of the day's messages should be maintained.

Other Security Features

Security Administrator

The Security Administrator (SA) is responsible for setting up new users on the funds transfer system, and setting the function levels of all users. The SA is a powerful user and has the tools to potentially bypass all security and effectively send a transfer with no supervision, if other compensating controls, such as dual verification, prompt balancing and timely activity log review are not in effect. Internal controls and proper separation of duties are important in protecting the corporate from significant risk. The number of SAs, usually between two to four, depends on the size and complexity of the corporate. The corporate should be able to justify the number of SAs. The SA should not have unaccompanied access to the funds transfer room or systems. If an SA does have unlimited access to a system, then the examiner should take exception to this situation.

User/Access Report Evaluation

The funds transfer system "User Profile Report" will be obtained for review during each examination. The examiner should ensure the report is generated as close as possible to the commencement of the on-site examination or supervision contact. The User Profile Report shows:

1. All authorized users;
2. Levels of user access; and
3. Authorities users have within each module.

The examiner should identify all users of this report and determine authorization levels ensure adequate segregation of duties and internal controls.

Staff members should not have more than one user ID. Doing so would enable them to bypass the verification requirement by signing on with the first ID to enter transactions, and then signing on with the second ID to perform the verification.

Verification Fields

Staff members with Supervisor function level or the SA have the ability to set the verification fields for funds transfers. Available options range from no verification of any field to required verification of every field. Verification refers to fields that must be sight verified or re-keyed by a second operator.

Supervisor Access Level

Wire room operating personnel should not have supervisory and level authority for FedLine Advantage. This authority allows modification of screen defaults and message status overrides. This should be assigned to staff independent of daily funds transfer duties. This setting also enables the user to create, change, and delete recurring wire templates.

Physical Security

Location of FedLine

PCs able to access FedLine Advantage should be located, if at all possible, in a secured room dedicated solely for that purpose, with only authorized staff and their supervisors having access. However, some (but not all) smaller corporates have limited space available and may take advantage of FedLine Advantage's open architecture, placing PCs in a specific, limited access, operations area. Stringent controls are needed if a corporate chooses this design over the traditional, secure wire room. In this case, the corporate should place PCs accessing FedLine Advantage in a low traffic area, but within sight of the workstations of all operators, and/or the operator's supervisor. Having PCs in a low traffic area will reduce the likelihood of unauthorized personnel gaining access to FedLine Advantage unnoticed. Having the PC within sight of the workstations of all the operators, and/or within sight of the supervisor, could also act as a psychological deterrent against any authorized operator initiating any unauthorized transaction. In addition, any other security controls available, such as a locking terminal cabinet, power-on passwords, etc., should be utilized when possible.

Number of Staff Present

At least two employees (that is, two employees who understand and have the authority to operate FedLine Advantage) should be present at all times when FedLine is in use. This should be a written requirement in the corporate's funds transfer policies and procedures.

Management should maintain a list of individuals authorized to be in the funds transfer room. Funds transfer room access should be restricted from unauthorized individuals such as maintenance staff, building management, etc.

Security of Telephone Lines

The corporate must establish controls to ensure all telephone lines are secure from eavesdropping. A breach of security could occur from either outside or inside the building. Security outside the building is the responsibility of the telephone company. However, security inside the building is the sole responsibility of the corporate. The examiner will ensure:

1. The corporate's telephone system does not allow one extension to listen in on another extension (not usually a problem, as most telephone systems in use today no longer allow this to occur); and
2. The telephone switching panel is secure within the building.

The location and security of the panel is important since, with the aid of some relatively simple equipment, an unauthorized person could listen to a telephone line at the panel. The room containing this panel should be locked, and the key maintained by management of the corporate. When properly controlled, management will know when a technician needs access to this panel. Each technician's identification should be checked, and proper precautions should be taken to avoid any breaches of security during times when the panel is unsecured.

Written Policies and Procedures

The Corporate Examination Questionnaire - Funds Transfer, OCCU 305Q, lists questions regarding internal control practices pertaining to the funds transfer operation. Many of the questions specifically ask whether certain practices are addressed in the corporate's written policies and procedures.

Written internal control practices ensure consistent application and enforcement, even when there is a change of staff or management. It is also easier to hold employees accountable for internal control practices when they are in writing.

Fraud risk is increased if an employee or interloper has the opportunity to gain unauthorized access to the system and initiate or alter a payment transaction in an attempt to misdirect or misappropriate funds. The following reduces fraud risk:

1. Written personnel policies and practices requiring, at a minimum,:

a) Vacancies in the unit be filled by internal transfers versus new employees, when possible;
b) Relatives be restricted from working in the accounting or data processing departments;
c) Individual responsibilities relating to security be in writing;
d) Written organizational security procedures exist;
e) Actions to be taken in the event of a security related incident be identified;
f) Formal training programs be developed to emphasize security and control;
g) Cross training exist within the unit;
h) Rotation of responsibilities be unannounced;
i) There be a minimum number of consecutive days of annual vacation;
j) Reassignment out of the unit be made when a notice of resignation is given; and
k) Terminated employees' sign-on ability is promptly canceled.

2. Management implementing adequate physical security controls, including the following:

   a) Limiting access to computer and communications equipment to authorized personnel;
   b) Protecting sensitive equipment within the secured area using access controls or device locks; and
   c) Securing and limiting access to all data on portable media (tapes, disks, hard copies, microfiche, etc.).

3. Management implementing the following to minimize risk of data loss and/or destruction:

   a) Purchasing commercially available software products to access production data files;
   b) Limiting access to specified programs or user IDs by setting up each file for read-only or read-and-write access; and
   c) Employing encryption, authentication, and dial back data protection techniques when accessing data-in-transit from one participant to another.

4. Management restricting access on software products using:

   a) Operator passwords to prohibit entry by unauthorized personnel;

b) Automatic features to control the number of unsuccessful password attempts, password expiration, or designated periods of inactivity;
c) Multi-level functions, by password, to require dual control and ensure no single employee can create and send transactions (e.g., restricting one operator to file creation and a second operator to file approval or transmission); and
d) System administration level procedures requiring secondary approval to assign, initiate, and maintain passwords.

5. Reconciliation of entries on the Federal Reserve Statement performed to verify the work settled as anticipated. Proper segregation of duties dictates staff responsible for reconciling transactions not be otherwise involved in the funds transfer processing.

6. Internal audits of the funds transfer process occurring on a periodic basis. Depending on the size of the corporate, audits could be performed internally or by a third party auditor. The size of the operation will dictate how often an audit of this area is performed. Examiner judgment should be used in this area.

OFAC Compliance with Wire Transactions

The Office of Foreign Assets Control (OFAC) of the Department of the Treasury administers and enforces economic sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals. While OFAC is responsible for promulgating, developing, and administering the sanctions for the Secretary of the Treasury, all of the financial institution regulators, including NCUA, cooperate to ensure financial institution compliance. The primary tool used is a listing by OFAC of "Specially Designated Nationals and Blocked Persons." The list changes regularly in response to changes in foreign policy. Corporate employees should be aware of the persons and entities on the list and assure such accounts and transactions are blocked or rejected and properly reported to OFAC. Software is available to monitor wire transactions.

Examiners must ensure the corporate is monitoring all funds transactions and the listing or software used is up-to-date. A corporate must monitor all funds that are transferred and cannot assume the member, U.S. Central, or the corresponding bank will review the transaction. Penalties can be assessed to each participant in the transaction. The corporate can receive additional information from the

OFAC website at www.ustreas.gov/ofac/ or by calling 1-800-540-OFAC(6322). Refer to the Compliance Section of the Examination Guide for additional information on OFAC and BSA compliance.

Written Funds Transfer Agreement with Members

The corporate should have a written funds transfer agreement with each member. The agreement should outline the duties and responsibilities of each party. The agreement's purpose is to protect the interests of both the corporate and its members. Among other things, it should specify the responsibilities of the member concerning security features such as password/PIN numbers/test keys and telephone "call-backs."
The corporate should obtain the advice of its attorney in drafting the agreement. Written documentation, on the attorney's letterhead, should be maintained as an indication the attorney:

1. Reviewed the agreement;
2. Found it to be in compliance with applicable law;
3. Believes it is adequate to protect the corporate's interests; and
4. Believes it adequately addresses the issue of "commercially reasonable security procedures" as discussed in Article 4(a) of the Uniform Commercial Code.

In addition to the agreement, the corporate should have written documents from each member indicating certain employees or officials authorized to request funds transfers. This may be the only document maintained by some corporates. In those cases, the examiner will take exception and require development of a formal funds transfer agreement.

Personnel Policies for Funds Transfer Operation

Even a corporate with a sound internal control structure may hire individuals who could commit funds transfer fraud. Personnel policies should be in place, which will reduce the possibility of hiring such individuals. Having an appropriate level of due diligence in the hiring process would help reduce this risk. Consistently applied written hiring policies and procedures improve the corporate's chances of a surety bond action if a claim is made against an employee.

The corporate should have written procedures addressing the review of references of funds transfer staff, including but not limited to:

1. Credit checks;

2. Bondability checks;
3. Prohibition checks; and
4. Criminal background checks.

The procedures should detail how background checks are completed. Procedures for verifying references and documenting the verification should be detailed. The corporate should be aware a bondability check only identifies whether the potential employee is bondable by the corporate's bonding company. (Normally, a corporate's bond is held by a company that specializes in credit union bonds.) These bondability checks attest only to bonding actions, which may have occurred as the result of previous credit union employment. If the individual committed previous crimes at some other type of financial institution, the bonding company may not be aware of these. Criminal conviction checks should not be limited to the state and municipal court records where the corporate is located. Federal court records should also be investigated, as many financial institution fraud cases are handled at that level.

The process of performing pre-employment credit and background checks involves a number of sensitive employment and privacy laws, many of which differ from state to state. Appropriate disclosures must be given to the applicant prior to performing credit and/or background checks. The corporate should always ensure the review and concurrence of legal counsel in determining its pre-employment policies and procedures.

The corporate should also have procedures, which address what steps should be followed when funds transfer personnel give notice of resignation, or are terminated. The procedures should include that immediately upon either occurrence, these individuals should be relieved of funds transfer responsibilities, and all access and authorization levels canceled at both the corporate and the Federal Reserve Bank. Access devices, if applicable, should be collected and destroyed. Employees should be transferred to a non-sensitive area after giving notice of resignation.

Contingency Planning for Funds Transfer Operation

Restoration of funds transfer operations is a critical factor in disaster recovery planning. If the corporate does not normally have a high volume of funds transfer activity, emergency funds transfer operations can be conducted manually via telephone contact with the FRB. If the corporate plans to use the telephone, staff must know the location of the back-up code word list.

If the corporate has a "mirrored" system at a hot-site location, the corporate must ensure it is adequately secured. The examination scope will include review of fund transfer system user access and machine security settings for any hot-site terminals. Procedures and controls should remain the same at the "hot-site" as are used at the main office.

Security Safekeeping

Security Safekeeping Policy

The corporate's investment policy should explicitly detail all authorized methods for safekeeping securities. The offering of the safekeeping program may be found in another board-approved policy. Specific procedures should be in place to ensure adequate separation of duties and controls. Access control limitations should be similar to systems employed in the wire transfer area. Safekeeping policies and procedures should be written with risk assessment in mind. "Prevention control" rather than "discovery" should be the underlying theme and objective.

Security Safekeeping Environment

Corporates are normally involved in a safekeeping environment and typically safekeep investments through a program offered by U.S. Central. However, they often have other arrangements with banks, other safekeeping facilities, and/or the Federal Reserve. While assessing the internal controls of the safekeeping program is important, evaluating the corporate's assessment of its safekeeping institutions is equally critical. The impact of an unauthorized security transfer can be similar to an unauthorized wire transfer by exposing the corporate to financial and reputation losses.

Internal Risk

Corporates typically minimize their risk by acting as a "pass-through" to an outside safekeeping institution. Contracts and procedures for member credit unions are often implemented to control the risk of potential legal liability or loss from a breach of security occurring outside of the corporate.

Review of Safekeeping Program

During the examination of a corporate that engages in a security safekeeping program, the examiner will review the program, policies, procedures, and internal controls. The examiner should document their analysis and conclusions of the program within the funds transfer memorandum.

In addition to network developed programs, the examiner may encounter "non-network" developed programs. Such programs may be developed in-house, by other corporates, or other outside financial entities. The examiner must have a complete understanding of the program and identify any potential risk to the corporate.

Separation of Duties

A written procedure needs to be on file, which describes the security transfer process and the individuals responsible. Segregation of duties in the movement of securities is a key internal control element. An adequate password system should be in place for members to initiate movement of securities. The same internal controls for the wire transfer area should be in place for security safekeeping.

The majority of security transfers are completed through U.S. Central. Requests for securities movement are initiated by electronic means. Access to the CCUN system and its input/transfer screen (DCHT) is password controlled. The examiner should determine that the CCUN verification function (DCHK) is not disabled. The examiner should verify that the DCHT function is not set using a "Z" which bypasses the second verification for "free delivery" securities.

Other safekeeping relationships must be reviewed carefully to assess the level of control in place. Built-in security features offered by custodians should be fully utilized by the corporate.

Account Reconciliation

At any time during the day, the corporate should have the ability to identify and document the location of a participating member's securities. Safekeeping procedures should require a reconciliation of the safekeeping account be performed daily and all securities in safekeeping be reconciled at least monthly to a master database. Other reconciliation processes can be used by a corporate. Examiner judgment must be used to ensure that an adequate reconciliation process is in place.

Examination Objectives

The objectives for reviewing funds transfer activities are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control the risk in its funds transfer activities;
2. Assess the corporate's payment processing and accounting controls to determine the integrity of funds transfer data and the adequacy of the separation of duties;
3. Assess the sufficiency of physical and logical security to protect the data security of the funds transfer department;
4. Assess the quality of oversight and support provided by the board of directors and management;
5. Determine corporate management and officials are adhering to established guidelines;
6. Determine if agreements concerning funds transfer activities with members, correspondent banks, and service providers are adequate and clearly define rights and responsibilities,
7. Assess the quality of risk management and support for FRB payment system risk policy compliance,
8. Determine the quality of risk management and support for internal audit and the effectiveness of the internal audit program for fund transfer systems,
9. Review the adequacy of backup, contingency, and business continuity plans for the funds transfer function; and
10. Initiate corrective action when the corporate's funds transfer policies, procedures, practices, and controls are deficient.

Examination Procedures

See Corporate Examination Procedures - Funds Transfer (OCCU 305P).

Examination Questionnaire

See Corporate Examination Questionnaire - Funds Transfer (OCCU 305Q).

References

1. NCUA Examiner's Guide;
2. FFIEC Information Systems Handbook, 2004 Edition;
3. Uniform Commercial Code, Article 4A; and
4. Open Door Training Reference.

Appendices

305A FEDWIRE DISCUSSION - Excerpts from the FFIEC Information Systems Examiner's Guide;
305B FRB Account Settlement and Posting;
305C Examiner's Guide to Open Door; and
305D Examiner's Guide to Fedplu$.

Appendix 305A

FEDWIRE DISCUSSION - Excerpts from the Federal Financial Institutions Examination Council's Information Systems Examiner's Guide

Fedwire is the Federal Reserve System's nation-wide electronic funds and securities transfer network. Fedwire links the 12 Federal Reserve Banks with the many depository institutions that maintain reserve or clearing accounts with the Federal Reserve. Fedwire processes approximately $2.3 trillion (2006) in funds and securities transfers each day. It provides for the electronic transfer of **immediate** and **irrevocable** payments between participating institutions, and functions as both a clearing and settlement facility. The Fedwire book-entry securities transfer system provides for the transfer of U.S. government and federal agency securities that settle on the books of the Federal Reserve.

Fedwire may be accessed by direct computer interface, via Internet or off-line by telephone through a PC-based electronic system called FedLine Advantage. FedLine Advantage is the next generation, secure platform that replaced the DOS-based FedLine. FedLine Advantage was developed by the Federal Reserve Banks and allows three methods of network access: frame relay, Internet, and direct telephone dial-up.

The Fedwire funds transfer system is a credit transfer system. Each funds transfer is settled individually on the books of the Federal Reserve as it is processed, and is considered a **final and irrevocable** payment. When a corporate sends a funds transfer request, it **irrevocably** authorizes its Reserve Bank to debit (charge) its account for the settlement account, and further authorizes the Reserve Bank of the receiving institution to give credit in the same amount to the payee. The Federal Reserve guarantees immediate availability of funds; once the Federal Reserve Bank credits the receiving institution's account or delivers the advice of payment, the Federal Reserve Bank will not reverse credit for the payment. Therefore, there is no settlement risk to the recipient of a Fedwire Transfer. The Federal Reserve Bank assumes the risk only if the sending institution overdraws its position at the Reserve Bank.

The Federal Reserve's payments system risk policies are designed to limit the risk a financial institution fails with its reserve account overdrawn. Reserve Banks require depository institutions to continuously monitor and adjust their reserve account positions ensuring adequate funds are on hand, or they are in compliance with established overdraft limits and collateral requirements.

Other risks associated with Fedwire funds transfers include potential loss due to errors, omissions, and fraud. Corporates are expected to have internal controls and segregation of duties sufficient to reasonably ensure the risk of loss from these risks is minimized.

NOTE: Although the following discussion regarding the DOS-based FedLine system is outdated, it is included to provide examiners a general understanding of how the previous system worked. Material related to the new FedLine Advantage system is confidential and will be covered and discussed during corporate examiner on-the-job training. Some security settings previously controlled by financial institutions are now controlled by the FRB. The information below can also be found in the FFIEC IT Handbook on FedLine (www.ffiec.gov).

FEDLINE TERMINAL SECURITY MEASURES

1. THE LOCAL SECURITY ADMINISTRATOR

The Local Security Administrator (LSA) is responsible for setting up new users on the local FedLine system. The LSA also is responsible for setting the function levels of all users. The LSA is a powerful user and has the tools to bypass all security and effectively send a transfer with no supervision if other compensating controls, such as limited access to the terminal, prompt balancing, and timely activity log review are not in effect.

The LSA should be someone who has NO day-to-day operational duties on the FedLine terminal. The LSA's main purpose is to add new users and change function security levels. Anytime the LSA uses the terminal, a member of the operations staff should be present to monitor his/her actions. If the FedLine terminal has a power on password, it should be implemented and the password restricted from the LSA. In addition, the LSA should not have a host access logon (HC) at the Federal Reserve host mainframe computer. Not having host communications authority prevents the LSA from logging onto the host mainframe and sending a transfer. (However, the LSA could queue a funds transfer (TQ status), and the next time a valid transfer exchange was made, the unauthorized transfer would be sent automatically.)

The LSA with unrestricted access could perform the following functions to bypass security and send a funds transfer without involvement by a second individual:

a) add two new user ID's with enter and verify capability, and then effect a transfer single - handily.

b) change the verification rule to "N," thus eliminating the verification requirement.

c) change the verification threshold dollar amount to $99,999,999.99, thus circumventing the verification requirements.

2. THE MISCELLANEOUS SECURITY SETTINGS

The FedLine Miscellaneous Security Settings will be reviewed at every examination. The settings are as follows:

a) User ID suspended - Consecutive bad password retries

This setting specifies the maximum number of consecutive invalid sign-on attempts operators can make before the local user ID is suspended. This prevents an unauthorized person from trying to guess the password of a legitimate user by limiting the number of invalid password retries. ***The Federal Reserve Board's recommended setting is 3.***

b) Users must periodically change their password every XX days

This setting specifies the maximum number of days operators can use their password before they must change it. ***The Federal Reserve Board's recommended setting is 30.***

c) Verification rule

This setting determines the message verification requirement, which requires more than one person be involved with the processing of all transfers completed on the system. Three options are available, N, U, and E (see the description of the option settings below**). The Federal Reserve Board's recommended setting is E, however U is acceptable.**

1) *N - No restriction (Very high risk)* This option allows the operator who entered and/or updated a message also to verify the same message. There is no dual control of any funds transfer if this option is chosen. For example, Joe enters message. He also can update and verify the same message.

2) *U - Verifying operator cannot be the last operator who updated the transfer*. This option prevents the last operator who entered or updated a transfer from verifying the same message. It would allow the original operator to verify the transfer if it was changed by a second operator. For example, Joe enters a transfer and Paul updates (changes) the same message. Paul cannot verify the same message, but Joe can.

3) *E - The verifying operator cannot be operator who entered or updated the transfer*. This option prevents any operator who entered or updated a transfer from verifying the same transfer. For example, Mary enters a transfer and Paul updates the same transfer. Neither Mary nor Paul can verify the same message. A third operator with verification authority must verify the transfer.

d) Override and release rule

This field is used to indicate the level of restrictions placed on overriding and/or releasing transfers. This potentially allows users to bypass verification. Only operators with *supervisor function* access level have the ability to perform the Override & Release function. Three options - N, U, or E - are also available for the override and release rule. ***The Federal Reserve Board's recommended setting is E.***

1) *N - No restriction on override or release*. Any operator with the supervisor function access level can override or release the verification of a transfer regardless of any previous processing performed.

2) *U - Limited restriction on override or release.* The operator overriding or releasing the transfer cannot be the operator who last updated the message. (This setting may be considered by smaller corporates with limited staff.)

3) *E - Full restriction.* The operator releasing the transfer cannot be the operator who updated or who originally entered the message.

e) Time-out Intervals

This parameter minimizes the amount of time a terminal remains active if a user forgets to sign-off. It causes the system to revert to the FedLine Sign-on screen after a specified amount of time passes in which no keystrokes have been entered. **The Federal Reserve Board's recommended setting is 10 minutes.**

f) Cycle-Date rollover and Print-delete option

Before the beginning of each day's work, a function must be performed on the FedLine terminal known as the "cycle date rollover." The purpose of this function is to reset the date on the terminal. The FedLine system requires the operator to clear or cancel any messages that are still pending (i.e. - have been initiated but not verified/ transmitted) before performing this function. If any messages are pending, requiring an operator to cancel them in order to complete the cycle date rollover, policies should require a record of these messages be reported to management. The software is originally set on "Full" as the default.

1) *FULL* - Prints a full recap report of the previous day's funds transfers before they are deleted by the cleanup cycle data mode change program.

2) *SUMMARY* - Prints an abbreviated report of the previous day's funds transfers before they are deleted by the cleanup cycle date mode change program.

It is recommended this option be set in the FULL account option so a complete detailed record is on file and can be reviewed.

g) Suppression of the Check for Possible Keyboard Eavesdropping

This option on the system allows the administrator to turn off or keep on the "Possible Keyboard Eavesdropping" message each time the system is entered. It is recommended this option be kept <u>on</u> to assure no other software on the system is affecting the FedLine II software.

3. THE USER/ACCESS REPORT

The user access report lists the various capabilities of each FedLine user. The report will be reviewed to determine no one person can effect a funds transfer, and access levels on all FedLine applications are limited to what users must have to do their job. Corporates have a tendency toward having multiple back-ups in case of absence, and having back-up staff with active access on FedLine. Excessive back-up personnel with continuous FedLine access should be discouraged.

The following additional controls should be observed in review of user/access levels.

a) The Local Administrator (LA) function should not have access to the funds transfer (FT) application or host communications (HC). In fact, there is no reason for the LA to have any other available applications beyond LA. Note: There is no way to determine conclusively at the corporate if any user has host access. This can only be determined by calling the data security department of the respective Federal Reserve Bank. The presence of the host communications (HC) under their user ID is usually a good indicator, but not conclusive since the LSA could use the "Master ID" to activate the HC application at any time.

b) No user should have more than one user ID. Doing so would enable the individual to enter a funds transfer using the first ID, then log back on and verify and send the message using the second ID.

c) No more than two staff members should be assigned as Local Administrators. The Federal Reserve Guidelines suggest an Administrator and one backup administrator.

d) No funds transfer staff should have the Funds Transfer "Supervisor" or "Manager" function. These functions have access levels that can be used to bypass the verification requirement. These access levels should only be activated by the LA in unusual circumstances. The LA should monitor the actions performed using these access levels and then de-activate the access levels when the action is completed. Note: It is possible the supervisor function may be needed in some FedLine applications such as Start-up/Shutdown. However, it is not normally needed for funds transfer.

4. THE VERIFICATION FIELDS

The "update funds application attributes" option allows staff members with "Manager" function level or the LA to set the verification fields and applicable verification thresholds for funds transfers. Verification means fields must be re-keyed by a second operator. If none of the fields has an "X" next to them, none have to be re-keyed. However, a second operator still has to call up the transfer on the screen and review it prior to releasing it.

Available options range from no verification of any field to required verification of every field. Between these two extremes, management and/or the LA can select individual fields that would be required to be verified. At a minimum, verification of the dollar amount should be required.

Verification thresholds allow the corporate to set a dollar amount over which all funds transfers must be verified. Normally, the threshold should be set at $0.00, which requires verification of all funds transfers. If the verification level is set at a higher amount, this amount should be approved by the board of directors and noted in the minutes. There should also be compelling reasons why management does not want to have a required review of all funds transfers by a second operator prior to transmission.

5. GENERAL CONTROLS

a) The "master" User-ID

It could occur that a local administration function needs to be performed but no LA is available. In case of such a situation, the "master" user-ID password should be stored in a secure location should the corporate need to access it. In no case should any operating personnel be able to access the "master" password individually. It should be maintained under dual custody, preferably in a lock box with dual keys/combinations.

b) Configuration Diskette

This diskette is used by the corporate, in conjunction with the Federal Reserve, if for some reason everyone is locked out of the system. The configuration diskette should also be stored in a secure location under dual custody.

c) Power On Password

Most micro-computers have a power on password feature, which requires a password be input before the computer will activate. If the FedLine terminal has this feature available, it should be activated. If a power on password is activated, it should not be disclosed to the local administrator. This would preclude the local administrator performing unauthorized system changes and/or transfers.

FRB Account Settlement and Posting

Corporate management must be aware of the order and timing of the various types of transactions which post to its Federal Reserve account throughout the business day, in order to properly manage the account and ensure overdrafts in the account are avoided. The following is a summary of the posting order.

Opening Balance (Previous Day's Closing Balance)

Items Posted at Opening of Fedwire:

+/-	Government and commercial ACH credit transactions
+	Advance Notice Treasury investments
+	Treasury, state, and local government securities interest and redemption payments
+	Treasury checks, postal money orders, local FRB Checks, and savings bond redemptions

Items Posted Throughout the Business Day

+/-	Fedwire Funds Transfers
+/-	Fedwire book entry securities transfers
+/-	Net settlement entries

Items which post by 9:15 a.m. Eastern Time

-	Original issues of Treasury Securities

Items which post at 11:00 a.m. Eastern Time

+/-	ACH debit transactions

Items which post at 11:00 a.m. Eastern Time

+/-	Commercial Check Transactions, including returns
+/-	Check correction amounting to $1 Million or more
+/-	Currency and Coin Deposits
+/-	Credit Adjustments amounting to $1 Million or more

Items which post by 1:00 p.m. Eastern Time

+/ Same day Treasury Investments

Items which post at 2:00 p.m.

+/ Manual Letters of credit (government grant drawdowns)

Items which post at 5:00 p.m. Eastern Time

+ Treasury checks, postal money orders, local FRB checks, savings bonds redemptions
+ Manual letters of credit
+/- ACH return items and check-transaction items

Items which post after Closing of Fedwire

+/- Other non-funds transfer transactions (non-cash government coupons, T&L calls, discount window loans, currency and coin)

Equals Closing Balance

Chapter 305 Appendix C

Examiner's Guide to Open Door

Introduction

Open Door is a web-based application that interfaces with the Corporate Credit Union Network (CCUN) and is used by corporate and member credit unions to enter and retrieve account information, initiate wire transfer requests, check share, loan, and investment rates, and transfer funds between accounts.

Modules

Open Door has several modules. For example, the web pages that support wire transfers make up a module. Other modules include Accounts, Transfers, Directory of Services, and Coin and Currency. Various functions may be performed within each module. An example is the Accounts module with three related functions: view account balance information, future dated transaction inquiry, and view selected history.

Corporate Credit Union Users and Member Credit Union Users

Two levels of Open Door users are recognized, corporate credit union users and member credit union users. Corporate users see all modules and menu options in Open Door including all security administrative functions. Member credit unions see a subset of menu options and have limited access to security administration functions with member credit union users restricted to changing their PIN and passwords. All other system administration is handled at the corporate user level.

Users and User IDs and Contacts

All users requiring access to Open Door are assigned a user ID. This user ID includes a user ID profile containing the authorization codes, dollar limits, and PIN information assigned to that user. Open Door also defines individual contacts, each representing a specific member credit union. A user ID is associated with one or more contacts, relating each user ID to a specific credit union or credit unions.

Each user holds a password, allowing access to the functions to which that user has been assigned permissions. A first time user must change the temporary password issued by the system administrator immediately upon logging on to the Open Door application. Future password changes are the responsibility of the user. A PIN number is assigned to the user if access to the wire transfer module is permitted.

Dual Controls

Open Door imposes dual control on both (1) security administrative activity and (2) initiation and release of wire transfer requests. An example of security administrative change using dual controls is when a corporate user with security administration access enters or updates someone's authorization codes. A different corporate user with security administration access must approve the entry or change. Dual controls on wire transfer initiation and release are also imposed by Open Door as well. One authorized individual must initiate the wire transfer request and a second authorized party must approve or release the request.

Verification Bypass Authorization

Corporate users may be assigned a bypass verification authorization code for use in member credit union wire transfer request processing. This allows corporate users to bypass verification of member wires when no employee at the credit union is available to verify the wire request. Dual control is still maintained; however, a credit union and a corporate employee are now acting on the wire for two party approval rather than two member credit union employees.

PIN Security

PIN security is an option for some functions such as credit union pre-authorized wire requests. PIN security options are available both at the credit union level and the corporate credit union level. PIN security may be switched off; however, an alternative validation method must be indicated if PIN security is removed from member to member transfers, or wire transfers.

Summary

In wide use by corporates and member credit unions, Open Door provides the means to establish generally acceptable security options and controls on critical activities and transactions. The combinations, permutations, and unique application possibilities presented by the program preclude explicit instructions touching on all potential pitfalls. However, the following guidance is provided as a risk-based approach to examination of Open Door.

Examination Goals

The examination goal is to verify sound segregation of duties and to ensure appropriate controls are imposed on funds transfer activity.

There are three essential areas to review:

1. Sound Segregation of Duties. Segregation of duties is controlled by the Open Door system administrators at each corporate. Examination procedures should include review of the corporate's controls on adding new users, both corporate and credit union, changing user authorities, and deleting inactive or expired users;
2. Transaction Controls. The corporate system administrators impose these controls by assigning various functions to each user ID along with assigning any dollar limits associated with that user ID. Examination procedures should include a general review of the functions assigned to corporate employees within each module in Open Door, looking for inappropriate access assignments. Additionally, a specific review of the functions assigned to corporate employees with access to the wire transfer module should be completed to verify restricted access to wire transfer applications, ensure appropriate dollar limits are assigned to wire room employees, and verify that sound segregation of duties is maintained within the wire transfer application; and
3. Open Door Wire Processing Rules. The corporate system administrator selects certain wire processing rules that effect the combinations of individuals allowed to create and send a wire transfer as well as wire transfer dollar amounts requiring second party verification. A corporate may hold to a standard application of control setting or, may vary the control settings based on the needs or desires of the member credit union.

Examination procedures need to determine:

a) PIN security is "on" for sensitive transactions;
b) Wire option amount settings are appropriate; and
c) The "Verify Bypass" function is allowed only when other risk mitigation measures are present.

Examination Guidance

Request Items:

Related Policy
Related Procedures
Related Contracts & Agreements
Employee Listing with Job Titles
Open Door Report – Member Listing
Open Door Report – Update Member Profile
Open Door Report – OD900 Operator Authority Report
Open Door Report – Authorization Code Maintenance
Open Door Report – Update Corporate Authorization Codes
Open Door Report – OD040 Non-Financial Transactions
Open Door Report – OD002 Security Violations

Security Administration

The function of the security administrator within Open Door is similar to the Local Security Administrator (LA) in Fedline. Therefore, Open Door examination procedures are similar to reviewing the Fedline LA function. The same questions should be asked. Who are the administrators? Are there more than two employees assigned this function? Is a formal process in place to add, change, or delete user authorities? How is a new credit union user added? How is a new corporate user added? What happens if a credit union user loses a password? How often are passwords changed? How often are PIN numbers changed?

Transaction Controls

Wire transfers are the most critical funds transfer feature of Open Door. Other account transactions are possible; however, only a wire transfer moves funds out of the CCUN. Open door imposes strict dual controls on all wire transfers. Action on the part of two users must occur to (1) initiate and (2) release a wire transfer. However, the combination of employees providing that dual control is variable. Two credit union employees may initiate and verify a wire, a credit union employee and a corporate employee may complete these actions, or two corporate employees may provide the necessary parties. Clearly not all combinations of personnel would be appropriate in all situations, even though dual controls are present. A number of other questions should be investigated as well. Are all of the authorized wire requesters assigned appropriate dollar limits? Do surrogates have access to credit union IDs and authorities that don't have dollar limits? What occasion would result in a physical callback? What dollar amount requires a physical callback? Are controls in general sufficient to minimize both the corporate's and the credit unions' risk?

Wire Processing Rules

Within each Member Profile Module there are dollar amount settings specifying the minimum dollar amount of a wire transaction requiring second party verification. In addition, dollar limits are allowed for new wires, pre-authorized wires, intra-network wires, and international wires. A setting of “0” requires all wire entries to be verified and a setting of 99,999,999 meaning no second-party verification is required unless the transaction is greater than 99,999,999.

The examiner needs to verify dollar limits and verification settings are established to provide adequate control of transactional risk. If the corporate or credit union has selected amounts greater than the default value of “0”, is the new amount supportable? Does the corporate request the credit union to establish dollar limits for each of its employees? Are corporate users’ dollar limits appropriate? Are credit union user limits frequently set at 99,999,999 rather than more realistic defaults? Is verification inappropriately bypassed for new wires or new templates? This review is most easily accomplished by reviewing (1) Open Door member profile screens (perhaps on a sample basis), (2) the corporate’s own settings for internal transactions, and (3) settings for large dollar participants.

There are also settings for pre-authorized wire template creation allowing establishment of a dollar limit on template creation and a choice for second-party verification to establish a new template. Default settings are “0” and “verification required”. Again, has the corporate deviated from the default settings and if so, are its actions supportable?

PIN security is another feature of Open Door allowing a selection of “on” or “off” for certain transactions. This is another member profile option setting and must also be reviewed on screen, from screen prints. Is PIN security turned off for any participant, and if so, why?

Unfortunately, as of this date, the member profile module does not support a printed report of wire option settings. They must be viewed on screen for each participating credit union and corporate or a query may be run and printed by the corporate. Sampling may suffice if corporate policy and procedures are strong.

OFAC Compliance

OFAC compliance is not a part of the Open Door system. Corporates are responsible for OFAC compliance for all wires processed through the system. Corporates cannot pass the responsibility to the member credit union, U.S. Central, or corresponding bank. Examiners must ensure that the corporate has developed a procedure to monitor all funds transactions by this system either by software or physical review of each transaction.

Contingency Plans

The corporate should have a written contingency plan that addresses the movement of funds should Open Door not be available. The plan should include how the request will be taken from the member credit union and alternative PIN numbers for emergency use. This can be accomplished by telephoning in wire requests and establishing emergency PIN numbers assigned and maintained by both parties.

Further Information

U.S. Central Credit Union has developed an Open Door Training Manual for program participants. This manual is available for reference at participating corporate credit unions and member credit unions and offers an in depth discussion of Open Door’s features and controls.

Chapter 305 Appendix D

EXAMINER'S GUIDE TO FEDPLU$

Introduction

Fedplu$ is a licensed software program used to facilitate the receipt and processing of wire transfer requests including communicating those requests to the Federal Reserve. The system has features to integrate the wire requests with general ledger systems, FAX systems, Internet connections, and other programs. The software is compatible with most current information technology (IT) networks and communication systems.

The system operates as a database. As the wire request is entered into the database, the entry is tested against various information and criteria stored within Fedplu$. Testing is facilitated by Fedplu$ displays and drop down menus.

Wire requests are segregated during the various stages of processing. These segregations are referred to as processing queues. Typically, a single entry would pass through an entry, verification, and a release queue; although, the system allows for extensive customization. Pre-established user authorities and system parameter settings control access to each queue and define the authorized actions a user may take at each stage of processing.

The program supports Fedline terminal communications for final transmission as well as direct connections with the Federal Reserve using high-speed bulk data communication lines.

Examination Goals

At a minimum, the examination should establish (1) there are sound controls on personnel having access to the software, (2) the authorized users hold appropriate authorities, and (3) the combination of user authorities and Fedplu$ system settings result in a sound segregation of duties.

Three Fedplu$ reports are necessary to complete this review. Including these reports as a requested item during pre exam planning is strongly recommended. Note that these reports must be reviewed together to properly understand the assigned authorities for each employee with access to the program.

Area of Review	Fedplu$ Report Title
(1) System Access	(1) Access Profile Report
(2) User Authorities	(2) User Security Report
(3) System Parameter Settings	(3) System Parameter Report

Access Profile Report

The Access Profile Report is a listing of the corporate's generic user profiles. Each user profile is restricted to certain rights and permissions within four categories of access.

Access Category	Rights and Permissions
Message Level:	Types of messages a profile ID can access.
Queue Level:	Processing queues a profile ID may access.
Access Level:	Functions that may be accessed within a queue.
Bank Level:	Accounts that may be accessed.

The licensed software owner creates a single generic profile for each job category in the organization needing access to the program. Once a generic profile is completed, it may be applied to all employees holding the same job.

There are no standardized names for each generic user profile nor does the system require a minimum or maximum number of profiles. Typically, the user would define a low level Operator profile, a higher level Operator profile, a Supervisor profile, and a System Administrator profile; however, the complexity of the operation and available staffing may result in fewer or a greater number of profiles.

The functions assigned to each profile should be reviewed to determine they are appropriate for the position. The examiner on a case-by-case basis must determine inappropriate profile configurations. Examples of inappropriate profile definitions would include a System Administrator profile with processing queue access, a low level operator profile with override authority or access to verification or release queues, or a profile intended for inquiry use that includes access to processing queues or operational functions.

Note that the access profiles do not, in themselves, establish dual controls. Although a profile's access level may allow the creation of a wire transfer request, but not the release of the request, dual controls are only fully established by activating certain Fedplu$ parameter settings. This will be discussed further under the System Parameter Report section of this Fedplu$ chapter.

User Security Report

The User Security Report identifies the specific pre-defined generic profiles assigned to each employee. A separate profile is assigned to each user for each of the Fedplu$ software's four categories of access. The profile's pre-defined authorities then apply for the individual employee. An individual may hold a different pre-defined profile for each of the four categories of access.

When the User Security Report is used in conjunction with the Access Profile Report, a complete picture of the employee's rights and permissions on the system can be determined. The Access Profile Report indicates the rights and permissions for each profile. The User Security report indicates which profile the employee holds.

Also listed on the User Security Report is a maximum dollar limit parameter setting for each employee. A determination of appropriate limits should be made taking into account the employee's responsibilities. This and other parameter limits are established as parameter settings and are discussed in the System Parameter Report section below.

System Parameter Report

The third report necessary to complete a review of Fedplu$ controls is the System Parameter Report. This report includes numerous settings, an indication of the extensive customization available within Fedplu$. This chapter will not attempt to define each of the over two hundred parameter settings that may be established. Examiners are referred to the Fedplu$ Users Guide issued to each licensed user for reference. However, the examiner must review, at a minimum, the parameter settings crucial to the establishment of dual controls on processing and system administration. Review of terminal access and certain thresholds settings should be undertaken as well.

A list of a number of critical switches and the recommended settings for each is provided in the table below. Each licensed user will need to make their own determination as to all settings in terms of their own operational and security needs. However, each of the recommended settings listed within the table establishes an important internal control. Settings other than the recommendations should be investigated and justified.

Critical System Parameter Switch	Recommended Setting
Archive admin messages	Yes
Archive securities messages	Yes
Update Local Balance	Yes
LTERM Password Expiration	30
Ignore OFAC in REMOTE	No

Threshold Requiring VERIFY	10,000 (or less)
Identical creator and verifier	No
Identical creator and releaser	No
Must enter PIN before CREATE	Yes
Dual verification for template	Yes
Number of allowed failed logon	3

Other Features

An operator is generally able to access PIN numbers for authentication and lists of authorized personnel for call back verifications using drop down menus available on screen. Verification of routing instructions for valid ABA numbers, Office of Foreign Asset Control (OFAC) compliance tests, and checks on available funds are generally automated.

Passing the request to each successive processing queue is also automated, dependent upon successful completion of certain defined actions while the request is in the previous queue. Examples would be requirements for a valid PIN number to pass from the entry to the verify queue, completion of a call back to pass from the verification to the release queue, and approval of a supervisor to pass from the release or exception queues to final communication to the Federal Reserve.

The software may be integrated with FAX communications. The Fedplu$ FAX module provides a FAX signature authentication process. Note the use of the FAX module holds a high degree of liability on the part of a financial institution. Accepting wire transfer instructions via FAX may not provide "commercially reasonable" security as defined under UCC 4A. Acceptance of wire requests sent by FAX should be strongly opposed.

The LU Name function, available to users with "System & Maintenance" authority, will identify communication pathways between Fedplu$ and outside systems.

There is a cash management host interface available that enables Fedplu$ to accept and process wire payments created by an external cash management system. Payments should be queued into Fedplu$ for review and release to the Fed. Bypassing this review and release queue is possible through parameter settings; however, this is not recommended.

OFAC compliance software can be used with the Fedplu$ system. The system filters the beneficiary and financial institution against OFAC known prohibited parties. Examiners should verify that the software has been installed, is being used, and is up-to-date.

Further Information

The examiner should request to review the Fedplu$ users manual at the participating corporate credit union for an in depth discussion of the features and controls.

Chapter 306

AUTOMATED CLEARING HOUSE

Introduction

The Automated Clearing House (ACH) is a network for electronically exchanging funds and related information among individuals, businesses, financial institutions, and government entities. ACH rules and regulations are established by the National Automated Clearing House Association (NACHA). Private ACH operators and other local and regional ACH associations provide input into the rules. Federal government ACH transactions fall under the government's "Green Book" ACH Rules.

The ACH Network

The Federal Reserve is the principal ACH operator, distributing ACH transactions through FedLine. There is one private sector operator, the Electronics Payment Network or EPN. The ACH network is made up of thousands of participants. Most financial institutions and large processor participants are members of one of approximately 23 regional ACH associations. All participants in the network can be classified into one or more of the following six categories:

1. Originator - The Originator is the entity that agrees to initiate ACH entries into the payment system according to an arrangement with a Receiver. The Originator is usually a company directing a transfer of funds to or from a consumer's or another company's account. In the case of a consumer-initiated entry, the Originator may be an individual initiating funds transfer activity to or from his or her own account.
2. Originating Depository Financial Institution (ODFI) – The ODFI is the institution that receives payment instruction from the Originators and forwards the entry to the ACH operator. A depository financial institution (DFI) may participate in the ACH Network as a RDFI (see below) without acting as an ODFI; however, if a DFI chooses to originate ACH entries, it must also agree to act as an RDFI.
3. ACH Operator - A central processing facility operated by a private organization or a Federal Reserve Bank (FRB) on behalf of DFIs. The operator receives electronic entries from ODFIs and distributes entries to the appropriate RDFIs (see below), and performs the settlement functions for the affected financial institutions.

4. Receiving Depository Financial Institution (RDFI) - A financial institution, which receives ACH entries from the ACH Operator and posts the entries to the accounts of its receivers (depositors).
5. Receiver - A natural person or organization, which has authorized an Originator to initiate an ACH entry to the Receiver's account with the RDFI. The receiver may be either a consumer or a company.
6. Third Party Service Provider (TPSP) - A third party service provider is an entity other than the Originator, ODFI, or RDFI that performs any functions on behalf of the Originator, ODFI, or RDFI with respect to the processing of ACH entries. A function of ACH processing can include, but is not limited to, the creation of ACH files on behalf of an originator or ODFI, or acting as a sending point or receiving point on behalf of an ODFI or RDFI, respectively. The ODFI and RDFI are still responsible for compliance with ACH rules and regulations.

ACH System Operations

The ACH system supports both credit and debit transactions. In credit transactions, funds flow from the Originator's account through the ODFI to an account held by the receiver at the RDFI. For ACH debit transactions, the funds flow from the receiver's account at the RDFI through the ODFI to the account of the Originator.

Examples of ACH Credits	Examples of ACH Debits
• Payroll direct deposits	• Insurance premium collections
• Social Security payments	• Mortgage and loan payments
• Dividend and interest payments	• Consumer bill paying
• Corporate bill payments to contractors and vendors	• Corporate cash concentration transactions
• Tax payments	• Point of Sale purchases

ACH data transmissions always flow in the same direction - from Originator to the ODFI to the ACH operator to the RDFI to the receiver. This is true whether the item is a debit or a credit. For credits, the ODFI's settlement account is debited and the RDFI's settlement account is credited. For debits, the ODFI's settlement account is credited and the RDFI's settlement account is debited.

The following are the steps for ACH origination:

1. The Originator (individual or business account holder) initiates a payment order to the ODFI;
2. The ODFI transmits the payment information to the ACH operator;

3. The ACH operator receives data from the ODFI and sorts the entries by routing number;
4. The entry is transmitted to the RDFI; and
5. The RDFI receives, processes, and posts the ACH data to the receiver account on settlement day.

ACH return items flow from the RDFI to the ACH Operator to the ODFI. The ODFI must notify the Originator of return items. Third party service providers may become involved at any step in the process. They may prepare files and send them to the ACH Operator on behalf of ODFI, or they receive them on behalf of the RDFI. Regardless of the role third party service providers play, the responsibility for rules adherence and liability falls on the appropriate financial institution using the third party service provider.

ACH Uses

The ACH Network supports a variety of payment applications. A unique Standard Entry Class (SEC) code identifies each application and the related ACH record format used to carry the payment and payment-related information. Each entry is also assigned a code to indicate the type of payment, such as debit or credit. An Originator initiates entries into the system, authorizing either a debit or credit, which affects either a consumer or a business account at the RDFI. Listed below are SEC codes and the different products each code supports. This list is not all-inclusive since new codes are always being developed and used.

<u>Consumer Applications</u>

1. Pre-arranged Payment and Deposit Entries (PPD) include both Direct Deposits and Direct Payments, as follows:

   a) Direct Deposit is a credit application that transfers funds into a consumer's account at the RDFI. These funds can represent a variety of deposits (e.g., payroll, interest, and pension); and
   b) Pre-authorized Bill Payment is a debit application. Companies with billing operations may participate in the ACH Network through the electronic transfer (direct debit) of bill payment entries. Through pre-established or single entry written authorizations, the consumer grants the company authority to initiate periodic charges to their account as bills come due. Examples of recurring bills paid by ACH include insurance premiums, mortgage payments, and installment loan payments.

An example of a non-recurring bill (i.e., the amount varies) paid by ACH is utility payments.

2. Point of Sales Entries and Shared Network Transactions (POS and SHR) are two SEC codes, which are most often initiated by the consumer via a plastic access card. They represent point of sale debit applications in either a shared or non-shared environment.
3. Point-of-Purchase (POP) entries are used by originators as a method of payment for the in-person purchase of goods or services by consumers. These are single authorization entries initiated by the originator based on a written authorization and account information drawn from a source document (e.g., check) obtained from the consumer at the time of purchase. The source document (check) is voided by the merchant and returned to the consumer at the time of purchase.
4. Machine Transfer Entries (MTE) are supported by the network for the clearing of transactions from Automated Teller Machines (ATMs).
5. Customer Initiated Entries (CIE) are limited to credit applications where the consumer initiates the transfer of funds to a company for payment of funds owed, typically through some type of home banking product.
6. Represented Check Entries (RCK) are used by originators to represent a check that has been processed through the check collection system and returned because of insufficient or uncollected funds.
7. Accounts Receivable Entry (ARC) enables originators to convert a consumer check received, via the U.S. mail or at a dropbox location, for payment of goods or services, to an ACH debit entry. The consumer's check, the source document, is used to collect the consumer's routing number, account number, check serial number and dollar amount for the transaction.
8. Telephone-Initiated (TEL) entries are used for debiting consumers' accounts pursuant to an oral authorization obtained from the consumers via the telephone. This transaction code requires either a relationship must exist between the originator and the receiver, or if no relationship exists, the receiver must initiate the telephone contact. Other special requirements for using this transaction code are outlined in the ACH Rules.
9. Internet-Initiated (WEB) entry SEC code is used for the origination of debit entries (either recurring or single entry) to a consumer's account pursuant to an authorization that is obtained from the receiver via the Internet. An example of a WEB entry is a consumer purchasing goods via the Internet. WEB transactions pose a unique risk to the consumer and should be monitored.

Corporate Applications

1. Cash Concentration or Disbursement (CCD) can be either a credit or a debit transaction where funds are either disbursed or collected between corporate entities. This application can serve as a stand-alone funds transfer or it can support a limited amount of payment-related data with the funds transfer.
2. Corporate Trade Exchanges (CTX) support the transfer of funds (debit or credit) within a trading partner relationship in which a full (ANSI ASC X12) message or payment-related (UN/EDIFACT) information is sent with the funds transfer. Upon receiver request, the ODFI must provide all payment related information in the addenda records transmitted with CCD and CTX entries. The information must be provided by the opening of business on the second banking day following the settlement date of the entry.

Other Applications

1. Automated Accounting Advice (ADV) is an optional service provided by ACH operators that identifies automated accounting advices of ACH accounting information in a machine-readable format. This facilitates the automation of accounting information for participating depository financial institutions (DFIs).
2. Automated Notification of Change (NOC) or Refused Notification of Change (COR) is used by an RDFI or ODFI when originating a notification of change or refused notification of change in an automated format.
3. Death Notification Entries (DNE) are used by agencies of the federal government to notify a DFI the recipient of a government benefit payment has died.
4. Return Entries (RET) are used by ODFIs that convert paper returns to an automated format. They may also be used by ODFIs that are originating dishonored returns, when the return being dishonored carries the SEC code RET. Upon request of the receiver, the ODFI must provide all payment related information contained in the addenda records transmitted as CIE entries. Information must be provided by the opening of business on the second banking day following the settlement date of the entry.
5. Truncated Entries (TRC/TRX) are used to identify batches of truncated checks. TRC is used for individual items and TRX is used for batches.
6. Destroyed Check Entries (XCK) can be used by an institution for collecting certain checks that have been destroyed.

7. Cross-border payments to Canada are permitted using SEC codes CBR (corporate) and PBR (consumer). These transaction codes will change in the near future to support financial institutions' compliance with OFAC regulations.
8. ACH debits and credits may be made directly to a financial institution's general ledger accounts for institutions whose ACH systems are interfaced with its loan accounts, including ACH credits posted directly to loan accounts.

Applicable Regulations

ACH Rules

NACHA ACH Rules are published annually and incorporate new rules and rules changes approved by the NACHA board. NACHA is a self-regulated body, which depends on users' compliance with ACH rules for the system to operate efficiently. The rules provide warranties and indemnification requiring entries to be originated, received, and returned promptly.

ODFIs are responsible for most of the warranties and indemnifications; however, many responsibilities pass through the ODFI to the Originator. The warranties and indemnifications reside mostly with the ODFIs and Originators because they have primary control over the initiation of entries. The passing through of responsibility to the Originator relies heavily if not exclusively on the agreements between the ODFI and the Originator.

Responsibilities of ODFIs include:

1. Ensuring entries are properly authorized;
2. Submitting timely entry of transactions into the ACH system;
3. Terminating the origination of entries, when appropriate;
4. Meeting requirements for data security and personal identification numbers in certain applications;
5. Ensuring entries contain the appropriate information;
6. Assuring an agreement is in place with Originators and sending points; and
7. Complying with ACH rules.

The ODFI indemnifies the RDFI, ACH operator, and ACH association against loss when breaching any of these warranties. NACHA may require ODFIs that fail to adhere to the ACH rules to reimburse an RDFI or ACH operator for claims, losses, or expenses (including attorneys' fees and costs) resulting directly or indirectly from breach of warranty. Thus, a failure to comply with the warranties may result in a loss to an ODFI. ODFIs assume responsibility for most warranties related to ACH transactions. The RDFI warrants to each ODFI, ACH operator and ACH association the law permits it to receive entries allowed by the ACH rules. RDFI also warrants its compliance with the rules concerning RDFIs and participating DFIs.

Responsibilities of RDFIs:

1. Receiving and validating all ACH entries;
2. Posting to receiver's accounts;
3. Validating pre-notifications;
4. Returning entries which do not post within proper time frames;
5. Handling remittance data as required by the receiver;
6. Making funds available to the receiver within proper time frames; and
7. Fulfilling responsibilities when a receiving point is used.

Electronic Funds Transfer Act (EFTA)

The EFTA provides for rights and duties of consumers and financial institutions regarding electronic funds transfers. EFTA covers both private sector and government-initiated transfers.

Regulation E

Regulation E was issued by the Federal Reserve Board of Governors implementing EFTA to ensure consumers have a minimum level of protection in disputes arising from electronic funds transfers.

Uniform Commercial Code Form 4A (UCC-4A)

UCC-4A was developed in part for funds transfers, but also applies to wholesale (institution-to-institution) ACH credit transactions and certain ACH credit transactions not subject to the EFTA.

Green Book

The Green Book is published by the Financial Management Services agency of the Treasury Department. It specifies procedures for ACH transactions, which are originated for the Federal Government.

ACH Risk Assessment

The risks associated with processing ACH payments vary based on whether the item is an ACH debit or credit, and whether the item is received or originated. ACH risks are similar to those within the funds transfer and check payment systems. Although ACH transactions are generally for small dollar amounts, participating financial institutions may be exposed to credit risk for the entire ACH transmission file, not just individual entries in the file.

Corporates must understand payment processing risks (i.e., credit/exposure, operational, fraud, systemic, and third party processing) and have detailed written policies and procedures in place to control them.

<u>Credit (Exposure) Risk - ACH Credits</u>

The risk a party to a transaction will not have sufficient funds for settlement is called credit (exposure) risk. Credit risk is also defined as "temporal" (time) risk. There is credit risk to both the ODFIs and RDFIs.

For ODFIs, this risk is associated with sending credit files to the ACH before funds are obtained from the Originator. This may occur when a member that is a party to the transaction fails or goes bankrupt before settlement. NACHA rules require credit limits be set, monitored, and reviewed by the ODFI for each Originator of credit entries. Due to the system's settlement delay, credit limits must also be monitored across multiple settlement days.

If a corporate acts as an ODFI, it must assign credit ratings and exposure limits to each of its Originators. Exposure limits must be monitored. An alternative would be requiring the members' accounts be pre-funded and/or collateralized. However, ACH rules do not require pre-funding or collateralization, and corporates requiring this could put themselves at a competitive disadvantage.

Corporates acting as third party service providers must similarly assign exposure limits to the credit unions it authorizes to use its ACH services. Assigning settlement limits allows the corporate to assess, monitor, and control its settlement risk associated with offering ACH services while not taking on the full risk of acting as an ODFI.

For RDFIs, credit risk is minimal. The ODFI warrants its ACH credit transmissions and is liable for them. The RDFI is not at risk unless the

ODFI fails, which would cause the Fed to reverse the transaction. Even a failed ACH Originator still leaves the ODFI liable for any ACH transmissions sent.

For ACH debits the RDFI has no credit risk. The ODFI has some credit risk if funds are made available to the Originator. Returns, stop payments, and NSF accounts may come back, in some cases, up to 60 days after the original settlement date. The ODFI might be required to return the funds to the receiver of the ACH debit. This risk is generally managed by requiring the Originator to maintain a reserve for returns at the ODFI, based on industry standards for returns of like debits, or based on experience with customers. Immediate funds availability is given only for amounts in excess of the reserve. The amount of the reserve varies depending on the application. For instance, the collection of mortgage payments would likely have a much lower return rate than magazine subscription payments.

Operational Risk

Operational risk, which varies with the type of processing, is the danger an unintentional error will alter or delay a transaction. Corporates must limit operational risk by implementing appropriate management controls. The following are examples of operational risks and the controls corporates should have in place.

Hardware failure - The risk of hardware failure is reduced by purchasing reliable equipment, observing regular maintenance, hiring and/or contracting for responsive service personnel, and ensuring adequate backup equipment exists.

Software failure - Operational problems caused by software failure are reduced by carefully testing the vendor’s or service provider’s software before relying on it for live processing. Corporates that develop their own software can reduce the risk of disruption due to software problems with sound software development practices (e.g., adequate documentation, sound testing procedures, tight change control procedures, effective recovery facilities, and periodic internal and external audits).

Security breaches and data loss - This risk can be managed by the use of security policies which require passwords, IDs, dual controls, and random changes in personnel and duties. Specific examples are discussed as follows:

1. Protect electronic files against unauthorized changes by using file security procedures and maintaining all hard copy records in locked storage;
2. Limit data access to authorized personnel;
3. Duplicate, back up, and store data off-site to protect against data loss or destruction;
4. Establish and maintain audit trails of all transactions and changes;
5. Account for all files to ensure staff only processes current files and does not inadvertently duplicate or omit files; and
6. Balance file totals during processing to ensure transactions are not dropped, changed, or duplicated.

Telecommunications failures can be avoided by implementing the following:

1. Maintaining equipment (lines, modems, authentication or encryption devices, etc.) in working order;
2. Physically protecting the equipment;
3. Developing diagnostic tools and backup transmission modes in the event of a problem; and
4. Employing redundant communications services, if available.

Power failure can be avoided by obtaining an uninterruptible power supply system (UPS). A UPS removes spikes and transients from public power, and provides auxiliary power during a blackout. Management should arrange for a generator to handle longer-term power failures, if cost effective.

Human error can be managed by following documented procedures for operating systems, security controls, and by providing adequate training for personnel. Management can further reduce the risk of human error through:

1. Proper oversight and supervision;
2. Ensuring detailed operating procedures are in place;
3. Providing for periodic internal and external audits;
4. Monitoring file and dollar controls; and
5. Ensuring an adequate audit trail exists.

Staffing problems may be manifested by absences, turnover, or work stoppages. Staffing problems are reduced by emphasizing cross training and good supervision. Staffing problems in small corporates often result from only one or two people knowing the process. While in very large corporates each activity may be so specialized very few people know the overall process.

Natural disasters are largely out of the control of management. The corporate must develop and test disaster recovery plans utilizing alternative sites and operations.

Fraud risk is increased if an employee or interloper has the opportunity to gain unauthorized access to the system and initiate or alter a payment transaction in an attempt to misdirect or misappropriate funds. Fraud risk is reduced by the following:

1. Written personnel policies and practices requiring, at a minimum,:

    a. Vacancies in the unit be filled by internal transfers versus new employees, when possible;
    b. Relatives be restricted from working in the accounting or data processing departments;
    c. Individual responsibilities relating to security are in writing;
    d. Written organizational security procedures exist;
    e. Actions to be taken in the event of a security related incident be identified;
    f. Formal training programs be developed to emphasize security and control;
    g. Cross training exists within the unit;
    h. Rotation of responsibilities be unannounced;
    i. There be a minimum number of consecutive days of annual vacation;
    j. Reassignment out of the unit be made when a notice of resignation is given; and
    k. Terminated employees' sign-on ability is promptly cancelled.

2. Management implementing adequate physical security controls, including the following:

    a. Limit access to computer and communications equipment to authorized personnel;
    b. Protect sensitive equipment within the secured area using access controls or device locks; and
    c. Secure and limit access to all data on portable media (tapes, disks, hard copies, microfiche, etc.)

3. Management should implement the following to minimize risk of data loss and/or destruction:

    a. Purchase commercially available software products to access production data files;

b. Limit access to specified programs or user IDs by setting up each file for read-only or read-and-write access; and
c. Employing encryption, authentication, and dial back data protection techniques when accessing data-in-transit from one participant to another.

Note: Both encryption and authentication require the use of a key, which may reside on a hardware component, such as a circuit card, or may be a data element that is entered into a security program or system. The assignment, distribution, and control of encryption or authentication keys are important data security controls.

4. Management must maintain detailed written policies for software and data change controls. The policies should, at a minimum:

   a. Permit only authorized software and data changes;
   b. Document, review, and approve all changes before coding is done;
   c. Test changes from the developers by a different group;
   d. Install changes utilizing a group other than the developers and testers;
   e. Maintain prior versions of changed programs to reverse changes, if necessary;
   f. Change emergency programs and data only with appropriate management approval; and
   g. Complete audit trails of all the changes, including a record of who requested the change, and the before and after versions.

5. Management must restrict access on software products using:

   a. Operator passwords to prohibit entry by unauthorized personnel;
   b. Automatic features to control the number of unsuccessful password attempts, password expiration, or designated periods of inactivity;
   c. Multi-level functions, by password, to require dual control and ensure no single employee can create and send transactions (e.g., restricting one operator to file creation and a second operator to file approval or transmission);
   d. System administration level procedures to require secondary approval to assign, initiate, and maintain passwords; and
   e. Adequate oversight practices by periodically reviewing user access changes and logical security access.

6. Management must set dollar and file exposure controls. These limits are to be used and enforced at the time of entry, batch or file creation, and at the time of transmission. Exposure limits must be established across multiple settlement days to account for the potential of overlapping settlements. NACHA rules require a file limit, a daily aggregate file limit, and a three-day aggregate file limit be established. This is because the first day's transmission does not settle until day two or three, exposing the ODFI to credit risk for the aggregate of all unsettled transmissions over several days.

7. Management must require procedures to implement the following operational controls:

   a. File controls to ensure staff:
      1. Accounts for all files at each step in ACH processing;
      2. Only processes current files; and
      3. Does not accidentally or intentionally duplicate or omit files from processing.

   b. Dollar controls to:
      1. Confirm dollar totals at each step in ACH processing; and
      2. Help ensure ACH files are in balance, accounts are accurately posted, and settled as anticipated.

   c. Date controls (file creation date, effective entry date, and settlement date) to monitor that files are processed within the time frames established by the various regulations.

   d. Exception reporting to monitor:
      1. Circumstances such as over-limit activity;
      2. Anticipated files not received; and
      3. File inconsistencies suggesting errors, intrusions, or duplications.

   e. Audit trails including procedures to:
      1. Maintain a record of all ACH transaction data and all changes to static data;
      2. Respond to member inquiries;
      3. Reconstruct a sequence of events if a problem occurs; and
      4. Comply with NACHA rules.

   f. Reconciliation of entries on the Federal Reserve Statement must be performed to verify the ACH work settled as anticipated. Proper segregation of duties dictates staff responsible for reconciling ACH transaction not be otherwise involved in the ACH processing.

g. Internal audits of the ACH process: NACHA rules require each financial institution complete an audit of its ACH operations at lease once every year (a copy of which must be retained on file). Completion of the audit by all financial institutions reinforces compliance with the ACH rules and improves the overall quality of the ACH network.

Systemic Risk

Systemic risk exists when the inability of one ACH participant to settle its commitments causes other participants the inability to settle their commitments. The consequences could cause a ripple effect throughout the network.

Systemic risk is closely related to credit risk. While a fraudulent or erroneous transaction could be a source of systemic risk, it is far more likely a participant's failure would trigger a major settlement failure.

The likelihood of systemic risk varies greatly among payment systems. There is a connection between the dollar volumes a network handles and the systemic risk involved; the greater the number of high dollar payments a network processes, the greater the systemic risk, and the greater the need for elaborate risk controls.

The threat of systemic risk related to ACH transactions is very small. The average dollar value of an ACH transaction is significantly less than that of FedLine or Clearing House International Payments System. Rarely does a financial institution's position with respect to gross ACH settlement approach its capital level. It is far more likely a financial institution's position on the Fedwire network will exceed its capital.

Third-Party Risk

Third-party service providers are data processing service bureaus, financial institutions, or other organizations that provide ACH processing services. Examiners must be aware of the risks and concerns present when a corporate uses a third-party service provider and must determine whether the corporate has current, detailed agreements in place stipulating responsibility and accountability between the parties. Third-party risks are as follows:

1. Allowing a member to send files directly to the ACH operator: A corporate, acting as an ODFI that allows a member direct access to its ACH operator exposes itself to credit, fraud, and operational risk. The corporate warrants the validity of the transactions sight unseen and is ultimately responsible for the transactions. If the member fails or transmits fraudulent or erroneous entries, the corporate is responsible for the member's actions;
2. Using a correspondent DFI for processing and/or settlement: A correspondent bank provides processing and/or settlement services to the corporate acting as an ODFI. This situation exposes the corporate to credit, operational, and fraud risk because the correspondent could make a mistake or fail to process or settle its transactions; and
3. Using a correspondent DFI or data processing organization for ACH processing only (not settlement): A corporate acting as an ODFI is exposed only to the risk the third party will make a mistake or error. In this situation, the corporate faces only fraud and operational risk with respect to the third party processor.

OFAC Compliance with ACH Transactions

The Office of Foreign Assets Control (OFAC) is part of the Department of the Treasury and administers and enforces economic sanctions against targeted foreign countries, terrorism sponsoring organizations, and international narcotics traffickers based on U.S. foreign policy and national security goals. Compliance with OFAC rules for ACH transactions resides with the Originators of the transaction. Third-party service providers are not required to "unbatch" transactions to monitor OFAC rules. Corporates who do not originate but process for member credit unions should remind members they may not process ACH payments in violation of OFAC rules. The Originators could face penalties for processing blocked or rejected transactions. Corporates who do originate transactions must verify they are in compliance with OFAC rules on the transactions processed.

ACH Risk Management Handbook

NACHA publishes an ACH Risk Management Handbook, which is a comprehensive guide to the ACH risk issues and control procedures discussed above. Additionally, Western Payments Alliance (WesPay) publishes a self-audit survival guide for financial institutions to conduct or have conducted audits of its compliance with the ACH operating rules. The examiner should ask the corporate if they have this information on file to ensure they are informed about the various risks and are performing the necessary compliance audits.

If the corporate does not have this information on file, they can obtain it by writing or calling NACHA at:

NACHA-The Electronic Payments Association
13450 Sunrise Valley Drive, Suite 100
Herndon, Virginia 20171
(703) 561-1100

Legal Agreements

Detailed agreements must be in place between the corporate and all outside parties (e.g., credit unions, leagues) using the ACH service which detail the exact services provided and the various liabilities of each party. Also, agreements must be on hand between the corporate and the Federal Reserve or a third party processor, if one is used.

Reference 2 contains a list of issues that should be included in an agreement between an Originator and an ODFI. ACH agreements should be reviewed to determine that each of the recommendations is included.

Examination Objectives

The objectives for reviewing ACH operations are to:

1. Gain an understanding of the corporate's ACH operations and internal control environment;
2. Determine whether contracts and agreements are sufficient to protect the corporate's interests and comply with applicable rules, regulations and laws;
3. Evaluate logical security and user access policies to ensure they are sufficient to mitigate operating and fraud risk;
4. Determine the quality of risk management and support of ACH processing activities including policies, procedures, physical and accounting controls;
5. Evaluate the adequacy of ACH contingency plans;
6. Assess the risk of the corporate's future plans to the ACH operating environment and the credit union network; and
7. Determine the quality of risk management and related controls over ODFI activity.

Examination Procedures

See Corporate Examination Procedures - Automated Clearing House

Examination Questionnaire

See Corporate Examination Questionnaires - Automated Clearing House

References

1. FFIEC Information Systems Handbook, 2004 Edition;
2. NACHA Rulebook;
3. Uniform Commercial Code, Article 4A; and
4. ACH Risk Management Handbook.

Appendices

306A Examiner's Guide to APEX Security Settings

EXAMINER'S GUIDE TO APEX SECURITY SETTINGS

Introduction

APEX is U.S. Central Federal Credit Union's (USC) Internet based Automated Clearing House (ACH) processing system. This system allows participating corporate and natural person credit unions to submit ACH files to the Federal Reserve through USC using any PC with an Internet connection.

The participant, not USC, is responsible for establishing the system's various control features. This guide is intended to allow an examiner to determine whether or not the settings in use by the participant are appropriate and meet basic safety and soundness standards. It is not intended to be a complete review of ACH operations.

What to Ask For:

The examiner should request printouts of the following two screens or view the screens on the participant's PC:

1. ACH Options Screen
2. ACH Security Settings Screen

The ACH Options Screen provides a summary report that will allow the examiner to determine whether the exposure limits settings, dual controls features, and permitted transaction settings are "on" or "off".

The ACH Security Settings Screen provides a summary report of terminal control settings including password standards and password change intervals.

What to Look For:

A representation of each screen, an explanation of the settings, and recommended settings necessary to activate critical internal control features of APEX are provided in this guide.

By comparing the settings displayed on the participant's screens with the commentary and recommendations, the examiner can determine if the settings, as established by the participant, provide the basis for sound internal controls on APEX system access and ACH file creation.

APEX Credit Union Definition Screens

ACH Options

Should ACH risk management be performed? ○ Yes ○No

Third Party ACH Operator? ○ Yes ○No

Must batches be reviewed? ○ Yes ○ No

Must templates by reviewed? ○ Yes ○ No

Are PPD payments permitted? ○ Yes ○ No

Are CCD payments permitted? ○ Yes ○ No

Are TAX payments permitted? ○ Yes ○ No

Are CTX payments permitted? ○ Yes ○ No

Are ENR payments permitted? ○ Yes ○ No

Are XCK payments permitted? ○ Yes ○ No

Security Parameters

Must users be approved? ○ Yes ○ No

Number of invalid logons

Minimum user ID Length

Maximum user ID Length	
User ID Edit Check	Normal ○
	Character Only ○
	Alphanumeric ○
Minimum Password Length	
Number of Prior Passwords	
Password Change Days	
Default Product Timeout	

ACH Options Settings

Should ACH risk management be performed?

A "yes" setting requires an exposure dollar limit to be established. The exposure limit establishes the maximum dollar amount allowed for a single file or a cumulative maximum dollar amount allowed for one day's transactions. Any credit union originating ACH debit or credit entries should have an exposure limit set, both for its own internal applications and for any ACH customers transmitting ACH files through the credit union (such as a sponsor or payroll processor). **A "no" setting is a material internal control weakness for an Originating Depository Financial Institution (ODFI) and exception should be taken.**

If PPD payment or CCD entries are permitted (see description of these settings below), the setting should be "yes" with a maximum allowable dollar amount established for each type of entry. A no setting would only be appropriate if the credit union's origination activity is limited to returns and non-financial ACH entries.

Third Party ACH Operator?

A "yes" setting allows the credit union to create ACH files for multiple companies or entities such as small employee groups (SEG). A "no" setting means files may be created for only one entity, usually the credit union itself. Neither setting is critical to internal controls. Either a "yes" or "no" is acceptable; however the setting should reflect actual operations.

Must batches be reviewed?

This setting establishes dual controls on ACH file creation. The preferred setting is "yes". **A "no" setting is a material internal control weakness for a credit union sending PPD or CCD entries (see description of these settings below) since it would allow an individual to create and send an ACH file without second party review.**

Must templates be reviewed?

This setting establishes dual controls on ACH template creation. Templates reduce the entry time required for recurring files by pre-formatting some of the necessary information. The preferred setting is "yes". **A "no" setting is a material internal control weakness since it would allow someone to create a fictitious template without second party review.**

Are PPD payments permitted?

A “yes” setting allows consumer ACH debit and credit transactions to be entered. If ACH activity is to be limited to only ACH returns and non-financial transactions, the setting should be “no”.

Are CCD payments permitted?

A “yes” setting allows corporate cash concentration entries to be created. This activity is generally undertaken for businesses and potentially involves high dollar amounts. A credit union involved with only consumer ACH transactions does not need this authority and the setting should be set at “no”.

Are TAX payments permitted?

ACH activity involving a member’s tax payments holds significant risk. A “yes” setting for ACH tax activity should be carefully considered by the examiner. Management should demonstrate that it understands the risks associated with this type of activity.

Are CTX payments permitted?

This ACH application is for corporate trade exchange entries. This will rarely be applicable to credit union ACH operations and for most users the setting should be “no.”

Are ENR payments permitted?

ENR ACH entries are automated enrollment entries to sign a member up for government electronic benefits payments such as social security or other pension programs. Even a small credit union that is not involved in ACH financial entries will likely want this setting to be “yes”. Since ENR entries are non-financial and do not involve the actual payments themselves, a “yes” setting represents minimal risk.

Are XCK payments permitted?

XCK entries involve destroyed checks. Having this setting at “yes” would rarely be necessary for a credit union; although, a “yes” setting in itself holds minimal risk.

APEX Security Parameter Settings

Must users be approved?

This setting enables required second party approval for adding a new user or changing an existing user's authorities. **A "no" setting is a material internal control weakness and exception should be taken since a no setting allows changes to user authorities without second party review.**

Number of invalid logons?

An appropriate number of invalid logon attempts is 3. A setting greater than 3 holds increased risk. If the setting is significantly higher than 3, exception should be taken.

Minimum user ID Length?

The default setting is 4. Exception should be taken if this setting is less than 3 since a shorter ID holds a higher risk that the ID could be chanced upon or compromised.

Maximum user ID Length?

APEX allows user IDs to be up to 16 characters in length. The higher the number assigned, the lower the risk of a compromised ID. Industry security practices recommend minimum user ID lengths of 7 or more characters. ID lengths of 4 or 6 characters are common. However, examiners should encourage credit unions to adhere to industry best practices.

User ID Edit Check?

User IDs may be letters, numbers, or a combination of both. The best security is provided by a combination of letters and numbers including both upper and lower case characters.

Minimum Password Length?

Passwords should be no less than four characters in length. However, industry best security practices encourage passwords of 7 or more characters. Examiners should encourage credit unions to adhere to industry best practices.

Number of Prior Passwords?

Password changes should require at least three change intervals before a password can be reused. (See Password Change Days)

Password Change Days?

The recommended password change interval is no less than 30 days.

Default Product Timeout?

This setting invokes a screen saver (blank screen) after the established time period of inactivity. A setting of 10 minutes or less is recommended as an industry best security practice; although the APEX default value is 15 minutes.

Chapter 307

CONTINGENCY PLANNING

Introduction

Corporate credit unions (corporates) have an integral role within the credit union community, serving as a depository for a large portion of credit unions' excess liquidity, and providing numerous correspondent services. A disruption in a corporate's operations for an extended period of time could be disastrous, not only for the corporate, but also its members. Thus, it is imperative contingency plans be developed detailing the alternative site(s) available in the event of service disruptions.

The primary objective in reviewing the contingency plan is to determine it adequately documents management's plans and its implementation has been demonstrated. Contingency plans and arrangements will vary among corporates, as a function of size, complexity, and a multitude of other variables.

Corporate Contingency Planning

The corporate's business continuity planning (BCP) process should reflect the following objectives:

- BCP is about maintaining, resuming, and recovering the business, not just recovery of the technology.
- The planning process should be conducted on an organizational basis.
- A thorough business impact analysis (BIA) and risk assessment is the foundation of an effective BCP.
- The effectiveness of a BCP can only be validated through testing or practical application.
- The BCP and test results should be subjected to an independent audit and reviewed by the board of directors.
- A BCP should be periodically updated to reflect and respond to changes in the financial institution or its service provider(s).

Written Disaster Recovery Plan

The corporate must have a comprehensive written disaster recovery plan. The plan must outline the specific courses of action management and staff will take following an occurrence which interrupts its ability to provide member services. Although it is impossible to anticipate every scenario, an adequate plan will address disruptions of varying severity and duration. The plan should address all critical services and operations provided by both internal departments and external sources. The plan must be a coordinated effort to minimize service disruptions to members, minimize financial losses, and ensure a timely resumption of operations in the event of a disaster.

To develop a reasonable and appropriate plan, management must perform a BIA to determine the criticality of each product or process and a risk assessment to evaluate risk scenarios. This will include a review of each department to assess their criticality in providing member services and their dependence on outside parties for continued performance. Plans must be developed to restore critical operational areas and service affected by a disaster.

The board of directors should review and approve the disaster recovery plan annually. Additionally, the board should be apprised of the scope, frequency, and results of contingency testing. The board should also ensure they are satisfied operating management implemented appropriate corrective action for significant contingency testing concerns.

During short-term disruptions, generally lasting less than one day, it may not be necessary for the corporate to relocate its operations. However, the plan should outline steps to be taken during such situations to ensure timely processing and transaction settlement. The plan must address and prioritize each "critical" operation within the corporate.

For disruptions exceeding one day, the plan needs to provide detailed relocation procedures for the corporate's operations. It would be preferable if the corporate has a dedicated facility which is readily equipped for the corporate to immediately use when a disaster occurs. (See further discussion in the section entitled Disaster Recovery Sites.)

A contingency job description should be developed for each employee outlining that individual's duties during implementation of the plan. This is necessary for two reasons:

1. During a disaster, the duties of some employees who normally perform non-critical functions may change significantly; and
2. During certain types of disasters, some employees may be unable to report to work; therefore, other employees will be required to perform their duties.

The emergency job descriptions should be cross referenced to position desk manuals and/or written operational procedure manuals.

BIA

A Business Impact analysis (BIA) is the first step in developing a BCP. It should include:

- Identification of the potential impact of uncontrolled, non-specific events on the institution's business processes and its members;
- Consideration of all departments and business functions, not just data processing; and
- Estimation of maximum allowable downtime and acceptable levels of data, operations, and financial losses.

Risk Assessment

For a disaster recovery plan to meet its objectives, management must evaluate the types of risk the institution is susceptible to and the impact each risk occurrence could have on financial performance, operations, and member services.

The risk assessment is the second step in developing a BCP. It should include:

- A prioritizing of potential business disruptions based upon severity and likelihood of occurrence;
- A gap analysis comparing the institution's existing BCP, if any, to what is necessary to achieve recovery time and point objectives; and
- An analysis of threats based upon the impact on the institution, its members, and the financial markets, not just the nature of the threat.

There are a number of risks that could potentially impact a corporate. The risks may be different between institutions as a result of geography, local environment, or the services offered. It is imperative management clearly identify and assess the risks associated with their unique operation.

Some potential risks management should consider are:

1. Natural - fire, flood, earthquake, hurricane;
2. Technical - hardware/software failure, power disruption, communications interference;
3. Human - riots, strikes, disgruntled employees and terrorist acts; and
4. Pandemic Infectious Disease Outbreak – a threat with the ability to spread rapidly over large areas, possibly worldwide.

Disaster Recovery Sites

Each corporate must have an alternate facility equipped and ready for immediate use in the event of a disaster. The facility, referred to as a recovery site, must be located far enough from the corporate to minimize the possibility of both locations being affected by a regional disaster. The recovery site should be located in a separate power grid and be served by a separate telephone central office than the corporate. The recovery site should be accessible to employees within a reasonable period of time.

The recovery site facility must be large enough and sufficiently supplied and equipped to accommodate the corporate's entire operation with a minimum number of employees needed for day-to-day operations. The contingency site contract must indicate the location will be available for a sufficient amount of time to allow the corporate to locate a new permanent facility, if necessary.

In some cases a corporate may establish its own alternative site, while in other cases the corporate shares a location with other entities. Cost is a major factor. Various companies market memberships in recovery sites at a set annual fee.

It is in the best interest of the corporate to have a written agreement with the management of the recovery site, or other parties with which they share the facility. The agreement should detail the conditions under which the site may be used. It is imperative should a disastrous event occur, the recovery site location is available and has the capability to handle the critical operations.

All of the corporate's essential personnel should have an understanding of the disaster recovery plan. Employees should know what to do if an emergency occurs and where and when to report to the recovery site location. The use of periodic tabletop walk-through exercises will enhance that knowledge. The facility should be tested, at least annually, to ensure it meets minimum requirements to continue essential services.

Reciprocal Agreements

Many corporates enter into agreements with their members or other corporates with compatible hardware/software capabilities. These arrangements usually are made on a "best efforts" basis whereby Corporate A agrees to backup Corporate B provided Corporate A has time available. There is a mutual agreement to share office facilities, data processing capacity, or other services in a disaster. This type of arrangement is less desirable than one where dedicated facilities are available, because it relies on the excess capacity of the reciprocal institution. Since the needs of parties are continually evolving, it is difficult for management to determine whether the available excess capacity is adequate to meet present or future demands. Presumably, the reciprocal institution would take care of its own needs first. Many reciprocal agreements contain written limitations to that effect.

Reciprocal agreements can play an important role in providing a secondary backup site in the event of a regional catastrophe rendering both the primary and recovery site locations inoperable. These agreements outlining both parties' responsibilities should be in a written contact.

Disaster Recovery Testing

The most comprehensive disaster recovery plan may be of little value if, under actual conditions, it fails to perform adequately. It is incumbent upon management to ensure to the best of their ability the plan will perform as proposed. Each corporate must perform at least a full scale test of its disaster recovery plan on an annual basis. Additionally, larger corporates may need to independently test various aspects of the plan more frequently (i.e., information systems, funds transfer, ACH, and item processing). A full scale test is one which covers all aspects of the corporate's operation and includes a full day's business volume. Item processing operations may be tested independently.

Periodic review should be performed to ensure, when a full-scale test is performed, all employees are familiar with their duties and responsibilities. Where practical, surprise tests could also be included to ensure employees maintain ongoing familiarity with the plan. In an actual emergency, the plan is more likely to be effective if all employees remain calm and are familiar with their responsibilities. Walk-through exercises will help keep staff familiar with the plans.

Corporates must maintain detailed documentation of each disaster recovery test. The results should be subjected to an independent audit and reviewed by the board of directors and senior management. Officials should utilize test results to make any necessary revisions to the plan to address weakness identified during testing.

Protective Measures Against Disasters and Disruptions

Physical disasters can be created by man or result from natural phenomena. Regardless of the cause, the best plan to prevent severe loss is effective backup procedures covering equipment, data, operating systems, application software, communication resources and documentation. These provisions enable reconstruction with minimal confusion and delay. Following are the basic security measures for major physical risks:

<u>Fire</u>

Computer center personnel must know what to do in a fire emergency. Instructions should be posted in prominent locations. Fire alarm boxes and emergency power switches should be clearly visible and unobstructed. Fire drills should periodically be held. Personnel should know how to respond to automatic extinguisher systems, as well as the location and operation of power and shut-off valves. Data centers should have industry standard chemical based fire suppressant systems. Where only water based systems are available, waterproof covers should be located near equipment in the event the sprinklers are activated. Hand extinguishers should be placed in readily accessible locations. All computer installations should be equipped with heat or smoke detectors. Detectors should be located away from air conditioning or intake ducts as they may hinder the build up of smoke required to trigger the alarm. Walls, doors, and partitions should be fire-resistant. The degree of fire protection in the data center should be consistent with the ability to easily restore information.

<u>Flooding</u>

A corporate should not locate its computer installation in or near a flood plain. If the computer equipment is placed below ground level or a sprinkler system is used, precautions to limit water damage should be taken. If there is a floor above the computer room, the computer room ceiling should be sealed to prevent water seepage.

Sabotage and Riot

Computer center personnel should know how to handle intruders, bomb threats, and other disturbances. Since attacks on computer installations have occurred, their locations should be inconspicuous. Sabotage could be caused by a disgruntled employee. Therefore, personnel policies should address the process for the immediate termination and removal from the premises of any employee considered a threat. Locked doors, intrusion detection devices, guard and other controls that restrict physical access are important preventative measures.

Power Failure

Voltage coming into the data center is often monitored by a recording voltmeter and regulated to prevent power fluctuations. In the event of power failure, an alternative power source should be provided. Independent power supply units consist of gas or diesel generators or a battery arrangement, providing electricity for a limited period to allow an orderly system shutdown. Most corporates use an uninterruptible power supply (UPS) system to allow an orderly critical function shut down.

Fraud or Theft

Physical measures to safeguard against loss from fraud or theft are comparable to those outlined for sabotage and riot. Exposure is reduced by restricting access to information that may be altered or stolen. Since fraud or theft may be perpetrated easily by insiders, personnel policies should be designed to minimize that possibility. Procedures to safeguard information are essential to ensure member confidence. This is supported by a strong system of internal controls and audit function. Additionally, there may be legal implications for the corporate if sensitive or confidential information pertaining to a member is released.

Equipment Failure

Equipment failure may result in extended processing delays. Performance of preventive maintenance enhances system reliability and should be extended to all supporting equipment, such as temperature and humidity control systems and alarm or detection devices.

Pandemic Planning

Pandemic planning presents unique challenges to the credit union community unlike most natural or technical disasters and malicious acts. The impact of a pandemic is much more difficult to determine because of the difference in the scale and duration of a pandemic event. As a result of these differences, corporates must plan for the potential adverse effects of a pandemic event. Experts believe the most significant challenge may be the severe staffing shortage likely to result from a pandemic outbreak.

Continuity plans to manage a pandemic event should include:

- A preventative program to reduce the likelihood the operations will be significantly affected by a pandemic event;
- A documented strategy which provides for scaling pandemic efforts;
- A comprehensive framework of facilities, systems, or procedures to continue critical operations if a large number of staff are unavailable for prolonged periods;
- A testing program to ensure the pandemic planning practices and capabilities are effective; and
- An oversight program to ensure ongoing review and updates are made to the pandemic plan.

Hardware Backup

Hardware backup is a critical step in contingency planning. The corporate needs to consider alternate processing capabilities for each of its computer installations in the event the work environment becomes disabled. These plans can take several forms and involve the use of another financial institution, data center, or installation.

In addition, hardware manufacturers and software vendors can be helpful in locating an alternate processing site and in some cases will be able to provide backup equipment under emergency conditions. In planning the recovery site facility, the corporate should consider the adequacy of hardware at the location, the ability to quickly relocate hardware, or an agreement to share compatible hardware at another facility.

Program or Software Backup

Software backup is another important phase of contingency planning. The program backup for all hardware platforms consists of three basic areas:

1. Operating system software;
2. Application software; and
3. Documentation.

All software and related documentation must have adequate off-premise storage. Even when using a "standard" software package from one vendor, the software will likely vary from one location to another based on options chosen by the institution during or subsequent to system implementation.

The operating system must be backed-up with at least two copies of the current version. Without it, even the most sophisticated computer hardware is useless. One copy should be stored in the tape and disk library for immediate availability in the event the original is impaired. The second copy should be stored in a secure, off-premise location. Duplicate copies should be tested periodically and recreated whenever there is a change in the original.

Application software, which includes both source and object versions of all application programs must be maintained in the same manner as the operating system software. Backup copies of programs must be updated as program changes are made. Minor updates to backup copies can be made on a group basis, but major revisions or enhancements to application programs should be updated immediately. Storing, testing, and updating such software should be addressed in the contingency plan.

Software vendors can usually supply institutions with copies of standard application software products if the originals are destroyed.

However, even assuming the vendor accurately maintained the institution’s parameters, selections, and modifications, there will probably be additional expenses and some delay in making the software operational. Under these circumstances, the institution is placing responsibility for storing software with vendors. Most vendors are reluctant to guarantee software availability, because they may not have current sets of the institution’s software. Thus, the corporate should maintain its own software backup at an off-site location to ensure minimal processing interruption during an emergency.

Documentation for the operating system and the application programs should also be backed up. A minimum level of documentation should be maintained at an off-site location. This should include current copies of:

1. Operating system options and modifications;
2. Application flowcharts;
3. Descriptive narrative for all systems and programs;
4. File layouts and transaction codes;
5. Operator run instructions; and
6. User manuals.

Procedure manuals are also necessary during disaster recovery. Duplicate copies of all critical procedures should be stored at the off-site location. Most importantly, a copy of the procedures outlining operations during emergencies must be maintained off-site.

Data File Backup

The most important area of backup involves the institution’s data files, regardless of the platform in which the data is located. Financial institutions must always be able to generate a current master file. Data files must be backed up both on and off site to provide recovery capability. Retention of current data files, or older master files and the transaction files necessary to bring them current, is important so processing can continue after disasters occur. The creation and rotation of data file backups is a daily activity in most institutions.

Telecommunications Backup

A data center must develop an effective backup plan, including an agreement for alternative site processing. For telecommunications, that plan also must address the communications media and equipment. The contingency plan should establish priorities and identify critical components of the network. Rerouting and redundancy may permit the use of alternate equipment, facilities, lines and circuits, but may still be limited by other considerations. Considerations include risk versus economics, the practicality of the selected backup components, and the security and data integrity provided by the backup plan.

Risks may be addressed by assessing individual components in the network, the dependence on each component, and the probability of it going down or becoming unavailable or unreliable. The costs of various backup alternatives must be weighed against the extent of risk protection each provides. This assessment also should address costs associated with testing, since all components of a plan should be periodically tested.

Financial institutions should have a file identifying all circuits by circuit number and a matrix outlining their location, priorities and uses. A duplicate of this file should be maintained at a different location in case of any problems.

The backup plan must address the practicality of each component. Selected alternatives must be able to accommodate the anticipated volumes or capacities at the necessary speeds to meet the established priorities. Reliability, flexibility, and compatibility - all components of the original planning process - also must be considered in formulation of the backup plan. Additionally, the telecommunications backup plan must be compatible with other contingency plans in the corporate, since it will affect users, data processing, and members.

Security and the data integrity of alternate components used must be considered in the contingency plan. Different components provide different quality and possess different risks. Alternate equipment selected should be checked to determine if it permits encryption.

The relative importance of applications processed and the extent a corporate depends on its telecommunications system will determine the degree of backup required. Management should make a careful appraisal of its backup requirements, decide on an effective plan, detail the procedures, and periodically test its effectiveness.

Examination Objectives

The examiner is to determine if the board of directors and operating management have taken necessary steps to ensure an appropriate contingency plan is in place to maintain the institution's critical operations and services in the event of a disaster. The examiner will need to determine:

1. The board of directors has adopted a written disaster recovery plan;
2. Appropriate review and analysis, in the form of a BIA and Risk Assessment have been performed by management to assess the potential risks and establish operational priorities during disaster occurrences;
3. The corporate has a recovery site location that will be available and fully functional in an emergency situation;
4. The corporate has in place written agreements, as necessary, with recovery site management, vendors, etc. If applicable, a reciprocal agreement is in place with the other institution that agrees to share facilities and capacity;
5. Disaster recovery plan testing is performed at least annually. Documentation of the tests is maintained and reviewed by the officials;
6. The disaster recovery plan is revised, as necessary, to address changes in operations, and to resolve problems arising during testing; and
7. The officials have taken steps to address protective measures against disasters and/or disruptions.

Examination Procedures

See Corporate Examination Procedures - Contingency Planning (OCCU 307P).

Examination Questionnaire

See Corporate Examination Questionnaire - Contingency Planning (OCCU 307Q).

References

1. FFIEC Information Systems Examination Handbook
2. NCUA Letter to Credit Unions (08-CU-01) Guidance on Pandemic Planning

Chapter 308

COMPLIANCE

Introduction

During each examination, examiners will review the corporate credit union's (corporate) compliance with regulations promulgated by NCUA and other agencies. Examiners must disclose violation of the laws, statutes, regulations, and sound business practices in the examination report and on OCCU Form 102F, the Document of Resolution.

This chapter outlines references to various Part 704 compliance issues as well as other applicable parts of the NCUA Rules and Regulations. More specific information can be obtained in the applicable chapters, as noted with the specific reference. Where there is no specific chapter for a compliance issue, the items are discussed herein.

Section 704.3 - Corporate Credit Union Capital

See Chapter 204, Capital and Appendix A to Part 704—Model Forms.

Section 704.4 - Board Responsibilities

See Chapter 301, Management.

Section 704.5 - Investments

See Chapter 201, Investments and Appendix B to Part 704- Expanded Authorities and Requirements.

Section 704.6 - Credit Risk Management

See Chapters 201, Investments, and 202 Asset and Liability Management.

Section 704.7 - Lending

See Chapter 203, Loan Review.

Section 704.8 - Asset and Liability Management

See Chapter 202, Asset and Liability Management.

Section 704.9 - Liquidity Management

See Chapter 202, Asset and Liability Management.

704.10—Investment Action Plan

See Chapter 201, Investments.

704.11--Corporate Credit Union Service Organizations (CUSOs)

See Chapter 311, Corporate Credit Union Service Organizations.

704.14—Representation

Each examiner must ensure the board of directors is in compliance with all phases of this section which addresses interlocks, representatives of organizational members, recusal provisions, and administration.

704.15-- Audit Requirements

See Chapter 309, Supervisory Committee/Audit Functions.

704.16 Contracts/Written Agreements

See Chapter 301, Management.

704.18 Fidelity Bond and Insurance Coverage

See Chapter 310, Bond and Insurance Coverage.

704.19-- Wholesale Corporate Credit Unions

Wholesale corporates are subject to all sections of Part 704, except for in this section it is subject to a different determination of earnings retention factor and threshold for notification of the board of directors, supervisory committee, and the OCCU Director.

748 – Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act

Security Devices

Part 748 establishes minimum security standards and procedures for credit unions. The examiner should determine the corporate has (1) established adequate security programs in accordance with the regulation, and (2) updates the program to reflect operational changes.

Corporate credit union management must provide adequate safeguards to:

1. Protect the credit union from robberies, burglaries, larcenies, and embezzlement;
2. Ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;
3. Respond to incidents of unauthorized access to or use of member information that could result in substantial harm or serious inconvenience to a member;
4. Assist in identification of persons who commit or attempt such actions and crimes; and
5. Prevent destruction of vital records (as defined by Part 749 of the NCUA Rules and Regulations).

The corporate’s security program must include administrative, technical, and physical safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities. At a minimum, corporate management should design and implement a comprehensive written security program to:

1. Identify key controls, systems, and procedures;
2. Assess internal and external threats;
3. Assign responsibilities;
4. Establish security procedures consistent with operating systems;
5. Provide for periodic training of all employees;
6. Protect against destruction, loss, or damage of information, and develop recovery procedures;
7. Ensure periodic testing of security programs;
8. Re-assess threats and the adequacy of controls;
9. Review monitoring systems and control procedures; and
10. Revise strategies.

Examiners will evaluate management's efforts to identify, assess, measure, mitigate, and monitor risks.

Bank Secrecy Act

Part 748.2 – This section of the NCUA Rules and Regulations ensures that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of Subchapter II of Chapter 53 of Title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated thereunder by the Department of Treasury, 31 C.F.R Part 103. Refer to Appendix A of this Chapter for guidance on Bank Secrecy Act requirements and examination guidelines.

Office of Foreign Assets Control (OFAC)

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President's wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations. Refer to Appendix B for additional information on OFAC compliance requirements.

Other Compliance Considerations

Charter and Bylaws

Examiners will review the corporate's charter and bylaws to determine if the corporate is operating within its limitations.

Operating Fees

Examiners must ensure that each Federal corporate complies with Section 701.6. This section states that each year or as otherwise directed by the NCUA Board, each Federal credit union shall pay to the Administration for the current NCUA fiscal year (January 1 to December 31) an operating fee. This fee will be in accordance with the schedule fixed from time to time by the NCUA Board, based on the total assets of each Federal credit union as of December 31 of the preceding year, or otherwise determined pursuant to paragraph (b) of this section.

Share Insurance

During each examination of a federally insured corporate, examiners must review the National Credit Union Share Insurance Fund (NCUSIF) account for accuracy. Examiners must document errors detected in the examination report along with corrective actions taken.

Examination Objectives

The objectives for reviewing the compliance area are:

1. Determine the corporate's policies, procedures, practices, and internal controls of all aspects of compliance are adequate as defined under regulation and federal and/or state laws;

2. Determine all reports required of corporates are filed accurately and timely;

3. Assess the adequacy of the credit union's BSA/AML compliance program. Determine whether the corporate has developed, administered, and maintained an effective program for compliance with the BSA and all of its implementing regulations.

4. Assess the corporate's risk-based OFAC program to evaluate whether it is appropriate for the institution's risk, taking into consideration its products, services, members, transactions, and geographic locations.

5. Determine the National Credit Union Share Insurance Fund and NCUA operating fees, where applicable, are accurate and paid on time; and

6. Initiate corrective action when the policies, procedures, practices, or controls are deficient or when violations of laws or regulations are noted.

Examination Procedures

See Corporate Examination Procedures - Compliance (OCCU BSA and OFAC Procedures).

Examination Questionnaire

See Corporate Examination Questionnaires - Compliance (OCCU BSA/AML and OFAC Questionnaires).

References

1. NCUA Rules and Regulations, Part 704

2. NCUA Rules and Regulations, Section 701.6

3. NCUA Rules and Regulations, Part 748

4. NCUA Rules and Regulations, Part 749

5. NCUA Website/Reference Information/Letters to Federal Credit Unions and Letters to Federally Insured Credit Unions

6. Chapter 18 (Regulatory Compliance) of the natural person credit union Examiner's Guide

7. Appendix 18A (Bank Secrecy Act) of the natural person credit union Examiner's Guide

8. Corporate Credit Union Guidance Letter No. 2004-02, June 2004, BSA Compliance Guidance

9. Corporate Credit Union Guidance Letter No. 2005-01, February 2005, Bank Secrecy Act (BSA) Compliance

10. FFIEC BSA/AML Examination Manual, July 2006

Excerpts from the Federal Financial Institutions Examination Council's BSA/AML Examination Guide

The federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks and credit unions. The federal banking agencies are charged with chartering (National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision), insuring (Federal Deposit Insurance Corporation and National Credit Union Administration), regulating, and supervising banks, credit unions, and savings associations. 12 USC 1818(s)(2) requires the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository institution.

This Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual provides guidance to all of the banking agencies examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations. The development of the examination manual was a collaborative effort of the federal banking agencies and the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, to ensure consistency in the application of the BSA/AML requirements. In addition, OFAC assisted in the development of the sections of the manual that relate to OFAC reviews.

While OFAC regulations are not part of the BSA, examination procedures include examining a bank or corporate credit union's policies, procedures, and processes for ensuring compliance with OFAC sanctions. Refer to Appendix 308B for more information on OFAC.

The federal banking agencies require each institution under their supervision to establish and maintain a BSA compliance program. In accordance with the Patriot Act, FinCEN's regulations require certain financial institutions to establish an AML compliance program that guards against money laundering and terrorist financing and ensures compliance with the BSA and its implementing regulations.

As part of a strong BSA/AML compliance program, the NCUA seeks to ensure each credit union has policies, procedures, and processes to identify and report suspicious transactions to law enforcement. The examination process assesses whether credit unions have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions reported.

NCUA Rules and Regulations, Part 748.2 require credit unions to develop and provide for the continued administration of a BSA compliance program reasonably designed to assure and monitor compliance with Department of Treasury regulations and related BSA implementing laws and regulations. The compliance program must be commensurate with its respective BSA/AML risk profile. Furthermore, the program must be fully implemented and reasonably designed to meet the BSA requirements. Policy statements alone are not sufficient; practices must coincide with the credit union's written policies, procedures, and processes. The compliance program must be:

- written
- approved by the board of directors, and
- be reflected in the minutes of the credit union.

Each credit union must also comply with the U.S.A. Patriot Act and its promulgating regulations and laws, which require a customer identification program to be implemented as part of the BSA compliance program.

The BSA/AML compliance program shall at a minimum:

1) provide for a system of internal controls to assure ongoing compliance;
2) provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

3) designate an individual responsible for coordinating and monitoring day-to-day compliance; and
4) provide training for appropriate personnel.

Risk Assessment

An effective BSA/AML compliance program requires sound risk management. The same risk management principles the credit union uses in traditional operational areas should be applied to assessing and managing BSA/AML risk. A well-developed risk assessment will assist in identifying the credit union's BSA/AML risk profile. Understanding the risk profile enables the credit union to apply appropriate risk management processes to the BSA/AML compliance program to mitigate risk. This risk assessment process enables management to better identify and mitigate gaps in the credit union's control environment. The risk assessment should provide a comprehensive analysis of the BSA/AML risks in a concise and organized presentation. The risk assessment should be shared and communicated with all business lines across the financial institution, the board of directors, management, and appropriate staff. As such, it is a sound practice the risk assessment be reduced to writing.

Examiners should review and evaluate the reasonableness of the credit union's BSA/AML risk assessment. The development of the BSA/AML risk assessment generally involves two steps: first, identifying the specific risk categories (i.e., products, services, members, entities, and geographic locations) unique to the credit union; and second, conducting a more detailed analysis of the data identified to better assess the risk within these categories. In reviewing the risk assessment, the examiner should determine whether management has considered all products, services, members, and geographic locations, and whether management's detailed analysis within these specific risk categories was adequate. If the credit union has not developed a risk assessment, this fact should be discussed with management. For the purposes of the examination, whenever the credit union has not completed a risk assessment, or the risk assessment is inadequate, the examiner must complete a risk assessment based on available information. Refer to the FFIEC BSA/AML Examination Manual Appendices I and J for more information on risk assessments.

System of Internal Controls

Management should structure the credit union's BSA/AML compliance program to adequately address its risk profile, as identified by the risk assessment. Management should understand the credit union's BSA/AML risk exposure and develop the appropriate policies, procedures, and processes to monitor and control BSA/AML risks. For example, the credit union's monitoring systems to identify, research, and report suspicious activity should be risk-based, with particular emphasis on high risk products, services, members, and geographic locations as identified by the credit union's BSA/AML risk assessment.

The board of directors, acting through senior management, is ultimately responsible for ensuring the credit union maintains an effective BSA/AML internal control structure, including suspicious activity monitoring and reporting. The board of directors and management should create a culture of compliance to ensure staff adherence to the credit union's BSA/AML policies, procedures, and processes.

Internal Controls

Internal controls are the credit union's policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the credit union. Large complex credit unions are more likely to implement departmental internal controls for BSA/AML compliance. Departmental internal controls typically address risks and compliance requirements unique to a particular line of business or department and are part of a comprehensive BSA/AML compliance program. Internal controls should:

- Identify "banking" operations (products, services, members, and geographic locations) more vulnerable to abuse by money launderers and criminals; provide for periodic updates to the credit union's risk profile; and provide for a BSA/AML compliance program tailored to manage risks.

- Inform the board of directors, or a committee thereof, and senior management, of compliance initiatives, identified compliance deficiencies, and corrective action taken, and notify directors and senior management of Suspicious Activity Reports (SARs) filed.
- Identify a person or persons responsible for BSA/AML compliance.
- Provide for program continuity despite changes in management or employee composition or structure.
- Meet all regulatory recordkeeping and reporting requirements, meet recommendations for BSA/AML compliance, and provide for timely updates in response to changes in regulations.
- Implement risk-based customer due diligence (CDD) policies, procedures, and processes.
- Identify reportable transactions and accurately file all required reports including SARs, Currency Transaction Reports (CTRs), and CTR exemptions. (Credit unions should consider centralizing the review and report filing functions within the organization.)
- Provide sufficient controls and systems for filing CTRs and CTR exemptions.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Provide for adequate supervision of employees that handle currency transactions, complete reports, grant exemptions, monitor for suspicious activity, or engage in any other activity covered by the BSA and its implementing regulations.
- Incorporate BSA compliance into the job descriptions and performance evaluations of appropriate personnel.

The above list is not all-inclusive and should be tailored to reflect the credit union's BSA/AML risk profile. Refer to the FFIEC BSA/AML Examination manual for additional policy guidance for specific risk areas.

Independent Testing

As part of the scoping and planning process, examiners should obtain and evaluate the supporting documents of the independent testing (audit) of the credit union's BSA/AML compliance program. The scope and quality of the audit may provide examiners with a sense of particular risks in the credit union, how these risks are being managed and controlled, and the status of compliance with the BSA. The independent testing scope and work papers can assist examiners in understanding the audit coverage and the quality and quantity of transaction testing. This knowledge will assist examiners in determining the examination scope, identifying areas requiring greater (or lesser) scrutiny, and identifying when expanded examination procedures may be necessary.

Independent testing should review the credit union's risk assessment for reasonableness. Additionally, management should consider the staffing resources and the level of training necessary to promote adherence with these policies, procedures, and processes. For credit unions that assume a higher risk BSA/AML profile, management should provide a more robust program, specifically monitoring and controlling the higher risks management and the board have accepted.

Parties Conducting Independent Testing & Frequency

A credit union's internal audit department, outside auditors, consultants, or other qualified independent parties should conduct independent testing. While the frequency of audit is not specifically defined in any statute, a sound practice is for the credit union to conduct independent testing generally every 12 to 18 months, commensurate with the BSA/AML risk profile of the credit union. Credit unions that do not employ outside auditors or consultants or have internal audit departments may comply with this requirement by using qualified persons <u>who are not involved</u> in the function being tested. The persons conducting the BSA/AML testing should report directly to the board of directors or Supervisory Committee.

Those persons responsible for conducting an objective independent evaluation of the written BSA/AML compliance program should perform testing for specific compliance with the BSA, and evaluate pertinent management information systems (MIS). The audit should be risk based and evaluate the quality of risk management for all "banking" operations, departments, lines of business, and subsidiaries. The testing should assist the board of directors and management in identifying areas of weakness or areas where there is a need for enhancements or stronger controls.

BSA Compliance Officer

The credit union's board of directors must designate a qualified individual to serve as the BSA compliance officer. The BSA compliance officer is responsible for coordinating and monitoring day-to-day BSA/AML compliance. The BSA compliance officer is also charged with managing all aspects of the BSA/AML compliance program and with managing the credit union's adherence to the BSA and its implementing regulations; however, the board of directors is ultimately responsible for the credit union's BSA/AML compliance.

While the title of the individual responsible for overall BSA/AML compliance is not important, his or her level of authority and responsibility within the credit union is critical. The BSA compliance officer may delegate BSA/AML duties to other employees, but the officer should be responsible for overall BSA/AML compliance. The board of directors is responsible for ensuring the BSA compliance officer has sufficient authority and resources (monetary, physical, and personnel) to administer an effective BSA/AML compliance program based on the credit union's risk profile.

The BSA compliance officer should be fully knowledgeable of the BSA and all related regulations. The BSA compliance officer should also understand the credit union's products, services, members, and geographic locations, and the potential money laundering and terrorist financing risks associated with those activities. The appointment of a BSA compliance officer is not sufficient to meet the regulatory requirement if that person does not have the expertise, authority, or time to satisfactorily complete the job.

The line of communication should allow the BSA compliance officer to regularly apprise the board of directors and senior management of ongoing compliance with the BSA. Pertinent BSA related information, including the reporting of SARs filed with FinCEN, should be reported to the board of directors or an appropriate board committee so these individuals can make informed decisions about overall BSA/AML compliance. The BSA compliance officer is responsible for carrying out the direction of the board and ensuring employees adhere to the credit union's BSA/AML policies, procedures, and processes.

Training

Credit unions must ensure appropriate personnel are trained in applicable aspects of the BSA. Training should include regulatory requirements and the credit union's internal BSA/AML policies, procedures, and processes. At a minimum, the credit union's training program must provide training for all personnel whose duties require knowledge of the BSA. The training should be tailored to the person's specific responsibilities. In addition, an overview of the BSA/AML requirements typically should be given to new staff during employee orientation. Training should encompass information related to applicable business lines, such as trust services, international, and private banking. The BSA compliance officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements as well as the activities and overall BSA/AML risk profile of the credit union.

The board of directors and senior management should be informed of changes and new developments in the BSA, its implementing regulations and directives, and the federal banking agencies' regulations. While the board of directors may not require the same degree of training as operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed to the credit union. Without a general understanding of the BSA, the board of directors cannot adequately provide BSA/AML oversight; approve BSA/AML policies, procedures, and processes; or provide sufficient BSA/AML resources.

Training should be ongoing and incorporate current developments and changes to the BSA and any related regulations. Changes to internal policies, procedures, processes, and monitoring systems should also be covered during training. The program should reinforce the importance the board and senior management place on the credit union's compliance with the BSA and ensure all employees understand their role in maintaining an effective BSA/AML compliance program. Examples of money laundering activity and suspicious activity monitoring and reporting can and should be tailored to each individual audience. For example, training for tellers should focus on examples involving large currency transactions or other suspicious activities;

training for the loan department should provide examples involving money laundering through lending arrangements.

Credit unions should document their training programs. Training and testing materials, the dates of training sessions, and attendance records should be maintained by the credit union and be available for examiner review.

As part of the scoping and planning procedures, examiners must review the credit union's OFAC risk assessment and independent testing to determine the extent to which a review of the credit union's OFAC program should be conducted during the examination.

Suspicious Activity Reporting

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Within this system, FinCEN and the federal banking agencies recognize, as a practical matter, it is not possible for a financial institution to detect and report all potentially illicit transactions that flow through the organization. Examiners should focus on evaluating a credit union's policies, procedures, and processes to identify and research suspicious activity. However, as part of the examination process, examiners should review individual Suspicious Activity Report (SAR) filing decisions to determine the effectiveness of the suspicious activity monitoring and reporting process. Above all, examiners and credit unions should recognize the quality of SAR data is paramount to the effective implementation of the suspicious activity reporting system.

Credit unions are required by federal regulations to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount;
- Criminal violations aggregating $5,000 or more when a suspect can be identified;
- Criminal violations aggregating $25,000 or more regardless of a potential suspect; and
- Transactions conducted or attempted by, at, or through the credit union (or an affiliate) and aggregating $5,000 or more, if the credit union or affiliate knows, suspects, or has reason to suspect the transaction:

- May involve potential money laundering or other illegal activity (e.g., terrorism financing);
- Is designed to evade the BSA or its implementing regulations; or
- Has no business or apparent lawful purpose or is not the type of transaction the particular member would normally be expected to engage in, and the credit union knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit, a withdrawal, a transfer between accounts, an exchange of currency, an extension of credit, a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a bank or credit union.

Safe Harbor for Banks from Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides a credit union and its directors, officers, employees, and agents that make a disclosure to the appropriate authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.

Systems to Identify, Research, and Report Suspicious Activity

Policies, procedures, and processes should indicate the persons responsible for the identification, research, and reporting of suspicious activities. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The level of monitoring should be dictated by the credit union's assessment of risk, with particular emphasis on high risk products, services, members, entities, and geographic locations. Monitoring systems typically include employee identification or referrals, manual systems, automated systems, or any combination. The credit union should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities considering the credit union's overall risk profile and the volume of transactions.

Upon identification of unusual activity, additional research is typically conducted. Customer due diligence (CDD) information assists in evaluating if the unusual activity is considered suspicious. After thorough research and analysis, decisions to file or not to file a SAR should be documented. If applicable, reviewing and understanding suspicious activity monitoring across the organization's affiliates, business lines, and risk types (e.g., reputation, compliance, or transaction) may enhance a credit union's ability to detect suspicious activity and thus minimize the potential for financial losses, increased expenses, and reputation risk to the organization.

Identifying Underlying Crime

Credit unions are required to report suspicious activity that may involve money laundering, BSA violations, terrorist financing, and certain other crimes above prescribed dollar thresholds. However, credit unions are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft, and various types of fraud). **Investigation is the responsibility of law enforcement.** When evaluating suspicious activity and completing the SAR, credit unions should, to the best of their ability, identify the characteristics of the suspicious activity. Part III, Section 35, of the SAR provides 20 different characteristics of suspicious activity. Although an "Other" category is available, the use of this category should be limited to situations that cannot be broadly identified within the 20 characteristics provided.

Law Enforcement Inquiries and Requests

Credit unions should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects, identifying unusual or suspicious activity related to those subjects, and filing, as applicable, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSLs), and section 314(a) requests.

Mere receipt of any law enforcement inquiry, does not, by itself, require the filing of a SAR by the credit union. Nonetheless, a law enforcement inquiry may be relevant to a credit union's overall risk assessment of its members and accounts. For example, the receipt of a grand jury subpoena should cause a credit union to review account activity for the relevant member. It is incumbent upon a credit union to assess all of the information it knows about its member, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The credit union should determine whether a SAR should be filed based on all member information available. Due to the confidentiality of grand jury proceedings, if a credit union files a SAR after receiving a grand jury subpoena, law enforcement discourages credit unions and banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the credit union.

SAR Decision-Making Process

The credit union should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision to file a SAR is an inherently subjective judgment. <u>Examiners should focus on whether the credit union has an effective SAR decision-making process, not individual SAR decisions</u>. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the credit union has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the credit union should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.

Credit unions are encouraged to document SAR decisions. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR; however, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact each suspicious activity reporting decision will be based on unique facts and circumstances, no single, standard form of documentation is required when a credit union makes a decision not to file.

Timing of a SAR Filing

The SAR rules require a SAR be filed no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a member to determine whether to file a SAR. The need for a review of member activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect the activity or transactions under review meet one or more of the definitions of suspicious activity.

For situations involving violations requiring immediate attention, in addition to filing a timely SAR, a credit union is required to immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the credit union's regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the Internal Revenue Service Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a credit union of its obligation to file a SAR.

Notifying Board of Directors of SAR Filings

Credit unions are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and credit unions should have flexibility in structuring their format. Therefore, credit unions may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, credit unions may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the credit union, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties.

SAR Quality

Credit unions are required to file SAR forms that are complete, thorough, and timely. Credit unions should include all known suspect information on the SAR form. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR form, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the narrative section, as stated on the SAR form, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

By their nature, SAR narratives are subjective, and examiners generally should not criticize the credit union's interpretation of the facts. Nevertheless, credit unions should ensure SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR form (e.g., no attachments to the narrative section will be included within the BSA reporting database). More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist credit unions in writing, and assist examiners in evaluating, SAR narratives. In addition, comprehensive guidance is available from FinCEN ("Guidance on Preparing a Complete & Sufficient Suspicious Activity Report Narrative") at www.fincen.gov.

Prohibition of SAR Disclosure

No credit union, director, officer, employee, or agent of a credit union that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. Thus, any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose a SAR has been prepared or filed, citing 31 CFR 103.18(e) and 31 USC 5318(g)(2). FinCEN and the credit union's federal banking agency should be notified of any such request and of the credit union's response. Furthermore, FinCEN and the federal banking agencies take the position that credit unions' internal controls for the filing of SARs should minimize the risks of disclosure.

SAR Record Retention and Supporting Documentation

Credit unions must retain copies of SARs and supporting documentation for five years from the date of the report. Additionally, credit unions must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency. "Supporting documentation" refers to all documents or records that assisted a credit union in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or supervisory agency.

Additional Information on BSA

Examiners can find more detailed information on conducting BSA/AML examinations in the FFIEC BSA/AML Examination manual. The manual may be accessed via the FFIEC website at www.ffiec.gov.

Appendix 308B

Excerpts from the Federal Financial Institutions Examination Council's BSA/AML Examination Guide on OFAC Compliance

Office of Foreign Asset Control (OFAC)

OFAC is an office of the U.S. Treasury Department that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against entities such as targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

OFAC acts under Presidential wartime and national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and to freeze assets under U.S. jurisdiction. United Nations and other international mandates are the basis for many of the sanctions, therefore, they are multilateral in scope, and involve close cooperation with allied governments. Other sanctions are specific to the interests of the United States. OFAC has been delegated responsibility by the Secretary of the Treasury for developing, promulgating, and administering U.S. sanctions programs.

All U.S. persons, including U.S. banks, bank holding companies, non-bank subsidiaries and credit unions, must comply with OFAC's regulations. The federal banking agencies evaluate OFAC compliance systems to ensure all financial institutions subject to their supervision comply with the sanctions. Unlike the BSA, the laws and OFAC issued regulations apply not only to U.S. banks, their domestic branches, agencies, and international banking facilities, but also to their foreign branches, and often overseas offices and subsidiaries. In general, the regulations require the following:

- Block accounts and other property of specified countries, entities, and individuals.
- Prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals.

Blocked Transactions

U.S. law requires assets and accounts of an OFAC-specified country, entity, or individual be blocked when such property is located in the United States, is held by U.S. individuals or entities, or comes into the possession or control of U.S. individuals or entities. For example, if a funds transfer comes from offshore and is being routed through a U.S. financial institution to an offshore bank, and there is an OFAC-designated party on the transaction, it must be blocked. The definition of assets and property is broad and is defined within each sanction program. Assets and property includes anything of direct, indirect, present, future, or contingent value (including all types of banking transactions). Financial institutions must block transactions that:

- Are by or on behalf of a blocked individual or entity;
- Are to or go through a blocked entity; or
- Are in connection with a transaction in which a blocked individual or entity has an interest.

For example, if a U.S. financial institution receives instructions to make a funds transfer payment that falls into one of these categories, it must execute the payment order and place the funds into a blocked account. A payment order cannot be canceled or amended after it is received by a U.S. financial institution in the absence of an authorization from OFAC.

Prohibited Transactions

In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction (i.e., the transaction should not be accepted, but there is no OFAC requirement to block the assets). In these cases, the transaction is simply rejected, (i.e., not processed). For example, the Sudanese Sanctions Regulations prohibit transactions in support of commercial activities in Sudan. Therefore, a U.S. financial institution would have to reject a funds transfer between two companies, which are not Specially Designated Nationals or Blocked Persons (SDNs), involving an export to a company in Sudan that also is not an SDN. Because Sudanese Sanctions would only require blocking transactions with the Government of Sudan or SDNs, there would be no blockable interest in the funds between the two companies. However, because the transactions would constitute support of Sudanese commercial activity, which is prohibited, the U.S. institution cannot process the transaction and would simply reject the transaction.

It is important to note OFAC specifying prohibitions against certain countries, entities, and individuals is separate and distinct from the provision within the BSA's Customer Identification Program (CIP) regulation that requires financial institutions to compare new accounts against government lists of known or suspected terrorists or terrorist organizations within a reasonable period of time after the account is opened. OFAC lists have not been designated government lists for purposes of the CIP rule. However, OFAC's requirements stem from other statutes not limited to terrorism, and OFAC sanctions apply to transactions, in addition to account relationships.

OFAC Licenses

OFAC has the authority, through a licensing process, to permit certain transactions that would otherwise be prohibited under its regulations. OFAC can issue a license to engage in an otherwise prohibited transaction when it determines the transaction does not undermine the U.S. policy objectives of the particular sanctions program, or is otherwise justified by U.S. national security or foreign policy objectives. OFAC can also promulgate general licenses, which authorize categories of transactions, such as allowing reasonable service charges on blocked accounts, without the need for case-by-case authorization from OFAC. These licenses can be found in the regulations for each sanctions program (31 CFR, Chapter V (Regulations)) and may be accessed from OFAC's web site. Before processing transactions that may be covered under a general license, financial institutions should verify such transactions meet the relevant criteria of the general license.

Specific licenses are issued on a case-by-case basis. A specific license is a written document issued by OFAC authorizing a particular transaction or set of transactions. To receive a specific license, the person or entity who would like to undertake the transaction must submit an application to OFAC. If the transaction conforms with U.S. foreign policy under a particular program, the license will be issued. If a financial institution's customer or member claims to have a specific license, the institution should verify the transaction conforms to the terms of the license and obtain and retain a copy of the authorizing license.

OFAC Reporting

Financial institutions must report all blockings to OFAC within ten days of the occurrence and annually by September 30 concerning those assets blocked (as of June 30). Once assets or funds are blocked, they should be placed in a blocked account. Rejected, prohibited transactions must also be reported to OFAC within ten days of the occurrence.

Financial institutions must keep a full and accurate record of each rejected transaction for at least five years after the date of the transaction. For blocked property (including blocked transactions), records must be maintained for the period the property is blocked and for five years after the date the property is unblocked.

Additional information concerning OFAC regulations, such as Sanctions Program and Country Summaries brochures; the SDN list, including both entities and individuals; recent OFAC actions; and "Frequently Asked Questions," can be found on OFAC's web site.

OFAC Program

While not required by specific regulation, but as a matter of sound "banking" practice and in order to ensure compliance, credit unions should establish and maintain an effective, written OFAC program commensurate with their OFAC risk profile (based on products, services, customers, and geographic locations). The program should identify high-risk areas, provide for appropriate internal controls for screening and reporting, establish independent testing for compliance, designate an employee or employees as responsible for OFAC compliance, and create training programs for appropriate personnel in all relevant areas of the institution. A credit union's OFAC program should be commensurate with its respective OFAC risk profile.

OFAC Risk Assessment

A fundamental element of a sound OFAC program is the credit union's assessment of its specific product lines, customer base, and nature of transactions and identification of the high-risk areas for OFAC transactions. The initial identification of high-risk members for purposes of OFAC may be performed as part of the credit union's CIP and customer due diligence (CDD) procedures. As OFAC sanctions can reach into virtually all areas of its operations, credit unions should consider all types of transactions, products, and services when conducting their risk assessment and establishing appropriate policies, procedures, and processes. An effective risk assessment should be a composite of multiple factors, and depending upon the circumstances, certain factors may be weighed more heavily than others.

Another consideration for the risk assessment is account and transaction parties. New accounts should be compared with OFAC lists prior to being opened or shortly thereafter. However, the extent to which the credit union includes account parties other than accountholders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories, and powers of attorney) in the initial OFAC review during the account opening process, and during subsequent database reviews of existing accounts, will depend on the credit union's risk profile and available technology.

Based on the credit union's OFAC risk profile for each area and available technology, the credit union should establish policies, procedures, and processes for reviewing transactions and transaction parties (e.g., issuing bank, payee, endorser, or jurisdiction). Currently, OFAC provides guidance on transactions parties on checks. The guidance states if a financial institution knows or has reason to know a transaction party on a check is an OFAC target, the processing of the transaction would expose the financial institution to liability, especially personally handled transactions in a high-risk area. For example, if a financial institution knows or has a reason to know a check transaction involves an OFAC-prohibited party or country, OFAC would expect timely identification and appropriate action.

In evaluating the level of risk, a credit union should exercise judgment and take into account all indicators of risk. Although not an exhaustive list, examples of products, services, members, and geographic locations that may carry a higher level of OFAC risk include:

- International funds transfers;
- Nonresident alien accounts;
- Foreign member accounts;
- Cross-border automated clearing house (ACH) transactions;
- Commercial letters of credit;
- Transactional electronic banking;
- Foreign correspondent bank accounts;
- Payable through accounts;
- International private banking; and
- Overseas branches or subsidiaries.

In the absence of a credit union performed risk assessment, Appendix M ("Quantity of Risk — OFAC Procedures") in the FFIEC BSA/AML Examination Manual can be used to provide guidance to examiners on assessing OFAC risks facing a credit union. The risk assessment can be used to assist in determining the scope of the OFAC examination. A comprehensive risk assessment is likely to indicate the credit union has sufficient programs and controls in place, allowing the examiner to focus on higher risk areas versus a full program evaluation.

Once a credit union has identified its areas with high OFAC risk, it should develop appropriate policies, procedures, and processes to address the associated risks. Credit unions may tailor these policies, procedures, and processes to the specific nature of a business line or product. Furthermore, it is a sound business practice for a credit union to periodically reassess their OFAC risks. Especially if the credit union offers new products, services, or business lines, or is entering new geographic markets.

Internal Controls

An effective OFAC program should include internal controls for identifying suspect accounts and transactions and reporting to OFAC. Internal controls should include the following elements:

Identifying and reviewing suspect transactions. The credit union's policies, procedures, and processes should address how the credit union will identify and review transactions and accounts for possible OFAC violations, whether conducted manually, through interdiction software, or a combination of both. For screening purposes, the credit union should clearly define its criteria for comparing names provided on the OFAC list with the names in the credit union's files or on transactions and for identifying transactions or accounts involving sanctioned countries. The credit union's policies, procedures, and processes should also address how it will determine whether an initial OFAC hit is a valid match or a false hit. A high volume of false hits may indicate a need to review the credit union's interdiction program.

The screening criteria used by credit unions to identify name variations and misspellings should be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a high-risk area with a high volume of transactions, the credit union's interdiction software should be able to identify close name derivations for review. The SDN list attempts to provide name derivations; however, the list may not include all derivations. More sophisticated interdiction software may be able to catch variations of an SDN's name not included on the SDN list. Low-risk credit unions or areas and those with low volumes of transactions may decide to manually filter for OFAC compliance. Decisions to use interdiction software and the degree of sensitivity of that software should be based on a credit union's assessment of its risk and the volume of its transactions. The volume of transactions processed through corporate credit unions generally prohibits manually screening for OFAC matches; automated interdiction software is strongly recommended.

In determining the frequency of OFAC checks and the filtering criteria used (e.g., name derivations), credit unions should consider the likelihood of incurring a violation and available technology. In addition, credit unions should periodically reassess their OFAC filtering system. For example, if a credit union identifies a name derivation of an OFAC target, then OFAC suggests the credit union add the name to its filtering process.

New accounts should be compared with the OFAC lists prior to being opened or shortly thereafter (e.g., during nightly processing). Credit unions that perform OFAC checks after account opening should have procedures in place to prevent transactions, other than initial deposits, from occurring until the OFAC check is completed. Prohibited transactions conducted prior to completing an OFAC check may be subject to possible penalty action.

In addition, credit unions should have policies, procedures, and processes in place to check existing members when there are additions or changes to the OFAC list. The frequency of the review should be based on the credit union's OFAC risk. For example, credit unions with a low OFAC risk level may periodically (e.g., monthly or quarterly) compare the member base against the OFAC list. Transactions such as funds transfers, letters of credit, and non-member transactions should be checked against OFAC lists prior to being executed. When developing OFAC policies, procedures, and processes, the credit union should keep in mind OFAC considers the continued operation of an account or the processing of transactions post-designation, along with the adequacy of their OFAC compliance program, to be a factor in determining penalty actions. The credit union should maintain documentation of its OFAC checks on new accounts, existing members, and specific transactions.

If a credit union uses a third party, such as an agent or service provider, to perform OFAC checks on its behalf, as with any other responsibility performed by a third party, the credit union is ultimately responsible for that third party's compliance with the OFAC requirements. As a result, credit unions should establish adequate controls and review procedures for such relationships.

Updating OFAC lists. A credit union's OFAC program should include policies, procedures, and processes for timely updating of the lists of blocked countries, entities, and individuals and disseminating such information throughout the credit union's operations and branches. This would include ensuring that any manual updates of interdiction software are completed in a timely manner.

Screening ACH transactions. All parties to an ACH transaction are subject to the requirements of OFAC. OFAC has clarified the application of its rules for domestic and cross-border ACH transactions and is working with industry to provide more detailed guidance on cross-border ACH.

With respect to domestic ACH transactions, the Originating Depository Financial Institution (ODFI) is responsible for verifying the originator is not a blocked party and making a good faith effort to determine the originator is not transmitting blocked funds. The Receiving Depository Financial Institution (RDFI) similarly is responsible for verifying the receiver is not a blocked party. In this way, the ODFI and the RDFI are relying on each other for compliance with OFAC policies. ODFIs are not responsible for unbatching transactions and ensuring they do not process transactions in violation of OFAC's regulations if they receive those transactions already batched from their customers. If the ODFI unbatches the transactions it received from its customers, then the ODFI is responsible for screening as though it had done the initial batching.

With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions, however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States. In the case of inbound ACH transactions, the RDFI is responsible for compliance with OFAC requirements.

Additional information on all types of retail payment systems is available in the FFIEC *Information Technology Examination Handbook.*

Reporting. An OFAC program should also include policies, procedures, and processes for handling items that are valid blocked or rejected items under the various sanctions programs. In the case of interdictions related to narcotics trafficking or terrorism, credit unions should notify OFAC as soon as possible by phone or e-hotline about potential hits with a follow-up in writing within ten days. Most other items should be reported through usual channels within ten days of the occurrence. The policies, procedures, and processes should also address the management of blocked accounts. Credit unions are responsible for tracking the amount of blocked funds, the ownership of those funds, and interest paid on those funds. Total amounts blocked, including interest, must be reported to OFAC by September 30 of each year (information as of June 30). When a credit union acquires or merges with another credit union, both credit unions should take into consideration the need to review and maintain such records and information.

Credit unions no longer need to file Suspicious Activity Reports (SARs) based solely on blocked narcotics- or terrorism-related transactions, as long as the credit union files the required blocking report with OFAC. However, because blocking reports require only limited information, if the credit union is in possession of additional information not included on the blocking report filed with OFAC, a separate SAR should be filed with FinCEN including that information. In addition, the credit union should file a SAR if the transaction itself would be considered suspicious in the absence of a valid OFAC match.

Maintaining license information. OFAC recommends credit unions consider maintaining copies of members' OFAC licenses on file. This will allow the credit union to verify whether a member is initiating a legal transaction. Credit unions should also be aware of the expiration date on the license. If it is unclear whether a particular transaction is authorized by a license, the credit union should confirm with OFAC. Maintaining copies of licenses will also be useful if another financial institution in the payment chain requests verification of a license's validity. Copies of licenses should be maintained for five years, following the most recent transaction conducted in accordance with the license.

Independent Testing

Every credit union should conduct an independent test of its OFAC program that is performed by the internal audit department, outside auditors, consultants, or other qualified independent parties. For large credit unions, the frequency and area of the independent test should be based on the known or perceived risk of specific business areas. For smaller credit unions, the audit should be consistent with the credit union's OFAC risk profile or be based on a perceived risk. The person(s) responsible for testing should conduct an objective, comprehensive evaluation of OFAC policies, procedures, and processes. The audit scope should be comprehensive enough to assess OFAC compliance risks and evaluate the adequacy of the OFAC program.

Responsible Individual

It is recommended every credit union designate a qualified individual(s) to be responsible for the day-to-day compliance of the OFAC program, including the reporting of blocked or rejected transactions to OFAC and the oversight of blocked funds. This individual should have an appropriate level of knowledge about OFAC regulations commensurate with the credit union's OFAC risk profile.

Training

The credit union should provide adequate training for all applicable employees. The scope and frequency of the training should be consistent with the credit union's OFAC risk profile and appropriate to employee responsibilities.

Chapter 309

SUPERVISORY COMMITTEE/AUDIT FUNCTION

Introduction

Duties and Responsibilities

The Supervisory Committee (committee) is responsible for the annual audit, the verification of members' accounts, the internal audit function, and overseeing board of directors (board) or other issues which may impact the corporate credit union (corporate). Included in such issues is the monitoring of follow-up on open audit and examination findings until they are resolved.

Part 704 of the NCUA Rules and Regulations notes to the extent they are not inconsistent with Part 704, other regulations applicable to federally chartered or insured credit unions apply to corporates as well. Part 715 imposes a duty on committees to determine policies and control procedures are sufficient to safeguard against error, conflict of interest, self-dealing, and fraud. This means committee members must possess sufficient expertise in corporate operations to independently evaluate the adequacy of internal and external audit work in relation to the sophistication of the corporate's current and planned activities. The committee members should also possess the ability to determine if augmentation of industry standard internal and external audit scopes needs to take place, and whether supplemental audits should be performed in specific areas. Additionally, committee members must be bondable.

Part 704 Guidance Letter No. 2, issued August 12, 1997, imposes additional duties on corporate committees with expanded authority. Such committees must consider the need for and timing of an external risk management review function which will test the reliability of models and systems employed by management to determine the level of risk the corporate is taking. Factors to be considered include the current known level of risk being taken, the status of the corporate's models and systems relative to their state of the art, the levels of knowledge and technical expertise exhibited by staff, and recommendations of auditors and examiners.

Due to the complexity of corporate operations, it is not unusual for the committee to work closely with management in developing corporate's internal audit program and determining the necessity of third party risk management reviews. However, the committee must clearly demonstrate independence in decision-making in these areas, and in all other areas of committee responsibility. Documentation in support of such independence should be present in committee meeting minutes, written committee procedures for the auditor evaluation and selection processes, internal audit scope determinations, and other areas of committee responsibility where written standards and guidance are appropriate. If no such documentation exists, the corporate examiner (examiner) should recommend that it be developed and maintained. If there are any questions as to the committee's independence, this should be discussed with the Corporate Field Supervisor (CFS).

<u>CPA Opinion Audit Required</u>

Section 704.15 of the NCUA's Rules and Regulations requires corporates to obtain annual opinion audits from an independent, duly licensed certified public accountant (CPA). This audit must be performed in accordance with generally accepted auditing standards and the audited financial statements must be prepared consistent with generally accepted accounting principles (GAAP), except where law or regulation provides for departure from GAAP (e.g. classification of shares). The committee shall submit the audit report to the board. A copy of the audit must also be submitted to the OCCU Director within 30 calendar days after its receipt by the board. A summary of the audit report shall be submitted to the membership at the next annual meeting. The summary audit report is often incorporated in the corporate's annual report.

Upon OCCU's receipt, the annual audit report is generally sent to the district examiner for review. If the examiner in charge (EIC) is not the district examiner, he or she should review the audit report and management letter for items relevant to the examination. If a management letter is not issued, the corporate should obtain a letter from the CPA firm confirming conditions did not warrant issuance of a management letter.

Other industry standard audit-related correspondence should also be reviewed. Such correspondence includes the audit engagement letter, representation letters issued by corporate management and corporate counsel, as well as the CPA firm's independence letter. If these letters are missing, or if they contain language out of the ordinary, the reasons for this should be investigated.

Scheduling the Review of the Audit Work Papers

Part of the pre-examination process includes sending a pre-examination letter to the corporate. Scheduling review of the audit work papers is coordinated through this letter. Typically, the EIC will review the audit and verification work papers during the pre-examination week. Communicating the results of the audit work paper review to the committee chairperson is recommended.

Section 704.15(b) requires that, if requested, audit work papers are to be made available for NCUA's review. Despite this regulatory requirement, some auditing firms have requested that examiners sign a release statement before the firm will provide the documents to NCUA. Examiners are not required to honor, nor should they honor, this request. If the auditor continues to deny access to the work papers, the examiner should notify the CFS. The notification should include the name and address of the auditing firm, as well as the name of the applicable partner. The CFS will provide the information to the OCCU Director, who will send a letter to the auditing firm citing the regulatory requirement that work papers are to be made available for review.

If the auditing firm continues to deny access to the work papers, the corporate's committee chairman should be notified of the problem. It is the ultimate responsibility of the committee to ensure the corporate is in compliance with the audit requirements of the regulation.

Sarbanes-Oxley Act of 2002 (H.R. 3763)

This legislation was enacted in response to several corporate governance scandals, including Enron Corporation and Global Crossing Limited. While this Act's requirements apply only to public companies, examiners should encourage committee members to familiarize themselves with the Act's requirements, encouraging them to voluntarily adopt those provisions which are consistent with sound business practices.

Examples of such actions might include:

1. Requiring an inquiry as to whether the CPA firm being considered for the audit engagement has registered with the Public Company Accounting Oversight Board, and whether it has ever been sanctioned by this body;
2. Requiring audit partner rotation; and

3. Establishment of a confidential employee "whistleblower" and member complaint handling process.

NCUA Letter 03-FCU-07 provides a summary of those sections of the Act which may have relevance to corporate credit unions. Committee members are expected to be familiar with the contents of this letter.

Review of Annual Audit

The review of the annual audit is an important step in the examination process. The quality of the work and cited conclusions can be a factor in determining the scope of the examination. A comprehensive audit, qualified only with respect to the classification of member shares as equity, can give the examiner added basis for confidence in the accuracy and reliability of the corporate's records. This confidence can limit the extent or scope of selected reviews. Conversely, an inadequate audit may cause the examiner to expand the examination's scope.

An audit is the critical and systematic examination of the financial statements, records of accounting transactions, and internal controls of the institution. An acceptable audit is one satisfying the requirements of each particular engagement when judged by professional standards of performance.

It is not possible to define exact standards of acceptability for all corporate credit union audits. The examiner must use professional judgment to determine whether the audit fulfills all required elements. At a minimum, the audit report must meet the requirements of Part 715 of the NCUA Rules and Regulations, to the extent these are not inconsistent with corporate credit union requirements set forth in Section 704.15.

If the audit disclosed areas that indicate material operational or financial weaknesses, the external auditor should do more than merely certify the numbers. If the examiner concludes that the audit does not adequately address all concerns, the situation will first be discussed with the CFS prior to discussion with the committee and the board. Moreover, the examination report will contain appropriate verbiage to reflect the nature of these discussions.

Guidance on auditing standards that must be met can be found in the AICPA's *Audits of Credit Unions*. However, there may be cases in which minimum standards are not adequate to evaluate the specific services or circumstances in a particular corporate. Based on the risk exposure and other circumstances in each corporate, the examiner must judge if an audit fulfills the regulatory requirements.

An examiner should consider an audit unacceptable if:

1. Material parts of the audit were not performed;
2. Material parts of the audit cannot be supported by work papers; or
3. Material areas of the corporate's operations were not audited.

When an examiner takes exception to the annual audit, the following information should be provided to the corporate and documented in the examination work papers:

1. Specific audit sections in question;
2. Records or accounts with significant errors or record keeping deficiencies;
3. Material area(s) unreviewed; and
4. Time anticipated to resolve the problems.

If an examiner cannot determine if the CPA adequately completed certain audit steps, or questions the CPA's independence or competence, the concerns should be discussed with the CPA. During the meeting, the examiner should determine if and how the CPA used additional audit steps. At this time, however, the examiner should not make any statements as to the acceptability of the audit, if, in fact, it is deemed to be unacceptable.

Examiners must maintain their objectivity and independence. They should reserve adverse comments for the final meeting with the committee. The examiner should explain the audit deficiencies to the auditor and provide the auditor an opportunity to comment. If the auditor agrees, the parties involved should reach agreement concerning what and when corrections will be made. In all cases, examiners will discuss major audit findings with the committee and document them in their examination work papers.

If the examiner cannot come to an agreement with the CPA on the deficiencies, the CFS should be contacted. The examiner should not rate the audit as unacceptable. NCUA must afford the independent accountant "due process." For NCUA to prevail in a due process proceeding, OCCU staff must document that the CPA did not present financial statements consistent with GAAP, or that the CPA did not perform the audit scope, procedures, testing, and reporting consistent with GAAS.

When NCUA deems a CPA's work unacceptable, examiners have several options:

1. Recommend that the committee cause to be performed the additional necessary tests, within an appropriate timeframe before the next examination, to provide NCUA with needed assurance;
2. Recommend to the board and the committee they include additional special procedures in the engagement letter in future audits; or
3. Recommend the agency enforce appropriate FIRREA actions, as deemed necessary.

If the issue cannot be resolved with the corporate and the committee, the CFS should consult with the OCCU Director to determine how the concern should be advanced to the Office of Examination and Insurance (E&I) and the Office of General Counsel (OGC). If the examiner, CFS, and OCCU Director are in concurrence, the examiner should consider the CPA's work "pending further review" until judged to be either acceptable or unacceptable. Examiners will not require the corporate to have another CPA redo the work unless the OCCU Director directs such action.

To facilitate the submission to E&I and OGC, the examiner should provide the following:

1. A memorandum summarizing the deficiency or deficiencies, accompanied by documentation supporting the examiner's position. The memorandum should be clear, concise, and fully supported by documentation sufficient for the state licensing authority, the AICPA Ethics Division, or NCUA through an administrative proceeding process, to track the facts and successfully draw the same conclusion as the examiner;
2. A copy of the credit union's engagement letter, management representation letter, and any other relevant contracts or correspondence with the CPA firm;
3. A copy of the examination report;
4. A copy of the audit report;
5. A description of the examiner's review regarding the CPA's work, and the CPA's working papers in determining inadequacy;
6. Documentation regarding attempts to resolve the inadequacies with the CPA;

7. A listing of the examiner's findings and exceptions provided to the committee, and any notes, minutes, transcripts, or recordings of the meeting held with it to discuss same; and
8. Any additional information or documentation evidencing the examiner's position which would persuade a reasonable person in a due process proceeding.

The prepared package will be forwarded to E&I to review, assess the merit of the case, and possibly enhance NCUA's position by adding appropriate references or language from professional literature (GAAP and GAAS), if needed. In some cases, E&I has been successful in initiating renewed dialogue with the CPA, which brings about resolution of the issues. However, if E&I is unsuccessful, OCCU will forward the package to OGC which will consider the possible courses of action, which include:

1. Referral to the state licensing authority;
2. Referral to the AICPA Ethics Division;
3. Prohibition action (in rare cases), if OGC can prove the grounds set forth in Section 206(g) of the FCU Act in an administrative hearing;
4. Cease and desist order (in rare cases) against the CPA for violation of law or regulation, or for committing an unsafe or unsound practice;
5. A civil money penalty (in rare cases) against the CPA for violating law or regulation; and/or
6. Cease and desist or civil money penalty actions against the corporate or its officials for failure to obtain an "acceptable" audit.

OCCU and the central office staff must work together to advance the case through the legal system to seek the appropriate resolution. At all stages of this process, all parties must understand the importance of good communication and feedback. Examiners should feel comfortable pursuing such cases through the established channels, confident that, in documented cases with merit, OCCU and central office staff will endeavor to obtain an acceptable resolution.

Auditor's Review of Internal Controls

During the analysis of the auditor's work, the examiner will pay particular attention to the internal controls and operational procedures review. If the audit does not include a review of internal controls in major areas such as payment systems and/or investments, discussion with the supervisory committee will emphasize the need to obtain an internal control audit covering these crucial areas. Deficiencies will be addressed in the executive summary, as appropriate.

Status of Auditor's Exceptions/Recommendations

The Corporate Examination Procedures - Supervisory Committee Audit and Verification Review, OCCU 309.1P, and/or a suitable examiner designed work paper, will be used to list all exceptions/recommendations noted by the auditor in the audit report or management letter. A copy of these reports may be attached to OCCU 309.1P in place of the pertinent auditor comments. Steps taken by management to correct any of the noted exceptions and/or to implement auditor recommendations, as well as the current status of the corrections/recommendations, must also be documented.

Internal Audit

A corporate with average daily assets in excess of $400 million for the preceding calendar year, or as ordered by the OCCU Director, must employ or contract, on a full- or part-time basis, the services of an internal auditor (Section 704.15b). The internal auditor's responsibilities will, at a minimum, comply with the Standards and Professional Practices of Internal Auditing, as established by the Institute of Internal Auditors. The internal auditor will report directly to the chair of the committee, who may delegate administrative supervision of the internal auditor's daily activities to the corporate's CEO. The internal auditor's reports, findings, and recommendations will be in writing and will be presented to the committee not less than quarterly.

Although not required by Section 704.15, corporates with assets less than $400 million typically have internal audit functions. This is due to the risks posed by selected corporate operations (e.g., wires), regardless of asset size.

The committee and/or internal audit staff must develop an internal audit program which sets the frequency and scope of each internal audit. Examiners can provide input/guidance to the committee and the internal audit staff. However, such suggestions are usually limited to situations when there are deficiencies in internal audit scope (e.g., areas presenting material risk not being audited), internal audit procedures (e.g., lack of follow-up procedures), or the frequency of internal audits is inadequate. Internal audit scopes should be geared toward a targeted risk approach.

Part 704 of NCUA's Rules and Regulations makes peer review mandatory. The rule specifies the responsibilities of the internal auditor, whether an employee or a contractor, must comply with the Standards of the Institute of Internal Auditors. The Standards call for at least one mandatory external quality control review every five (5) years.

Examination Objectives

The objectives of the supervisory committee and audit function review are to:

1. Determine that all regulatory audit requirements are being met;
2. Evaluate the effectiveness of the committee through review of its audit implementation and oversight processes;
3. Evaluate the independence and competence of those who provide the internal and external audit functions, as well as the overall adequacy of the internal audit function;
4. Determine the procedures performed by the internal and external auditors are adequate to identify and to prompt the correction of deficiencies representing material risk;
5. Evaluate the adequacy of the annual opinion audit and verification of members' accounts, relative to the corporate's needs;
6. Determine that areas of concern noted during the external and/or internal audits are followed up by the committee or internal audit staff for corrective action; and
7. Initiate corrective action (issuance of DORs and/or OEFs) when deficiencies are identified with either the committee, the annual audit process, or the internal audit staff/processes.

Examination Procedures

See Corporate Examination Procedures - Supervisory Committee (OCCU 309P).

See Corporate Examination Procedures - Supervisory Committee Audit and Verification Review (OCCU 309.1P).

Examination Questionnaire

See Corporate Examination Questionnaire - Supervisory Committee (OCCU 309Q).

References

1. Federal Credit Union Act, Section 115, Supervisory Committee; powers and duties; suspension of members; passbook (12 CFR Section 1761d);
2. NCUA Rules and Regulations, Sections 704.15 (Audit Requirements) and 715 (Supervisory Committee Audits and Verifications);
3. AICPA Audit and Accounting guide, Audits of Credit Unions;
4. NCUA's Examiner's Guide, Chapter 5, Supervisory Committee; and
5. NCUA Letter No. 03-FCU-07, the Sarbanes-Oxley Act.

Chapter 310

BOND AND INSURANCE COVERAGE

Introduction

Obtaining insurance coverage for every insurable risk has been replaced by the risk management concept. Risk management, which includes insurance coverage, is intended to minimize the cost associated with assuming certain types of risk and providing prudent protection. It deals with pure risks that are characterized by chance occurrence and may only result in a financial loss.

Categories of Risk

Insurable risk can be separated into three major categories: property, liability, and personnel. First, the most commonly known property risk relates to loss of real property from natural events (such as flood, fire, or hurricane) or intentional causes (such as vandalism or arson). This category also includes the loss of any corporate credit union (corporate) asset, including currency, securities, electronic data, or records. Property risk also includes indirect expenses that result from property losses, such as relocating to temporary facilities or loss of business while replacing facilities. Secondly, liability risk includes suits resulting from injury or death of employees and the public, suits alleging official misconduct, and individual or class action suits alleging mistreatment or violations of law, regulation, or contractual obligations. All phases of the corporate's operations are susceptible to liability risk. Finally, personnel risk relates to the risks associated with the loss of key personnel. This risk is more pronounced in small and medium-size corporates that lack management succession plans.

Stages in Risk Management

There are three stages in risk management: risk identification and analysis, risk control, and risk treatment. Through its risk assessment process, each corporate should document its rationale and decision-making process for each of the three stages typically used for insurance risk management.

The importance of risk control is readily apparent when an uninsurable risk is involved. However, the significance of minimizing premium cost through risk controls cannot be overlooked. A corporate's primary defenses against loss are its policies, procedures, and internal controls. These systems and guidelines are integral parts of the risk and insurance management program. They must be communicated to and understood by all corporate personnel. Also, the corporate should provide audit coverage to ensure those controls are followed.

Once risks have been identified and risk controls implemented, management must decide the most appropriate method of treating a particular risk. A corporate has various options of treating a particular risk. It can implement additional controls to minimize that risk, yet still retain it. It may also transfer the risk to another party through insurance or contractual transfer, or a combination of these options. A basic concept of risk management is those risks that carry the potential for catastrophic or significant losses should not be retained.

Board Responsibility

Section 704.18 of the NCUA Rules and Regulation requires fidelity bond coverage to be obtained for all employees and officials in corporates. Also, the bond must provide coverage for the fraud and dishonesty of all employees, directors, officers, and committee members. Additionally, the bond may also provide coverage for lack of faithful performance, but coverage is not required by regulation.

The board of directors must determine and document the maximum loss a corporate is willing and able to assume. Additionally, Section 704.18(b) of the NCUA Rules and Regulations requires the board to (at least annually) carefully review the bond insurance coverage in force to determine its adequacy in relation to risk exposure and the minimum fidelity bond requirements disclosed in 704.18(d).

Fidelity Bond Insurance

Typically, fidelity bond insurance includes reimbursement for loss, not only from employee dishonesty, but also from robbery, burglary, theft, forgery, mysterious disappearance, and in specific instances, damage to offices or fixtures of the corporate. Fidelity bond coverage applies to all corporate locations. However, automated teller machines (which are not prevalent at corporates) are not covered, but can be specifically added under a rider.

It is the standard procedure for insurance companies to write fidelity bonds on a “discovery basis.” Under this method, the insurance company is liable up to the full amount of the policy for losses covered under the terms of the bond and discovered while the bond is in force, regardless of the date, which the loss was actually sustained by the corporate. This applies even though lower coverage amounts or more restrictive terms might be in effect on the date the loss was sustained.

All fidelity bonds require a loss be reported to the bonding company within a specified time after a reportable item comes to the attention of management. Therefore, management must diligently report all potential claims to the corporate’s insurance company. Failure to do so may jeopardize coverage for the loss.

Most corporates obtain excess coverage, as Section 704.18 (d)(2) of the NCUA Rules and Regulations states “it is the duty of the board of directors of each corporate to provide adequate protection to meet its unique circumstances by obtaining, when necessary, bond insurance coverage in excess of the minimum requirement.”

Other Types of Insurance

Corporates may also need other specialized forms of insurance for which the fidelity bond, along with the related policies, endorsements and specific coverage previously mentioned, provide insufficient protection. The following list depicts some of those coverages:

1. Automobile - public and property damage;
2. Extra expense;
3. Fire;
4. General liability;
5. Key person;
6. Umbrella liability;
7. Excess Electronic Crime Policy or E-commerce;
8. Valuable papers and destruction of records; and
9. Compliance.

Recordkeeping

The breadth of available insurance policies and differences in the coverages, emphasize the importance of maintaining a concise, easily referenced schedule of insurance coverage. These records should include, at a minimum the:

1. Coverage provided, detailing major exclusions;
2. Underwriter;
3. Deductible amounts;
4. Upper limits;
5. Term of the policy;
6. Date premium(s) are due; and
7. Premium amount.

Records of losses must also be maintained, regardless of whether or not the corporate was reimbursed. This information indicates areas where internal controls may need to be improved and is useful in measuring the level of risk exposure in a particular area.

Bidding Process for Insurance/Bonding

The bidding process for insurance/bonding coverage is the responsibility of the corporate's board. Insurance must be obtained from an NCUA approved carrier. The extent of an examiner's involvement will be to ensure the bidding process is completed in accordance with the board's polices regarding contracts. More detailed information on contracts is contained in Chapter 301, Management.

Examination Objectives

The objectives of the bond and insurance review are to:

1. Determine if the corporate's bond and insurance polices, procedures, practices, and internal controls are adequate to address risk, in relationship with capital. The procedures must, at a minimum, require annual review of the corporate's bond and insurance coverage in relationship to identified risks;

2. Determine the corporate's risk management process adequately identifies, controls, and address insurance risks;

3. Determine if bonding coverage meets the minimum coverage amounts in Section 704.18(d) of the NCUA Rules and Regulations;

4. Determine if the board of directors have established reasonable guidelines and mitigating controls for non-insured risk;

5. Determine if insurance coverage adequately protects against significant or catastrophic loss;

6. Determine if recordkeeping practices are sufficient to enable effective risk and insurance management;

7. Initiate corrective action when policies, practices, procedures or internal controls are deficient or when violations of law, regulations, and rulings are noted; and

8. Determine if potential losses are reported to bonding or insurance companies pursuant to policy provisions.

Examination Procedures

See Corporate Examination Procedures - Bond and Insurance Coverage (OCCU 310P).

Examination Questionnaire

See Corporate Examination Questionnaire (OCCU 310Q).

References

1. NCUA Rules and Regulations (Section 704.18); and

2. Comptroller's Handbook for National Bank Examiners - Risk Management and Insurance (Section 406).

Chapter 311

CORPORATE CREDIT UNION SERVICE ORGANIZATIONS

Introduction

A corporate credit union service organization (corporate CUSO) is an entity that:

1. Is at least partly owned by a corporate credit union;
2. Primarily serves credit unions;
3. Restricts services to those related to the normal course of business of credit unions; and
4. Is structured as a corporation, limited liability company, or limited liability partnership under state law.

Corporate CUSOs are proliferating, primarily because these entities a) offer their corporate owners the opportunity to generate significant fee and other revenues without a substantial balance sheet commitment, and b) permit corporate owners to offer selected services to their members which cannot be provided directly by corporates under current statute and regulation. It is not unusual for a corporate to have investments in and/or loans to a number of different corporate CUSOs.

Section 704.11 of NCUA's Rules and Regulations authorizes corporates to invest up to 15 percent of capital in member and non-member corporate CUSOs. The aggregate of all investments in and loans to member and non-member corporate CUSOs must not exceed 30 percent of capital. However, an additional 15 percent of capital can be loaned if the loans are collateralized by assets in which the corporate has perfected a security interest under state law. Note that while Section 704.7(e)(2) of NCUA’s Rules and Regulations states corporate CUSOs are not subject to Part 723, this statement is made relative to Part 723 loan limitations, which are superseded by Section 704.11 limits. Loans to corporate CUSOs are still subject to the due diligence requirements imposed on business loans by Section 704.11(c), which incorporate selected subsections of Part 723 by reference.

A corporate CUSO's organizational requirements (i.e., corporation, limited liability company, or limited liability partnership) are designed to limit the risk of loss to the affiliated corporate to the extent of the corporate's loan and/or investment balance. It should be noted, however, that the loss of a service provided by the corporate CUSO could affect the operations, financial condition, and reputation of affiliated corporates beyond the amounts loaned or invested.

Corporate CUSOs are chartered under state law and, therefore, must comply with all state laws, including state licensing and regulated activities' laws. Corporate CUSOs, being separate legal entities neither chartered nor insured by NCUA, are not subject to NCUA regulation. However, under the agreement terms required by Section 704.11(g)(4), NCUA does have the contractual right to "complete access to [corporate CUSO] books, records and any other pertinent documentation." For this reason, the term "corporate CUSO examination" is used throughout this chapter.

NCUA performs corporate CUSO examinations using a risk-based focus. Corporate CUSO examinations are performed in a consensual manner in cooperation with corporate CUSO management. State supervisory authorities (SSAs) may participate in corporate CUSO examinations, as determined by individual circumstances.

In instances when disputes arise between the examiner and a corporate CUSO over access to books and records or problem resolution, the examiner should look to the corporate field supervisor (CFS) and the OCCU office for guidance on resolution. It is important examiners take a professional, reasonable approach with corporate CUSO management and consult their CFS if they encounter circumstances that cannot be cooperatively resolved. Examiners should tailor review procedures according to the size, complexity, and risk activities of the corporate CUSO.

Section 704.11(f) prohibits any official of a corporate, which has an investment or loan to a corporate CUSO, from receiving, either directly or indirectly, any salary, commission, investment income, or other income, compensation, or consideration from the corporate CUSO. This prohibition also extends to immediate family members of officials.

Corporate CUSOs are formed to provide a wide variety of services to both corporates and natural person credit unions. Corporate CUSOs often provide investment and ALM advisory services, broker/dealer services, shared branching networks, operational services such as accounting, EDP, and human resources management services, as well as other services related to corporate and natural person credit union operations. In all cases, the examiner must not only determine the corporate's investment does not pose excessive credit risk, but also the services provided do not pose operational risk to the corporate(s) using the services of the corporate CUSO. Therefore, the examiner should always perform a limited financial and operational review of all corporate CUSO investments and/or loans on the books of a corporate during standard corporate examinations.

When evaluating a corporate's investment or loan to a corporate CUSO, the examiner should use a "two-tiered approach." The first tier evaluation will include a general corporate CUSO review as part of the overall examination scope. This review should determine, for each corporate CUSO the corporate has loaned to or invested in:

1. Compliance with Section 704.11 requirements. This includes a review of the corporate CUSO's current and proposed services to determine they are related to the normal course of credit union business.

2. Whether the corporate can legally be considered a separate entity relative to the corporate CUSO investment. Corporates are required by Section 704.11(d)(2) to obtain a written legal opinion concluding the corporate CUSO is organized and operated in a manner the corporate will not reasonably be held liable for the obligations of the corporate CUSO. These opinion letters can contain disclaimers limiting the circumstances under which the opinion is to be considered valid. The examiner must review the letter during each examination, to ensure current corporate CUSO operations conform to all the requirements and conditions imposed by the opinion letter. If this is determined not to be the case, a new opinion letter will be required which clearly establishes a corporate veil remains present, or operations will have to be modified to

conform with conditions imposed by the existing opinion letter. Additional discussion concerning this issue is provided below.

3. The overall financial condition and operating results of the corporate CUSO, and the extent of any financial risks the investment/loan may pose to the corporate. Corporate CUSOs are required to provide quarterly financial statements to corporates who have loaned to or invested in them. The examiner should determine these financial statements have been regularly received and are being reviewed by the corporate, and a credit analysis of all corporate CUSO loans and/or investments is performed at least annually. Newly formed corporate CUSOs may initially incur operating losses. The corporate CUSO's success in achieving budgeted performance goals during this start-up period should be considered during the evaluation of its of long-term financial prospects and the reasonableness of any corporate CUSO investment's carrying value. The corporate's financial records should accurately reflect any permanent impairments to corporate CUSO investments or to loans extended to corporate CUSOs. The corporate CUSO's annual audit should also be reviewed, to determine that any weaknesses disclosed therein are being adequately addressed.

4. The quality of any services the corporate CUSO may provide to the corporate being examined, and any operational risks that may be incurred by the corporate as a result of those services. Risks may include inadequate establishment of the rights and responsibilities of all parties involved with provision or use of the services, as well as risks posed by the manner in which services are being provided. For example, if the corporate has a website which advertises corporate CUSO services and links to the corporate CUSO, sufficient disclaimers should be in place to ensure members soliciting corporate CUSO services understand the service provider is a separate legal entity. Letter No. CU 2003-08 provides additional information on risks in this area.

Additional examination considerations present themselves when the corporate CUSO being reviewed is majority- or wholly-owned by the corporate being examined:

1. Majority- or wholly-owned corporate CUSOs are not required to obtain a separate annual audit if they are included in the corporate's annual consolidated audit. The corporate's consolidated annual audit will have to be reviewed to determine if comments relative to the corporate CUSO have been provided.

2. Corporates may elect to insure majority- or wholly-owned corporate CUSOs through existing corporate contracts, including bond contracts. These contracts have to be carefully reviewed to determine that the cost of coverage, dollar amount of coverage, and covered events for the corporate CUSO are clearly identified, that the corporate CUSO is the insured entity, and that coverage is sufficient given the nature and volume of the corporate CUSO's activities. The insurance contracts must also establish that, in the event claims relative to the corporate CUSO affect coverage available to the corporate, remaining corporate coverage will meet regulatory requirements. Corporate CUSO insurance coverage obtained through a corporate's insurance contracts could negatively impact the determination that a corporate veil is present, and should be discouraged if a number of other negative factors which could affect this determination are also present.

3. Majority- or wholly owned corporate CUSOs often share space and staff with their corporate owner. Comprehensive, reasonable, and accurate shared services agreements should be in place to ensure the corporate CUSO is being operated as a separate entity. Directors of such corporate CUSOs are often staff members or officials of their owner corporate. The examiner should determine separate meetings of the corporate CUSO board of directors take place, are documented by meeting minutes, and transactions involving both entities are "arm's length" as supported by written documentation.

If the "tier one" reviews discussed above disclose any material weaknesses (financial or operational) regarding the corporate CUSO, the examiner will recommend to the CFS a "tier two" review of the corporate CUSO operation. A tier two review will consist of an on-site corporate CUSO examination. The examination will be coordinated with the management of the corporate CUSO, and will be undertaken in order to gain a more comprehensive understanding as to the financial condition and quality of services provided by the corporate CUSO. The major objective of the examination will be to determine the degree of risk that the corporate CUSO poses to the NCUSIF and the investing corporate(s).

OCCU Instruction No. 15200 (REV), dated May 2, 2006 (CUSO Review Guidance), and attendant Appendices A through F currently provide guidance, checklists, procedures, reporting requirements, and review information concerning corporate CUSO examinations. Selected areas of that instruction are expanded upon below.

When performing an on-site review of the corporate CUSO's operations, the examiner may inquire about its managerial controls and working arrangements with leagues or trade associations, if applicable. The following are guidelines which may assist the examiner in the review of corporate CUSO operations and management:

1. Management - The examiner should arrange to review the corporate CUSO's policies, procedures, budgets, business plan, goals and objectives, reporting processes, articles of incorporation, and bylaws. The examiner should discuss with management the nature and extent of managerial planning, the overall reasonableness of the business plan, and budgetary projections.

2. Business Plan - Good business planning involves management's development of a written business plan before the organization begins doing business. A corporate CUSO's business plan, at a minimum, should include:

    a) A statement of goals (including profitability goals) and objectives;
    b) Policies, procedures, and time frames for achieving the goals and objectives;
    c) Budget projections demonstrating management's efforts to meet profitability and capitalization goals and achieve (and maintain) self-sufficiency; and
    d) Monitoring techniques to inform management of the operation's status.

Management should revise and update the business plan, as necessary, to ensure it is current. A corporate CUSO's well-developed and maintained business plan provides affiliated corporates and credit unions a valuable resource for making decisions about permissible investments and lending.

3. Managerial Personnel - An on-site corporate CUSO review provides the examiner an opportunity to observe and ascertain management's ability to effectively direct and control the corporate CUSO's operations. As part of the key personnel review, the examiner may find it helpful to request employee resumes and evaluations (i.e., depending upon state law, etc.) as well as note, in the work papers, key management background information. The adequacy of key personnel experience and education depends on the types and levels of service offered by the corporate CUSO. Observed managerial weaknesses should be noted in OCCU’s CUSO examination report.

4. Minutes - The examiner should review board minutes for content, decisions, and required frequency of meetings according to the corporate CUSO's bylaws. If available, the examiner may also request other minutes, including those of user/client meetings, special meetings, and executive committee meetings.

5. Investment/Loan Documents - The examiner should review investment and loan documents and corporate CUSO agreements of affiliated corporate and natural person credit unions.

Review of Corporate CUSO Services

The examiner should ensure the corporate CUSO is performing permissible services and is primarily serving credit unions or their members as required by regulation.

The corporate CUSO's quality of services provides information about the ongoing feasibility of the corporate CUSO. If available, membership surveys, complaint departments, and third party studies can assist the examiner in assessing the quality of services.

Review of Financial Performance

The examiner should evaluate the corporate CUSO's financial condition to determine its ability to meet its goals, objectives, and financial projections, analyze its prospects for future success, and assess the risk to affiliated corporate and natural person credit unions. Since financial trends for a start-up operation can be uncertain, it is important the examiner differentiate between start-up corporate CUSOs and those that have been in business for some time (e.g., cash flow projections, since start-up costs are expensed as they are incurred). Review of the following areas may assist examiners in performing the financial condition review:

1. Trend Analysis - The financial analysis of a corporate CUSO is similar to that performed during corporate examinations. However, some ratios used to evaluate corporate CUSOs may differ from those used for corporates. To better understand the corporate CUSO's trends and ratios, corporate examiners normally request at least three years' financial data. Comparative ratios (both over the prior three years and versus industry averages) assist the examiner in determining the reasonableness of the corporate CUSO's current financial condition. Both Dunn and Bradstreet and Robert Morris Associates publish industry averages.

2. Profitability - Due to tax consequences, corporate CUSO profitability objectives may differ from those of credit unions. However, corporate CUSOs still require sufficient cash flow to meet their objectives. The examiner should analyze earnings to ensure they are sufficient to pay for services offered, while achieving profitability and capital goals.

3. Cash Flow - Profitable corporations, including corporate CUSOs, do not always have positive cash flow. This is often true in the initial or start-up stages but can also be a result of mismanagement. Conversely, since corporate CUSOs hope to reduce taxes by minimizing net income without affecting cash flow, it is not uncommon for the CUSO to be unprofitable but have positive cash flow.

To analyze cash flow, the examiner may request cash flow statements. If the corporate CUSO does not prepare cash flow statements and cash flow appears to be a problem, the examiner should analyze the cash flow position to ensure the CUSO has sufficient cash flow to maintain normal operations. Depending on its severity, negative cash flow may require the examiner to expand the scope, review the situation with management, and develop (with corporate CUSO management) a plan to reverse the trend.

4. Taxes - As taxable entities, corporate CUSOs should adjust their projections for anticipated tax liabilities. During the review, the examiner may request a copy of the corporate CUSO's IRS filings (and documentation of other local, state, or municipal taxes for which the corporate CUSO is liable) for evaluation of proper payments and inclusion in the supporting work papers.

Review of Accounting and Audit Functions

The examiner should review the independent auditor’s report, notes to the audit report, engagement letter, report of reportable conditions (if these letters are available), and other correspondence before determining the scope of the general ledger review. If the CPA's competence and independence are not in question, the examiner may place greater reliance on the CPA's work.

The examiner may determine a comprehensive General Ledger review is not mandatory. In these instances, the examiner may limit the General Ledger review to those areas that may be of concern. For example, the examiner may choose to review only the corporate CUSO's tax filings and aging of receivable and payables, or only the appropriateness of classification of accounting information (e.g., expenses improperly capitalized or income improperly recognized). The examiner may want to pay particular attention to the collectibility of accounts receivable. If uncollectible receivables are material, NCUA may require affiliated corporate and natural person credit unions to reserve for their investments in and loans to the corporate CUSO.

When the examiner believes reviewing the actual audit work papers is necessary, permission should be obtained from the corporate CUSO to review the work papers and management should be requested to make necessary arrangements with the CPA firm. Review of audit work papers often provides meaningful information not evident from a review of the audit report (e.g., the CPA's assessment of the corporate CUSO's internal controls, or a statement regarding its viability as an ongoing concern).

The examiner should also confirm the corporate CUSO is following GAAP, as required by Section 704.11(g)(1).

Internal Control Assessment

The examiner's scope for an on-site corporate CUSO examination may include assessing the adequacy of internal controls necessary for the corporate CUSO's business. Likewise, if the corporate CUSO has an internal audit function, the examiner will arrange to review the internal audit scope and procedures.

Electronic Data Processing

During an on-site review, the examiner may arrange to review the corporate CUSO's information processing system, including related controls and the disaster recovery plan.

Legal Review

Section 704.11(d) requires a corporate investing in or lending to a corporate CUSO take reasonable steps to ensure a court would not "pierce the corporate veil" and hold it liable for the obligations of the corporate CUSO. This can happen when the assets of a corporation (the CUSO) are insufficient to satisfy its debts and there is a parent entity (the corporate) which is so closely identified with the corporation the judicial system requires holding the parent liable for those debts. Section 704.11(d)(2) requires a written attorney's opinion stating the corporate CUSO has been structured as a separate legal entity to limit the corporate's potential exposure to no more than the loss of funds invested in and/or loaned to the corporate CUSO. The legal opinion should address the factors specified in the cited regulation.

The examiner should review the following, evidencing a corporate veil has been established and has not been pierced:

1. Articles of incorporation or partnership agreement filed with the state;

2. Written bylaws;

3. Minutes of the first meeting of shareholders or partners or a unanimous consent of the shareholders or partners electing the board of directors;

4. Minutes of the director's first meeting or a unanimous consent of the directors electing officers and authorizing the issuance of the shares (if applicable) and adoption of the bylaws;

5. Review of stock certificates (if applicable);

6. Proof of capitalization and a determination that capitalization is minimally adequate to support the business plan; and

7. An opinion letter from an attorney, licensed to practice in the state where the corporate CUSO principally operates, stating that the corporate CUSO is structured in such a manner as to limit the liability of the corporate credit union to the investment in and/or loan to the corporate CUSO.

Affiliated corporates should obtain a new legal opinion if the corporate CUSO restructures its organization or if its current or planned operations raise potential liability issues.

There is usually no single controlling component the courts examine in determining whether to pierce the corporate veil thus imposing liability on the parent organization. The factors courts have considered include inadequate capitalization of the corporate CUSO, lack of separate and distinct CUSO identity, common boards of directors, management, or employees, corporate control of the corporate CUSO, the use of the same or similar forms by both entities, the lack of organizational meetings by the corporate CUSO, and lack of separate books and records.

To evidence distinction in identity, the corporate CUSO must demonstrate it operates separately from the corporate. The following questions and their response can aid the examiner in determining whether the corporate CUSO is operating as a separate entity with its own financial resources and necessary distinction in management and operations:

1. Is the corporate CUSO holding shareholder or partner meetings and board of director meetings regularly as required by the bylaws (it should be)?

2. Are payments made by the corporate CUSO to the corporate for rent, shared employee costs, etc., supported by appropriate management agreements, equipment leases, or real estate leases (i.e., office space, mailing addresses, and telephone numbers should be separate, etc.)?

3. Is the corporate providing guarantees to the corporate CUSO which could cause the corporate to incur liability in excess of the permitted investment limitation in the regulation?

4. Is there a good faith attempt to separate the identities of the corporate and corporate CUSO both in operation and management (i.e., corporate CUSO management should be separate from corporate management, red flags may include corporate management personnel holding a majority of corporate CUSO board positions)?

5. Is the capitalization of the corporate CUSO adequate in relation to its business plan?

Additionally, during on-site reviews, the examiner may arrange to review the corporate CUSO's compliance with all other applicable regulations, such as consumer regulations, state laws, and requirements imposed by other regulatory agencies (e.g., the SEC) as dictated by the nature of its business.

Finally, corporate CUSOs are encouraged to maintain appropriate levels of liability insurance and bonding. Management should periodically review coverage to ensure adequate protection. In reviewing the adequacy of bond coverage, examiners should use their professional judgment considering the CUSO's type (e.g., shared branching CUSOs would require similar coverage as credit unions), state law requirements, and insurance company recommendations.

Reserving

In the rare instance an examiner concludes the risk associated with a corporate CUSO's operation necessitates reserving by the affiliated corporates, the examiner will submit, with the concurrence of the CFS, a reserve recommendation with the report but in a separate memorandum to the OCCU Director. Examples of severe unresolved problems that may result in examiners recommending reserving include:

1. Material negative cash flow resulting in an inability to meet obligations;

2. Continual operating losses resulting in, or leading to, a deficit in retained earnings; and/or

3. Piercing of the corporate veil.

Reporting Format

Exceptions taken during the corporate CUSO examination will be communicated to corporate CUSO management as Other Examiner's Findings at an exit conference at the conclusion of the examination field work. Copies of these findings will be sent to the chairman of the board of the affiliated corporate(s).

The examiner will prepare a corporate CUSO examination report that will include, at a minimum, an executive summary as to the state of the corporate CUSO's financial and operational condition. The executive summary will outline strengths and weaknesses within the operation, and will clearly address any risks corporate CUSO operations may pose to the investing or lending corporate. The report may include a confidential section communicating any internal comments to the OCCU (central) office, as well as a summary as to the scope of the corporate CUSO examination. The report will be distributed to the CFS, the OCCU central office, affiliated corporates, state supervisory authorities of affiliated corporates, and to the subject CUSO (i.e., excluding the confidential section, as appropriate).

When the corporate CUSO poses significant risk to the corporate, the examiner will develop plans for action, review them with the CFS and OCCU Director (if necessary), and present them to corporate management. This may include, but is not limited to, reserving requirements. Since corporate CUSOs are not regulated institutions, NCUA does not have the authority to provide corporate CUSOs with a Document of Resolution. However, corrective action can be communicated to the corporate(s) having investments or loans to corporate CUSOs so they can minimize their risk of loss.

Examination Objectives

The examiner will address the following major examination objectives during the review of the corporate's investment in or loan to a corporate CUSO:

1. Determine the corporate is in compliance with the corporate CUSO investment and loan limitations as provided in 704.11(b);

2. Determine the corporate CUSO is structured in a manner consistent with 704.11(a)(4);

3. Determine the corporate CUSO is operated as a separate entity from the corporate. This will include a determination there exists an adequate "corporate veil" between the two entities;

4. Determine the services offered by the corporate CUSO are related to the normal course of business of credit unions;

5. Determine there are no conflicts of interest between an official of the corporate and the corporate CUSO pursuant to 704.11(f);

6. Determine the corporate CUSO has provided, and is in compliance with, the written agreement required by 704.11(g); and

7. Determine if circumstances warrant an independent corporate CUSO review.

Examination Procedures

See Corporate Examination Procedures - Credit Union Service Organizations (OCCU 311P).

Examination Questionnaire

See Corporate Examination Questionnaire - Credit Union Service Organizations (OCCU 311Q).

References

1. Section 704.11 of NCUA's Rules and Regulations

2. Chapter 25 of the NCUA Examiner's Guide, Corporate Credit Union Service Organizations

Chapter 401

CORPORATE RISK INFORMATION SYSTEM (CRIS)

Introduction

Corporate credit unions (corporates) are unique financial institutions. They are the only institutions, other than Federal Reserve and Federal Home Loan Banks, that exist primarily to provide financial, liquidity, and correspondent services to other financial institutions (e.g., credit unions).

The system used to detect, measure, and monitor these risks must be unique to the environment in which it will be used. Whereas the financial stability of corporates is crucial to their credit union members' success in providing services to their members, a regulatory risk rating system needs to be highly effective in identifying and measuring specific areas of risk during the supervisory process. By accurately detecting and communicating risk areas, NCUA can achieve the most effective supervisory efforts possible, and help avoid a major financial and operational crisis in the corporate credit union system (System).

NCUA's responsibilities to effectively detect, communicate, and control risk within the System, necessitates a highly specialized and effective risk rating system.

NCUA considers management's role in corporates to be the major catalyst in the financial and operational success of the institutions. In order to benefit NCUA, a corporate risk rating system must effectively evaluate, measure, and report the qualitative strengths and weaknesses of management personnel, practices, and policies. This system operates independent of the quantitative risk measures such as empirical levels of capital, earnings, and net economic value.

CRIS separates the assessment and communication of quantitative financial risks from qualitative operational and managerial risks and assigns individual Financial Risk and Risk Management Composite and Component Ratings, respectively.

The Financial Risk Composite Rating is:

> An assessment of measurable risk exposure to the corporate's capital, relative to levels of exposure to credit, interest rate, and liquidity risk as of the date of the examination.

The Risk Management Composite Rating is:

> A qualitative risk assessment derived from the examiner's evaluation of management's policies, practices, and expertise in identifying, measuring, monitoring, reporting, and controlling risk.

Used in conjunction, the components allow NCUA to more effectively focus resources in specific areas of risk identified during the supervisory process, and develop and implement appropriate supervision strategies.

The CRIS rating system's examination and supervision objectives are:

1. To detect, evaluate, and measure financial and operational risks;
2. To determine the effect these risks may have upon the financial (capital) strength of the institutions;
3. To assess the quality of management, policies, and procedures;
4. To assess and control risk to the National Credit Union Share Insurance Fund (NCUSIF); and
5. To provide a rating system, internal to NCUA, that will be used to allocate agency resources for ongoing examination and supervision needs of corporates.

CRIS System

CRIS provides individual composite ratings for both Financial Risk and Risk Management, based upon certain components as follows:

1. The Financial Risk Composite rating is derived by the measurement and interrelationship of five quantitative components: Empirical Capital Level; Earnings; Interest Rate Risk Exposure; Liquidity Risk Exposure; and Credit Risk Exposure; and
2. The Risk Management Composite rating is similarly derived through the evaluation of seven components stressing the qualitative nature of risk management. These are: Capital Accumulation Planning; Profit Planning and Control; Interest Rate Risk Management; Liquidity Risk Management; Credit Risk Management; Operations Risks; and Board Oversight, Audit & Compliance.

Disclosure of CRIS to Corporates

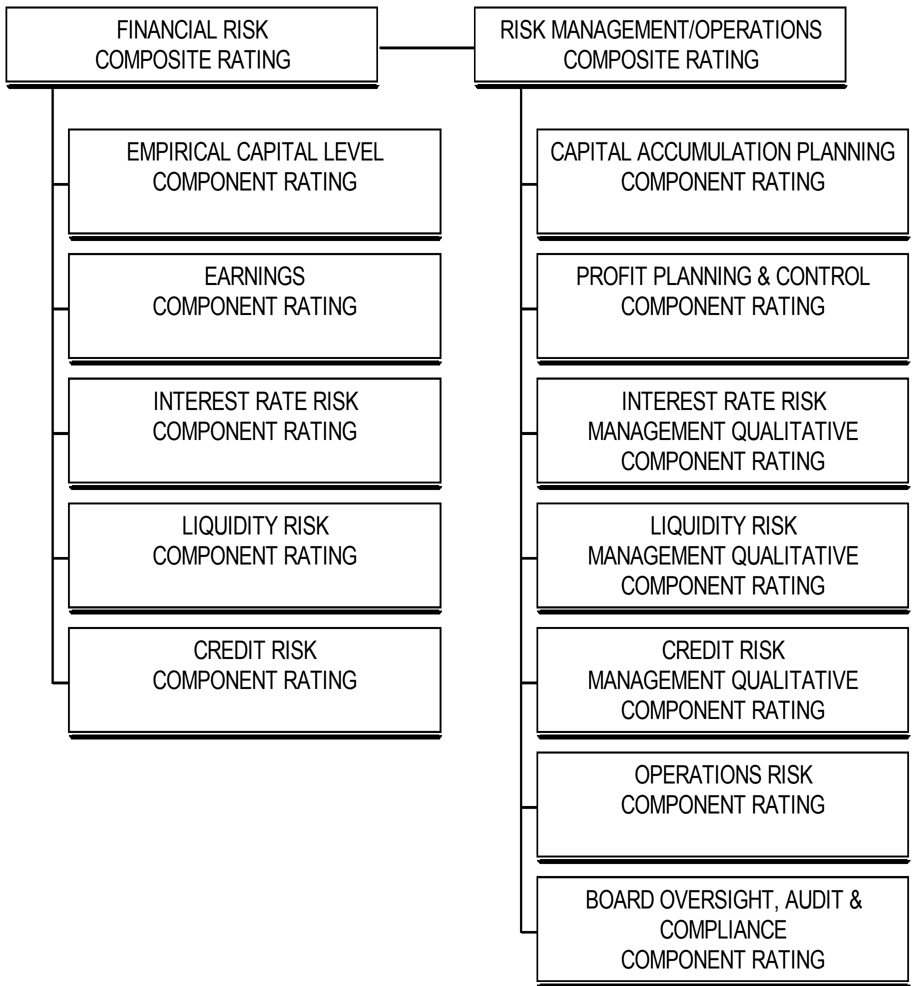
The major emphasis of the examination report will focus on the individual areas of concern identified during the examination and implementing corrective action. However, both the Financial Risk and Risk Management composite and component ratings will be disclosed in the Executive Summary section of the examination report. To eliminate the problem of officials focusing on the ratings as opposed to the issues, the ratings will not be disclosed until after the issues are discussed with a corporate's board during the joint conference.

Coordinating the disclosure of CRIS with State Supervisory Authorities (SSA)

Each SSA has specific procedures for the disclosure of their risk rating systems to state chartered corporates. Examiners should coordinate their efforts with the SSA to ensure the intent of the agreements reached in the Document of Cooperation and individual agreements with SSAs, as well as the conditions in Chapter 104 of this guide, are met.

The diagram on the next page provides a practical depiction of the CRIS rating system.

CORPORATE RISK INFORMATION SYSTEM (CRIS)



Interrelationship of CRIS Composites, Components and Evaluation Factors

Under CRIS the corporate will be assigned a Financial Risk and a Risk Management composite rating. The composite ratings are derived through the interrelationship between underlying component ratings. The component ratings are derived through the examination of relevant Evaluation Factors. Examiners will rate the components and composites 1 through 5; 1 being the best and 5 the worst. The risk rankings assigned to the Evaluation Factors will be used to determine the overall component ratings to which they relate. Definitions of component and composite ratings are defined in detail in Appendix 401A, CRIS Composite and Component Rating Definitions and

Evaluation Factors. Assignment of separate Financial Risk and Risk Management Composite Ratings provides a more effective manner of identifying immediate and potential risks to a corporate's financial strength. By providing separate ratings for quantitative (financial risk) and qualitative (risk management abilities) factors, an accurate and effective risk assessment of the corporate can be made.

Evaluation Factors

Evaluation Factors are reviewed as part of the overall examination process by the examination team. Each Evaluation Factor must be assessed by the examiner as it applies to both the corporate's scope of business and any Part 704 Expanded Authorities (if applicable). Evaluation Factors are assigned specific risk rankings based upon the examiner's review and professional judgment. Generally, the risk ranking assigned to each Evaluation Factor should be independent of others. If applicable, certain Evaluation Factors may be given more weight in determining the overall composite. Examiners should use professional judgment when determining whether to place more emphasis on one Evaluation Factor over another when deriving an overall component rating. Each Evaluation Factor is assigned a risk ranking as noted in the tables below:

Financial Risk Component	
Risk Ranking	**Degree of Risk to Capital and/or Earnings**
1	Low Risk
2	Moderate (managed) Risk
3	High Risk
4	Excessive Risk
5	Critical Risk
Risk Management Component	
Risk Ranking	**Quality of Policy or Risk Management Process**
1	Exceptional
2	Acceptable
3	Minimally Acceptable
4	Inadequate
5	Seriously Deficient

The risk rankings assigned to the Evaluation Factors must be derived based on professional judgment of the operating principles and standards in this Corporate Examiner's Guide, the Guidelines for Submission of Requests for Expanded Authority, and other industry accepted standards. The Financial Risk and Risk Management components will be derived as a result of the interrelation of the risk rankings assigned to the individual Evaluation Factors.

Composite and Component Ratings

Financial Risk Composite Rating

The Financial Risk Composite Rating is derived, by not only assessing the corporate's empirical level of capital and earnings, but also determining credit, interest rate, and liquidity risk exposures, and the effects these risks could have on the earnings and capital levels. Individual component ratings are assigned to these areas when developing the overall composite rating.

The examiner must keep in mind that the Financial Risk Composite Rating is a quantitative assessment of relative capital strength in relation to earnings performance and financial risks. The Financial Risk Composite Rating is not an arithmetic average of the individual components. The component ratings should be evaluated independently using the guidelines in Appendix 401A and the examiner's judgment to derive and assign the overall Financial Risk Composite Rating. The component ratings are similarly derived through an assessment of the individual Evaluation Factors reviewed as part of the examination scope. Guidelines for examiner assessment of the individual Financial Risk components are provided in specific sections of this chapter, and throughout the Corporate Examiner's Guide. A list of Evaluation Factors is listed in Appendix 401A, along with definitions of the Financial Risk Component and Composite Ratings.

Risk Management Composite Rating

The ability of management to develop appropriate business plans, operational policies and procedures, and risk management policies and practices is crucial to ensure the ongoing financial soundness of each corporate. CRIS acknowledges the importance of management's capabilities by providing a separate and distinct composite rating in assessing the abilities and effectiveness of corporate management. The Risk Management Composite Rating should reflect the examiner's assessment of the qualitative factors attributable to the management of financial risk and those inherent within corporate operations (i.e., processes and results that cannot be measured on a numerical basis). The Risk Management Composite Rating will be derived through the assessment of the seven individual Risk Management Component Ratings, as follows:

1. Capital accumulation planning;
2. Profit planning and control;
3. Interest rate risk management;
4. Liquidity risk management;
5. Credit risk management;
6. Operations; and
7. Board oversight, audit & compliance.

The Risk Management Composite Rating is determined as a result of the examiner's review of the corporate's operational processes, policy making and planning capabilities, and risk management and reporting process. The Risk Management Composite Rating is not measured on financial results. This Composite Rating will be assigned as a result of the examiner's review of each component's Evaluation Factors as they relate to the corporate's scope of operation and Expanded Authorities (if applicable).

Assignment of Composite Ratings

The examiner will follow the composite rating definitions outlined in Appendix 401A to assign both the Financial Risk and Risk Management Composite Ratings. OCCU Form 102I will be used to facilitate this process. On OCCU 102I, the examiner in charge (EIC) will assign ratings using team member recommendations; however, the EIC makes the final CRIS rating decisions.

Examiners have the latitude to increase or decrease any component or composite rating based on individual circumstances and/or professional judgment; however, rationale supporting increases and/or decreases should be documented in the confidential section of the examination report. OCCU 102I will be included with the field and office copies of the examination report. The work papers will provide support for the component and composite ratings by listing the risk rankings assigned to the individual Evaluation Factors.

Empirical Capital Level & Capital Accumulation

Since the revision of Part 704 in 1998, corporates have increased retained earnings, some more successfully than others. When reviewing capital, the examiner should specifically address retained earnings trends and ratios in relation to financial and operational risks.

Meeting minimum capital requirements is a key factor in determining capital adequacy. More importantly, the examiner must consider whether the corporate's operations and risk position requires capital above the minimum regulatory threshold. For example, the examiner should consider whether the corporate will continue to maintain adequate capital levels in light of current and planned activities, such as Expanded Authorities.

Corporates operating at Base or Base-Plus Expanded Authority must maintain a minimum capital ratio of 4 percent. However, a corporate with Part I or II Expanded Authority will need a minimum 4, 5, or 6 percent capital ratio depending on their corresponding NEV exposure limit of 20, 28, or 35 percent, respectively. The examiner must keep in mind these ratios are merely the minimum regulatory requirement; given additional risks in each corporate, these ratios may be minimally adequate or even inadequate.

As part of the risk rating process the examiner will assign a Financial Risk Component Rating to Empirical Capital Strength and a Risk Management Component Rating to Capital Accumulation Planning. The capital versus risk relationship will be reflected in the Overall Financial Risk Composite Rating when the Empirical Capital Level Component Rating is evaluated in relation to the other risk related components (i.e., interest rate, liquidity, credit, earnings risks).

<u>Empirical Capital Level</u>

In assigning this component rating, the examiner should consider all capital related Evaluation Factors and any additional issues directly or indirectly affecting capital. At a minimum, the following Evaluation Factors should be considered:

Retained Earnings Ratio:

Retained earnings and the retained earnings ratio are defined in Section 704.2 of the corporate rule. When assigning a risk ranking to this factor, the examiner should consider the corporate's overall level of financial and operational risks, including any Expanded Authorities. Generally, a corporate taking on higher degrees of credit, interest rate, liquidity, and operational risk should maintain a higher level of retained earnings, as noted in the table below:

Recommended Risk Rankings for Retained Earnings Evaluation Factor			
Risk Ranking	**Base, Base+**	**Part I**	**Part II**
1	5.0% or greater	5.5% or greater	6.0% or greater
2	3.0 to less than 5.0%	3.5% to less than 5.5%	4.0% to less than 6.0%
3	2.0% to less than 3.0%	2.5% to less than 3.5%	3.0% to less than 4.0%
4	1.0% to less than 2.0%	1.5% to less than 2.5	2.0% to less than 3.0%
5	less than 1.0%	less than 1.5%	less than 2.0%
Note: Part III corporates are evaluated using the column corresponding with their Part I or Part II authority and NEV threshold. Part IV and V corporates are evaluated under the Base and Base+ column unless they have an expanded authority level requiring use of another column. Wholesale corporates are evaluated under the column for Part I authority.			

Core Capital Ratio: When assigning the ranking for the core capital ratio (as defined in Section 704.2), the examiner will take into account the corporate's earnings retention position, and the trend and mix of capital.

Capital Ratio: Section 704.3 and Appendix B to Part 704 set forth specific capital ratio requirements for Base and each level of Expanded Authorities. As noted in Appendix B, the minimum capital ratio is also established as a result of the designated NEV exposure limit chosen by corporates with Part I or II Expanded Authorities. The examiner should consider the corporate's current capital level, and ability to achieve future capital goals when assigning the rating for this Evaluation Factor. The table below establishes the recommended risk rankings based on each corporate's Expanded Authorities or operating level:

Recommended Risk Rankings for Capital Ratio Evaluation Factor							
Risk Ranking	**Base & Base+**	**Part I 20% NEV**	**Part II 20% NEV**	**Part I 28% NEV**	**Part II 28% NEV**	**Part I 35% NEV**	**Part II 35% NEV**
1	6.0% or greater	6.50% or greater	7.00% or greater	7.00% or greater	7.50% or greater	7.50% or greater	8.00% or greater
2	5.0% or less than 6.0%	5.50% or less than 6.50%	6.00% to less than 7.00%	6.00% to less than 7.00%	6.50% or less than 7.50%	6.50% or less than 7.50%	7.00% or less than 8.00%
3	4.0% or less than 5.0%	4.50% or less than 5.50%	5.00% or less than 6.00%	5.00% or less than 6.00%	5.50% or less than 6.50%	5.50% or less than 6.50%	6.00% or less than 7.00%
4	3.0% or less than 4.0%	3.50% or less than 4.50%	4.00% or less than 5.00%	4.00% or less than 5.00%	4.50% or less than 5.50%	4.50% or less than 5.50%	5.00% or less than 6.00%
5	Less than 3.0%	Less than 3.50%	Less than 4.00%	Less than 4.00%	Less than 4.50%	Less than 4.50%	Less than 5.00%
Note: Part III corporates are evaluated using the column corresponding with their Part I or Part II authority and NEV threshold. Part IV and V corporates are evaluated under the Base and Base+ column unless they have an expanded authority level requiring use of another column. Wholesale corporates are evaluated under the column for Part I authority.							

Capital Trends: When determining the Empirical Capital Component Rating, the EIC must consider the capital level, mix, and trends as of the effective date of the examination. The EIC should also consider the risk rankings assigned to the above Evaluation Factors. The overall Financial Risk Composite Rating will reflect the relationship between Empirical Capital Strength and balance sheet and operational risk levels.

Capital Accumulation Planning Component Rating

As part of the examination process, the examiner will evaluate and assess the strength of the corporate's capital accumulation plan, and the effectiveness with which it is implemented. The capital accumulation plan should be developed after careful consideration of current and projected balance sheet and operational risk activities (i.e., Expanded Authorities, new services, etc.).

Capital accumulation plans will be evaluated and assigned a component rating that will be included in the derivation of the overall Risk Management Composite Rating. The evaluation of capital accumulation plans will require the examiner draw upon a variety of other financial and risk related factors impacting the corporate. Chapter 204 of this guide provides discussion of some of the attributes of effective capital accumulation planning.

Earnings and Profit Planning Component

A corporate should have earnings sufficient to accumulate capital levels to meet or exceed minimum capital requirements and absorb operating losses. The minimum capital requirements will vary in relation to Expanded Authorities, as well as the corporate's overall balance sheet and operational risk profile. Examiners should use professional judgment to evaluate the adequacy of earnings in relation to the level of capital and the risks inherent in the portfolio, and any off-balance sheet risks. For example, a corporate with Parts II and IV Expanded Authorities will be evaluated more stringently than one with Base-Plus Expanded Authority because it has the authority to expose its capital and earnings to greater risk.

When examiners assess the adequacy of corporate earnings, general economic and market related factors should be considered. Earnings trends and balance sheet flexibility are two factors that should be considered, in addition to actual financial results.

Given the complexity of each corporate's balance sheet, there is no easy formula for determining the adequacy of earnings. The examiner should look for earnings characteristics such as stability, trend, and composition. The level of operating expenses should be reviewed in relation to the overall earnings composition. The examiner should be cognizant of the risk/return tradeoff or concept often employed as part of corporate asset/liability management strategies. Generally, assets carrying additional risk should provide an adequate compensating return used to build capital, or to provide the membership with greater return.

Although the minimum capital requirements are specifically set forth in Section 704.3, and Appendix B to Part 704, the adequacy of earnings is subjective based on qualitative and quantitative factors as well as the examiner's professional judgment. These qualitative and quantitative measures may relate to, but are not limited to, the current capital level, the level of credit, interest rate, liquidity, and operational risk, and management's effectiveness. Further guidance for evaluating earnings is discussed in Chapter 302 of this guide.

When evaluating the adequacy of earnings, the examiner should consider the following factors:

<u>Quantitative Earnings Evaluation Factors (Financial Risk Composite)</u>

1. Net Income Level;
2. Earnings Trends;
3. Earnings Composition (gross income, cost of funds, fee income);
4. Operating Expenses;
5. Product Line Profitability; and
6. Non-Operating Income Level.

<u>Qualitative Earnings Evaluation Factors (Risk Management Composite)</u>

1. Budgeting and Reporting;
2. Earnings in Relation to Capital Planning;
3. Effectiveness of Cost Accounting Systems; and
4. Pricing Strategies and Policies.

Sensitivity to Interest Rate Risk

Interest rate risk (IRR) is the exposure of capital and earnings to movements in interest rates. The economic perspective, termed net economic value (NEV), focuses on the difference in the fair value of assets and the fair value of liabilities in today's interest rate environment and the sensitivity of NEV to interest rate changes. The accounting perspective, referred to as net interest income (NII), focuses on the effect of interest rate changes on the corporate's projected earnings under both current and projected interest rate scenarios.

The IRR Component Rating addresses the corporate's performance in identifying, measuring, monitoring, reporting, and controlling exposure to interest rate changes. The examiner will assess quantitative and qualitative factors in order to assign an Interest Rate Risk Exposure Component Rating and an Interest Rate Risk Management Component Rating, respectively.

Given the importance of each corporate's IRR management process, qualitative factors such as the robustness of the model and validity of the assumptions will be utilized in assigning both the quantitative and qualitative components.

In deriving the IRR Component Rating, the examiner is to consider 12 Evaluation Factors listed in this section. The examiner should determine whether rankings for additional factors are to be documented under the "other" caption. The component rating should be assigned on a case-by-case basis using professional judgment, and consider the interrelationships of the Evaluation Factors in light of any Expanded Authorities.

The Sensitivity/IRR Evaluation Factors focus the examiner on the sensitivity measures, documentation, and testing the corporate performs, rather than on management's capabilities. The examiner's evaluation of management's effectiveness and expertise should be considered when assigning the IRR Management Component Rating under the overall Risk Management Composite.

Considering the interrelationships of the various Evaluation Factors, the examiner may assign a lower or higher ranking than is specified in the guidelines; however, the rationale or justification for such decisions should be well-documented in the examination work papers. The examiner should refer to Appendix 401A when assessing these Evaluation Factors.

Qualitative IRR Exposure Evaluation Factors

Base case NEV ratio: Under Section 704.8, a corporate must calculate its NEV ratio at least quarterly; the NEV ratio must be calculated monthly, if the NEV ratio falls below 3 percent at the last testing date. In general, corporates with Expanded Authorities must compute their NEV ratio monthly; however, the specific requirements are detailed in Appendix B to Part 704.

Section 704.8 establishes a minimum NEV ratio floor of 2 percent under the worst-case test for parallel shocks in the Treasury yield curve. Therefore, a 2 percent base case NEV ratio represents a weak capital position and an excessive risk level limiting the corporate's flexibility to respond to interest rate shocks and comply with the Section 704.8(d)(1)(ii) NEV Exposure Measure. Corporates in this situation have a very small margin for error with their NEV modeling process and even a slight increase in IRR jeopardizes their compliance with the 2 percent NEV ratio floor.

Examiners should compare each corporate's base NEV ratio, NEV Exposure Measure, and NEV Volatility Measure to the following tables to assist them in determining the overall IRR Component Rating:

BASE NEV RATIO			
Ranking	**Base, Base +**	**Part I**	**Part II**
1	6.0% or greater	6.5% or greater	7.0% or greater
2	5.0% to 5.99%	5.5% to 6.49%	6.0% to 6.99%
3	4.0% to 4.99%	4.5% to 5.49%	5.0% to 5.99%
4	3.0% to 3.99%	3.5% to 4.49%	4.0% to 4.99%
5	Less than 3.0%	Less than 3.49%	Less than 3.99%

NEV Exposure Measure (worst case NEV ratio): Section 704.8(d)(1)(ii) provides that a corporate must limit its risk exposure to a level that does not result in an NEV ratio below 2 percent under parallel shocks in the yield curve of plus/minus 300 basis points. Generally, a low risk corporate would maintain an NEV Exposure Measure above 3 percent, as noted below.

NEV EXPOSURE MEASURE	
Ranking	**All Authorities**
1	5.0% or greater
2	4.0% to 4.99%
3	3.0% to 3.99%
4	2.0% to 2.99%
5	Less than 2.0%

NEV Volatility Measure (post shock percentage change in NEV ratio): The corporate must limit its IRR exposure under parallel shocks in the yield curve across a range of plus/minus 300 basis points to a level that does not result in an NEV Volatility Measure of more than 15, (Base), 20 (Base+), 20, 28, or 35 for corporates having Part I and/or II Expanded Authority. Refer to the tables below.

NEV VOLATILITY MEASURE		
Ranking	**15% NEV Limit**	**20% NEV Limit**
1	less than 6.0%	less than 9.0%
2	6.0% to less than 9.99%	9.0% to 14.99%
3	10.0% to 14.99%	15.0% to 19.99%
4	15.0% to 19.99%	20.0% to 27.99%
5	20.0% or greater	28.0% or greater

NEV VOLATILITY MEASURE		
Ranking	**28% NEV Limit**	**35% NEV Limit**
1	less than 12.0%	less than 15.0%
2	12.0% to 19.99%	15.0% to 24.99%
3	20.0% to 27.99%	25.0% to 34.99%
4	28.0% to 34.99%	35.0% to 39.99%
5	35.0% or greater	40.0% or greater

Qualitative IRR Management Evaluation Factors

Risk Model Capabilities: This Evaluation Factor reflects the examiner's conclusions regarding the capabilities of the NEV model as implemented by management or a third-party vendor (i.e., if NEV modeling is outsourced). The examiner should refer to Chapter 202, Asset/Liability Management, and to corporate staff for documentation of the fundamental characteristics of the risk model. The examiner should document any overrides of industry standard inputs indigenous to NEV modeling.

Modeling Assumptions: This Evaluation Factor considers whether the price sensitivities are reasonable and supportable in light of any prepayment speed assumptions. The examiner will consider the source (such as information vendor or in-house systems) of prepayment estimates used to measure and monitor the price sensitivity of complex investments. If the model generates securities valuation output at the individual instrument level, such detail may serve as appropriate evidence of securities price sensitivity monitoring.

Additional NEV and Stress Testing

The examiner should assess the frequency, accuracy, and validity of the additional tests periodically required by Section 704.8(d)(2). This assessment should include determining whether management should go above and beyond the regulatory requirements, based on balance sheet risk, or external factors (i.e., interest rate environments, economic conditions, event risk, etc.). For example, performing rate shocks of 400 or 500 basis points and/or ramped simulations may be prudent. Consideration should also be given to the corporate's Expanded Authority level when assessing whether the frequency and scope of additional testing are adequate.

Modeling Process/Internal Control: The examiner should assess the reasonableness of the modeling process, including the audit trail, and the change control process (i.e., a change of algorithm or a change of source of volatility, etc.).

ALCO Documented Strategies: The examiner should review ALCO's documented strategies and assess whether balance sheet changes have been consistent with those strategies. The examiner may consider documented changes in strategies and changes in market conditions in assigning this ranking.

Compliance, Including Internal Validation: The examiner should review the corporate's documentation of its compliance with internal policy limits and with Section 704.8 requirements.

Third Party Validation: The examiner should review any third party validation for scope, methodology, and reasonableness, as required by Section 704.4.

Policies/Procedures: The examiner should review any IRR policies and procedures to determine whether material omissions or deficiencies exist.

Other: The EIC should assign other evaluation factors in light of individual circumstances and any Expanded Authorities.

Liquidity Risk Exposure and Management

Liquidity Risk is the exposure of capital and earnings to costs incurred by the corporate in meeting present and anticipated cash flow needs. Liquidity Risk generally arises from potential mismatches between asset and liability cash flows. Liquidity Risk assessment is complicated by the uncertainties of asset and liability cash flows due to embedded options or other derivatives impacting cash flows. Liquidity Risk includes the risk of early and unexpected share account redemptions.

Liquidity Risk Management includes assessing the memberships' potential liquidity needs in a variety of economic scenarios. Reference should be made to Section 704.9 (Liquidity), and Chapter 202 (ALM) of this guide for further liquidity related factors.

Liquidity sources typically include advised and committed LOCs from U.S. Central or other institutions' repurchase transactions, security sales, and commercial paper. The examiner should assess the corporate's analysis of assets to determine the degree of marketability and potential use of assets as collateral to provide liquidity in the event that this option becomes necessary and is cost beneficial. The examiner should assess the corporate's analysis of the behavior of its shares under normal and alternative economic scenarios, including under a stress ("worst-case") scenario. Management's analysis of the potential liquidity impact arising from any off-balance sheet activities is also a factor.

In measuring and managing net funding requirements, a corporate should prepare a schedule comparing future cash inflows to outflows over a series of time periods. The difference between cash inflows and outflows in each period, or the excess or deficit of funds, becomes a starting-point for a measure of a corporate's future liquidity excess or shortfall. The assessment of different economic scenarios should provide a basis for the corporate's plans to fill any liquidity shortfalls. The examiner should assess the adequacy of the cash flow related assumptions under different scenarios.

The examiner should assess the corporate's access to external (market) sources of liquidity. This assessment should include a review of the diversification of its liabilities, the documented established relationships with liability-holders (e.g., commercial paper), and the corporate's asset-sales markets, if any. Building strong relationships with funding sources can provide a corporate with additional options in the event contingency liquidity plans need to be implemented. The frequency of contact with and use of a funding source are two indicators of the strength of a funding relationship.

At a minimum, the following Quantitative and Qualitative Liquidity Risk Evaluation Factors should be reviewed:

<u>Quantitative Liquidity Risk Evaluation Factors</u>

1. Significant asset/liability concentrations;
2. Core funds determination; and
3. Liquidity measures - cash budgeting.

<u>Qualitative Liquidity Management Evaluation Factors</u>

1. Policies/Procedures (i.e., objectives and contingency plans);
2. Alternative Funding Sources:
    a. Development
    b. Maintaining market presence
    c. Testing
    d. Commercial Paper
    e. Repurchase opportunities;
3. Disintermediation plan (worse case);
4. Early withdrawal penalties;
5. Compliance/monitoring; and
6. Other relevant factors.

Credit Risk

Credit risk is present any time a corporate extends credit, purchases investments, makes commitments and guarantees, and enters into contractual agreements, whether reflected on or off balance sheet. In other words, credit risk is found in all activities where success depends on counterparty, issuer, or a borrower's ability to perform or repay.

Credit risk arises when engaging in a broad range of activities including, the selection of investment products, brokers, and counterparties. Credit risk also arises due to country or sovereign exposure, as well as indirectly through guarantor performance. These credit risks are discussed in more detail in Chapters 201, Investments and 203, Loan Review.

When rating credit risk, the examiner should consider both the quantitative level of credit risk the corporate is exposed to (i.e., concentration risks, third party credit ratings of investment securities, etc.), as well as qualitative factors (i.e., credit risk management policies and procedures). At a minimum, the following key factors should be evaluated when determining Credit Risk Exposure and Credit Risk Management Component Ratings:

<u>Quantitative Credit Risk Exposure Evaluation Factors (Financial Risk Composite)</u>

1. Concentrations of credit by investment type;
2. Concentrations of credit by issuer;
3. Concentrations by sector or industry;
4. Concentrations of loan commitments and/or guarantees; and
5. Loan delinquency and charge off ratios and trends.

<u>Qualitative Credit Risk Management Evaluation Factors (Risk Management Composite)</u>

1. Quality of investment, loan, and credit risk management policies and procedures;
2. Quality of loan underwriting;
3. Quality of credit administration, documentation, and reporting (securities, counterparties, credit ratings, watch lists, outstanding commitments, and ongoing monitoring);
4. Quality of assets; and
5. Other applicable credit risk factors.

The examiner must tailor the scope of the credit risk management review to the corporate's Part 704 Expanded Authority level. For example, a corporate with Base operating authority and a relatively simple investment portfolio will not be expected to have an extremely sophisticated credit risk management function. However, corporates with Part I or II Expanded Authorities can purchase lower rated investments requiring a more elaborate credit risk management process. Specifics related to the credit review required for the various Expanded Authorities are discussed in Chapter 201, Investments, and in the Guidelines for Submission of Requests for Expanded Authority.

Operations, Board Oversight, Audit & Compliance

Management consists of the board of directors, various committees, and operating management. The quality of management is the most important element in the successful operation of a corporate. The quality of this element is normally the factor most indicative of how well risk is identified, measured, monitored, reported, and controlled.

Strong management is a key factor in a corporate remaining financially sound, regardless of external factors. External factors include items such as event risk, economic conditions, interest rate environments, and other factors impacting the corporate's balance sheet or financial condition. The ability to promptly address existing problems and risks, and the capacity to be forward thinking, contribute to the success of each corporate, and help ensure membership obligations are continuously met.

Management's expertise level must be commensurate with its current and projected risk activities. Specific capabilities of officials and operating management will be evaluated and ranked when reviewing the risk management process established for various risk activities.

When assigning the component ratings to Operations and Board Oversight, Audit & Compliance, the examiner will draw upon the analysis of various qualitative risk factors. This process will provide an assessment of the officials overall ability to effectively identify, measure, monitor, report, and control each of the numerous risks inherent in the corporate's operation. Other less tangible or measurable aspects of the management function will be reviewed and risk ranked under the component Evaluation Factors listed below. The examiner should refer to various chapters of this guide when assessing the quality of specific managerial and operational functions.

The following Evaluation Factors should be considered in conjunction with the Expanded Authorities under which the corporate operates (if applicable). The assessment of management's performance under each of these Evaluation Factors is used to determine the overall Operations and Board Oversight, Audit & Compliance Component Ratings.

Operations Component Rating

1. Overall completeness of documented procedures for all operational areas;
2. Adequacy of internal controls for all operational areas;
3. Adequacy of management of MIS systems risk including the LAN, wires, ACH, and item processing; and
4. Other evaluation factors as applicable.

Board Oversight, Audit and Compliance Component

1. Management's overall strategic planning process;
2. Appropriateness and completeness of succession planning;
3. Management's ability to attract and retain sufficiently qualified and experienced personnel;
4. Quality of policy and procedure making activities for all operational areas;
5. Adequacy of continuing education and training for the board, committees, and staff;
6. Effectiveness of the board, committees, and staff;
7. Independence and effectiveness of compliance function;
8. Response to supervision;
9. Accuracy of financial reporting and accounting functions;
10. Response to the internal and external audit functions;
11. Extent of cross training and backup processes;

12. Adequacy and effectiveness of the corporate's infrastructure;
13. Management's effectiveness in addressing legal matters;
14. Effective use of consultants, vendors, and outsourcing; and
15. Other evaluation factors as applicable.

Both the Operations and Board Oversight, Audit & Compliance Component Ratings are qualitative. The overall evaluation of management effectiveness and internal controls does incorporate many of the underlying quantitative factors of the other risk management components, as well as internal, operational, and system controls for corporate operations.

When considering the assignment of risk rankings to the above Evaluation Factors, the examiner should refer to applicable sections of this guide, Part 704, and the Guidelines for Submission of Requests for Expanded Authorities.

Examination Objectives

The EIC's assignment of CRIS Composite Ratings culminates an examination team's review of all significant financial, operational, and compliance evaluation factors in a corporate.

The examination objectives in assigning a CRIS Rating are to:

1. Reflect the weaknesses and corrective actions noted in the examination report;

2. Communicate the EIC's overall assessment of the corporate's condition and viability to NCUA; and

3. Disclose to management NCUA's overall assessment of the corporate's Financial Risk and Risk Management abilities.

Supervision

Supervision provided to individual corporates will be based upon the asset size, Expanded Authority level, and the CRIS Composite Ratings. Supervision plans are developed by the EIC with the concurrence of the CFS and the OCCU Director as discussed in Chapter 102 of this guide.

Examination Procedures

See Corporate Examination Procedures - CRIS (OCCU 401P).

Appendices

Appendix 401A - CRIS Composite and Component Rating Definitions & Evaluation Factors

Appendix 401B - CRIS Examination Workpaper OCCU 102I

Appendix 401A

CRIS COMPOSITE AND COMPONENT RATING DEFINITIONS AND EVALUATION FACTORS

FINANCIAL RISK COMPOSITE RATING

The Financial Risk Composite Rating is based on a careful evaluation of a corporate's financial performance. The five key components used to assess an institution's financial strength are empirical capital measures, credit risk exposure, interest rate risk exposure, liquidity risk exposure, and level and composition of earnings.

The composite rating scale ranges from 1 to 5, with a rating of 1 indicating the strongest level of financial performance relative to the institution's complexity, risk profile, and approved expanded authorities (as applicable); and the level of least supervisory concern. A rating of 5 indicates a critically deficient level of financial performance and an excessive risk profile given approved expanded authorities (as applicable); and the greatest supervisory concern. The composite ratings are defined as follows:

1. Corporate credit unions in this group exhibit a strong financial condition in every respect and generally have financial risk component ratings of 1 or 2. Any financial weaknesses are minor and can be corrected or improved in a routine manner by the board of directors and management. These corporate credit unions are the most capable of withstanding economic instability and market interest rate fluctuation. These corporates are in compliance with all regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. As a result, these corporate credit unions exhibit the strongest financial performance and risk profile relative to the complexity of operations and approved expanded authorities (as applicable).

2. Corporate credit unions in this group are fundamentally sound. For a corporate to receive this rating, no component rating will be more severe than 3. Only moderate financial weaknesses are present and are well within the board of directors' and management's capabilities and willingness to correct. These corporate credit unions are stable and are capable of withstanding business fluctuations. These corporate credit unions are in substantial compliance with all regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. Risk exposures are acceptable relative to the complexity of the corporate's operations and expanded authorities granted (if applicable).

3. Corporate credit unions in this group exhibit a degree of supervisory concern in one or more of the component areas. These corporates exhibit a combination of financial weaknesses that may range from moderate to severe; however, the individual components are not rated more severely than 4. Corporate credit unions in this group generally are less capable of withstanding business fluctuations and are more vulnerable to outside influences than those corporates rated a composite 1 or 2. These corporates may be in significant noncompliance with regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. The overall risk profile of the corporate is less than satisfactory relative to the complexity of operations, and expanded authorities granted (if applicable).

4. Corporate credit unions in this group generally exhibit serious financial deficiencies resulting in unacceptable performance. The problems range from severe to critically deficient. Corporate's in this group are generally not capable of withstanding business fluctuations. There may be significant noncompliance with regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. The corporate's overall risk profile is unacceptable relative to the complexity of operations and expanded authorities granted (if applicable). Institutions in this group pose a risk to the National Credit Union Share Insurance Fund (NCUSIF).

5. Corporate credit unions in this group exhibit critically deficient performance and risk profiles relative to the complexity of operations and expanded authorities granted (if applicable). The volume and severity of problems are beyond the board and management's ability or willingness to control or correct. Immediate NCUSIF financial or other assistance is needed in order for the corporate to be viable. Continual supervisory attention is necessary. Institutions in this group pose a significant risk to the NCUSIF and failure is highly probable.

RISK MANAGEMENT COMPOSITE RATING

The Risk Management Composite Rating is based on a careful evaluation of a corporate's risk management policies, practices, and expertise. The seven key components used to assess an institution's managerial strength are: Capital Accumulation and Planning, Profit Planning and Control, Interest Rate Risk Management, Liquidity Risk Management, Credit Risk Management, Board Oversight Audit & Compliance, and Operations.

The rating scale ranges from 1 to 5. A rating of 1 indicates: the highest quality risk management, operational, and supervisory practices relative to the institution's complexity, risk profile, and approved expanded authorities; and the level of least supervisory concern. A rating of 5 indicates: a critically deficient quality of risk management, operational, and supervisory practices given approved expanded authorities; and the greatest supervisory concern. Composite ratings are defined as follows:

1. A rating of 1 indicates strong performance by management and the board of directors and strong risk management practices relative to the corporate's authorities granted under Part 704. All significant risks are consistently and effectively identified, measured, monitored, and controlled. Management and the board have demonstrated the ability to promptly and successfully address existing and potential problems and risks.

2. A rating of 2 indicates satisfactory management and board performance and risk management practices relative to the corporate's authorities granted under Part 704. All operational policies and practices are deemed fundamentally sound. Minor weaknesses may exist, but are not material to the safety and soundness of the corporate and are being addressed.

3. A rating of 3 indicates management and/or board performance requires improvement, or risk management practices are less than satisfactory given the corporate's expanded authorities under Part 704. The capabilities of management or the board of directors may be insufficient for this corporate. Financial and/or operational problems and significant risks may be inadequately identified, measured, monitored, or controlled.

4. A rating of 4 indicates deficient management and/or board performance or risk management practices are inadequate considering the corporate's expanded authorities under Part 704. The levels of financial and/or operational problems and risk exposures are excessive. Financial and/or operational problems and significant risks are inadequately identified, measured, monitored, or controlled and require immediate board and management action to preserve the corporate's soundness.

5. A rating of 5 indicates critically deficient management and board performance or risk management practices. Management and/or the board of directors have not demonstrated the ability to correct financial and/or operational problems and implement appropriate risk management practices. Financial and/or operational problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the continued viability of the corporate.

INDIVIDUAL FINANCIAL RISK AND RISK MANAGEMENT COMPONENT RATINGS

Empirical Capital Measure Component Ratings

A rating of 1 indicates a strong capital level. No negative trends are apparent.

A rating of 2 indicates a satisfactory capital level. Some negative trends may be apparent; however, the retained earnings and capital ratios meet or exceed the minimum regulatory requirements. Generally, the corporate is not approaching a capital position that will require either an earnings retention requirement, under Section 704.3(i), or a capital restoration plan under Section 704.3(g).

A rating of 3 indicates retained earnings and capital ratios meet or exceed the minimum regulatory requirements of Section 704.3(i) and Section 704.3(d); however, the rating indicates the capital position is approaching a level where either earnings retention, under Section 704.3(i), or a capital restoration plan, under Section 704.3(g), will be required.

A rating of 4 indicates either the retained earnings and/or capital ratios are less than the minimum regulatory requirements of Sections 704.3(i) and 704.3(d), as applicable. Indications are the corporate will be subject to either Section 704.3(i) and/or a capital restoration plan for some time.

A rating of 5 indicates a critically deficient level of capital such that the corporate credit union’s viability is threatened.

Capital Accumulation Planning Component Ratings

A rating of 1 indicates the corporate has set forth reasonable plans for the continued maintenance or accumulation of capital in relation to other financial and operational risks incurred by the corporate, and has consistently achieved the objectives set forth in those plans.

A rating of 2 indicates the corporate has set forth reasonable plans for the continued maintenance or accumulation of capital in relation to other financial and operational risks incurred by the corporate, and has normally achieved the goals set forth in those plans.

A rating of 3 indicates capital accumulation plans set forth by management are weak in relation to the financial and operating risks incurred by the corporate, and goals and objectives set forth in those plans are frequently not achieved.

A rating of 4 indicates capital accumulation plans either are non-existent, or seriously deficient in relation to the corporate's current capital level, financial and operational risks.

A rating of 5 indicates corporate management is either unwilling or incapable of developing and implementing effective capital accumulation plans putting the future solvency of the institution in jeopardy.

Earnings and Profitability Component Ratings

A rating of 1 indicates strong earnings. Earnings are more than sufficient to support operations and to accumulate adequate reserves and undivided earnings after considering credit risk, liquidity risk, interest rate risk, growth, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings.

A rating of 2 indicates the level of earnings is satisfactory. Earnings are sufficient to support operations and maintain the accumulation of adequate reserves and undivided earnings after considering credit risk, liquidity risk, interest rate risk, growth, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings. Earnings that are relatively static, or even experiencing a slight decline, may receive a 2 rating provided the corporate credit union's level of earnings is adequate in relation to the core capital and retained earnings ratios.

A rating of 3 indicates a level of earnings that needs improvement. Earnings may not fully support operations and provide for retained earnings growth commensurate with asset growth after considering credit risk, liquidity risk, interest rate risk, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings.

A rating of 4 indicates a deficient level of earnings. Earnings are insufficient to maintain appropriate retained earnings. Corporate credit unions so rated may be characterized by erratic fluctuations in net income or net interest margin, the development of significant negative trends, nominal or unsustainable earnings, intermittent losses, or a substantive drop in earnings from previous reporting periods.

A rating of 5 indicates critically deficient earnings. A corporate credit union with earnings rated 5 is experiencing losses representing a distinct threat to its viability through the erosion of capital.

Profit Planning and Control Component Ratings

A rating of 1 indicates management has set forth a reasonable and accurate budgeting and cost accounting process that allows for the effective management of fee income and operating expenses in relation to net-interest margin, asset growth, and capital accumulation objectives. Budgeted goals and objectives are consistently obtained with no major variances or revisions to projections required.

A rating of 2 indicates management has set forth a reasonable and accurate budgeting and cost accounting process enabling the effective management of fee income and operating expenses in relation to net-interest margin, asset growth, and capital accumulation objectives. Budgeted goals and objectives are normally obtained. Minor variances and revisions are sometimes incurred.

A rating of 3 indicates management's budgeting and cost accounting processes are weak and normally ineffective in measuring, monitoring, and controlling corporate earnings.

A rating of 4 indicates management's budgeting and cost accounting processes are unreasonable, inaccurate, and critically deficient in measuring, monitoring, and controlling corporate earnings.

A rating of 5 indicates management is unwilling or unable to develop and implement effective budgetary and cost accounting systems.

Interest Rate Risk Exposure Component Ratings

A rating of 1 indicates NEV is strong and well controlled and there is minimal potential financial performance will be adversely affected or regulatory requirements will be violated. The level of earnings and the NEV ratio provide substantial support for the degree of market risk taken by the corporate credit union.

A rating of 2 indicates interest rate sensitivity is acceptable and adequately controlled. There is only moderate potential financial performance will be adversely affected or regulatory requirements will be violated.

A rating of 3 indicates control of interest rate exposure needs improvement or there is significant potential the NEV ratio will be in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The level of earnings and the NEV ratios may not adequately support the degree of NEV exposure.

A rating of 4 indicates the corporate's interest rate sensitivity is in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The NEV or NEV ratio reflect an immediate need to plan and take action to restructure the balance sheet to bring the corporate into compliance.

A rating of 5 indicates a corporate's interest rate sensitivity is in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The level of risk is unacceptable and/or an imminent threat to the corporate's viability.

Interest Rate Risk Management Component Ratings

A rating of 1 indicates interest rate risk management practices are strong for the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. No weaknesses are noted, and no supervisory concerns exist.

A rating of 2 indicates interest rate risk management practices are satisfactory for the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. Some minor weaknesses may be noted with limited supervisory concern.

A rating of 3 indicates interest rate risk management practices need to be improved given the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. Major weaknesses are noted, and a high degree of supervisory concern exists regarding the adequacy of interest rate risk management policies and practices.

A rating of 4 indicates interest rate risk management practices are deficient under any expanded authorities approved (if applicable). Severe weaknesses are noted. Management lacks the expertise to set forth appropriate risk management strategies and practices, and major supervisory concerns exist regarding the adequacy of interest rate risk management polices and practices and regulatory intervention may be necessary.

A rating of 5 indicates interest rate risk management practices are wholly inadequate for the authority, sophistication, and level of interest rate exposure of the corporate. Critical deficiencies are noted. Management lacks the willingness and expertise to set forth appropriate risk management strategies and practices. Supervisory intervention is required.

Liquidity Risk Exposure Component Ratings

A rating of 1 indicates strong liquidity levels and reliable access to sufficient sources of funds on favorable terms to meet present and anticipated liquidity needs.

A rating of 2 indicates satisfactory liquidity levels and funds management practices. The corporate has access to sufficient sources of funds on acceptable terms to meet present and anticipated liquidity needs.

A rating of 3 indicates a weak level of liquidity in relation to short- and long-term cash funding needs. Corporates rated 3 may lack ready access to funds on reasonable terms or may evidence significant weaknesses in funds management practices.

A rating of 4 indicates deficient liquidity levels, and the need for frequent borrowing to fund daily cash needs. Corporates rated 4 may not have, or be able to obtain, a sufficient volume of funds on reasonable terms to meet liquidity needs.

A rating of 5 indicates liquidity levels or funds management practices so critically deficient the continued viability of the corporate is threatened. Corporates rated 5 require immediate external financial assistance to meet maturing obligations or other liquidity needs.

Liquidity Risk Management Component Ratings

A rating of 1 indicates liquidity management policies and practices are strong. Management has developed and maintained reasonable and accurate processes to measure, monitor, and control short- and long-term access to funds. Effective policies have been set forth, identifying effective liquidity contingency plans. No supervisory concerns are noted.

A rating of 2 indicates liquidity management policies and practices are adequate. Management has developed and maintained processes to measure, monitor, and control short- and long-term access to funds. Liquidity contingency plans have been developed. Some minor weaknesses in these plans, policies, and practices may be noted. Some minor supervisory concerns may be noted.

A rating of 3 indicates liquidity management policies and practices are weak. Management's policies and processes for measuring, monitoring, and controlling short- and long-term access to funds may be unreasonable or inaccurate. There is normally a lack of sufficient liquidity contingency plans in place. A high degree of supervisory concern exists.

A rating of 4 indicates liquidity management policies and practices are deficient. Management may lack the appropriate expertise to develop and maintain reasonable and effective processes to measure, monitor, and control short- and long-term access to funds. Major supervisory concerns exist.

A rating of 5 indicates liquidity management policies and practices are critically deficient. Management lacks the ability and willingness to set forth appropriate liquidity management strategies, and regulatory intervention is necessary.

Credit Risk Exposure Component Ratings

A rating of 1 indicates a low level of credit risk exposure with respect to corporate capital and regulatory requirements. No supervisory concern is noted.

A rating of 2 indicates a satisfactory level of credit risk exposure with respect to capital and regulatory requirements. Some concentrations, watch list assets, and other credit weaknesses may exist. However, only minor supervisory concern exists.

A rating of 3 indicates a high degree of credit risk exposure. There may be a significant level of concentrations, watch list assets, and other credit weaknesses apparent. The severity of these risks requires an elevated level of supervisory concern.

A rating of 4 indicates the corporate's assets have a deficient level of credit quality. Significant credit concentrations, watch list assets, and other credit risks are apparent that may subject the corporate to potential losses and threaten its viability. Major supervisory concerns exist.

A rating of 5 indicates a severely high degree of credit risk. Losses have been incurred due to these weaknesses, and the viability of the corporate is threatened. Major supervisory concern and follow up are required.

Credit Risk Management Component Ratings

A rating of 1 indicates strong credit analysis practices. The expertise of management and staff as well as sophistication of policies and practices are commensurate with approved expanded authorities (if applicable). Credit risk is of minimal supervisory concern.

A rating of 2 indicates satisfactory credit administration policies and practices commensurate with approved expanded authorities (if applicable). Some minor weaknesses may be noted; however, management has demonstrated the ability and willingness to correct them in an expedient and effective manner. Only limited supervisory concern is required.

A rating of 3 indicates administration practices are less than satisfactory, considering the corporate credit union's expanded authority (as applicable). There is generally a need to improve credit administration practices, and management has been slow to initiate improvement. Moderate supervisory concern is required.

A rating of 4 indicates a corporate with deficient credit administration practices under base or any expanded authority level. There is a definite need to improve credit administration practices, and management may not possess the necessary expertise to do so. Major supervisory concern and follow up are required.

A rating of 5 indicates critically deficient credit administration practices. The corporate may have significant exposures threatening viability. Management is unwilling or unable to initiate improvement and regulatory intervention is required.

Board Oversight, Audit & Compliance Component Ratings

A rating of 1 indicates strong board, committee, and management oversight. Effective managerial polices and procedures are evident in all areas of operation. Effective succession and backup plans are in place. Appropriate position descriptions and responsibilities have been set, and management and staff continually receive relevant and effective education to enable them to effectively meet the responsibilities of those positions. The corporate has an active and effective audit and compliance program, commensurate with expanded authorities granted. No supervisory concerns exist.

A rating of 2 indicates satisfactory board, committee, and management oversight. Effective managerial polices and procedures are in place for material areas of operation. Some minor weaknesses may be noted. The officials have set forth succession and backup plans that are either completely adequate or exhibit only minor weaknesses. Position descriptions and responsibilities have been set forth, and management and staff generally receive relevant and effective education to enable them to meet their responsibilities. The corporate has a satisfactory audit and compliance program, commensurate with expanded authorities granted (if applicable). In some cases only minor audit and compliance related weaknesses will be noted. Management is responsive to audit and supervision efforts and addresses any deficiencies noted in a timely and effective manner. Only minor supervisory concern exists.

A rating of 3 indicates generally weak board, committee, and/or management oversight. Managerial polices and procedures are not in place for material areas of operation. Weaknesses are noted in existing policies. The officials have either not set forth succession and backup plans, or the plans are considered unreasonable and ineffective. Position descriptions and responsibilities have not been set forth, and management and staff generally do not receive relevant and effective education to enable them to effectively meet their responsibilities. The corporate's audit and compliance program may be unsatisfactory commensurate with expanded authorities granted (if applicable). Management may not be responsive to audit and supervision efforts. Major supervisory concern exists.

A rating of 4 indicates serious managerial weaknesses. The board, committees, and senior management have demonstrated an inability to set forth adequate infrastructure and organizational policy and practice. Critical supervisory concern exists.

A rating of 5 indicates critically deficient management oversight. The board, committees, and senior management are unwilling or unable to address organizational weaknesses. Regulatory intervention is required.

Operations Component Ratings

A rating of 1 reflects high quality operational policies, procedures and processes. Management's abilities, procedures, and practices are of minimal supervisory concern.

A rating of 2 reflects acceptable operational policies, procedures, and processes. Some minor weaknesses may be noted that management is willing and able to correct in an effective and efficient manner. Management's abilities, procedures, and practices warrant only a limited level of supervisory attention.

A rating of 3 reflects a moderate degree of weakness. Management's abilities, operational policies, procedures, and processes are less than satisfactory. The severity of these weaknesses and risks require an elevated level of supervisory review. There is a general need to improve management infrastructure and/or operational policies and practices.

A rating of 4 reflects serious deficiencies with respect to management's abilities, operational policies, procedures, and processes. The unsatisfactory nature of abilities, polices, procedures, and practices have put the assets of the corporate, members, and the NCUSIF at a high level of risk of financial loss or interruption of service. There is a definite need to improve the quality of policies and practices. Extensive supervisory attention is warranted.

A rating of 5 reflects critical deficiencies with respect to management's abilities, operational policies, procedures, and practices. The unsatisfactory nature of policies and practices may have caused financial losses, and threatens the viability of the institution. Management is unwilling or unable to take effective corrective action.

CORPORATE RISK IDENTIFICATION SYSTEM (CRIS)

Listing of CRIS Evaluation Factors by Component

Empirical Capital Component Ratings

Quantitative Empirical Capital Measures
Retained Earnings Ratio
Core Capital Ratio
Capital Ratio
Trends
    Ratio
    Dollars
Other

Qualitative Factors (i.e. Capital Accumulation Planning)
Reasonableness of Capital Accumulation Plan in Relation to Current Capital Levels and Risk Profile

Earnings Component Ratings

Quantitative Earnings Measures
NI Level
Trends
Composition
    Gross Income
    Cost of Funds
    Fee Income
    Operating Expenses
Other

Qualitative Profit Planning and Management Factors
Budgeting and Reporting
Earnings in Relation to Capital Plans
Effectiveness of Cost Accounting Systems and Product Profitability
Pricing Strategies and Policies
Other

Interest Rate Risk Component Ratings

Quantitative Interest Rate Risk Exposure Measures
NEV Base Ratio
NEV Exposure Measure (worst case scenario relative to regulatory floor)
NEV Volatility Measure (change)
Other

Qualitative Interest Rate Risk Management Evaluation Factors
Robustness of Net Economic Value Simulation Models
Robustness of Net Interest Income Simulation Models
Additional NEV and Stress Testing
Expertise of Management and Staff - Interest Rate Risk Management
Modeling Process / Internal Control
ALCO Documented Strategies
Compliance Program and Third Party Validation (if applicable)
Policies/Procedures
Other

Liquidity Component Ratings

Quantitative Liquidity Risk Exposure Evaluation Factors
Concentration Risks
Reasonableness of Core Funds Determination
Liquidity Measures - cash budgeting
Other:

Qualitative Liquidity Risk Management Evaluation Factors
Policies / Procedures
- Objectives
- Contingency Plans

Alternative Funding Sources
- Development
- Maintaining Market Presence
- Testing
- CP
- Repo

Existence of Disintermediation Plan
Existence and Reasonableness of Early Withdrawal Penalties
Compliance / Monitoring
Other

Credit Risk Component Ratings

Quantitative Credit Risk Exposure Evaluation Factors
Concentrations of Credit by Investment Type
Concentrations of Credit by Issuer
Concentrations of Lending, Commitments and Guarantees
Third Party Credit Ratings
Other

Qualitative Credit Risk Management Evaluation Factors
Quality of Credit Risk Management Policies (Investments and Loans)
Quality of Credit Risk Management Procedures (written)
Quality of Loan Underwriting Practices
Quality of Credit Administration, Documentation, and Reporting (Investments)
Quality of Assets
Other

Board Oversight, Audit & Compliance Component Rating
Overall strategic planning process Appropriateness and completeness of succession planning Ability to attract and retain sufficiently qualified and experienced personnel Quality of policy-making activities in all areas of operations and at all levels of management Overall adequacy and effectiveness of the corporate's infrastructure Overall effectiveness of the board of directors Overall effectiveness of committees Overall effectiveness of senior management Independence and effectiveness of compliance functions Responsiveness to supervision Sufficiency of and response to the internal audit function Sufficiency of and response to the external audit Extent of cross training and backup Adequacy of continuing education and training for officials, senior management, and staff Effectiveness in addressing legal matters Effective use of consultants Effective use of vendors and outsourcing Other evaluation factors as applicable

Operations Component Rating
Overall completeness of documented procedures for all areas of operations Accuracy of financial reporting and accounting functions Adequacy of internal controls in all areas of operations Adequacy of management of MIS systems risk including the LAN, wires, ACH, and item processing Other evaluation factors as applicable

Corporate Credit Union:
Effective Date:

FINANCIAL RISK AND RISK MANAGEMENT COMPOSITES (1 to 5):

	EXAM	COMMENTS
Financial Risk:		
Empirical Capital Component Rating:		
Earnings Component Rating:		
Interest Rate Risk Exposure Component Rating:		
Liquidity Risk Exposure Component Rating:		
Credit Risk Component Rating:		

Risk Management:		
Capital Accumulation Planning Component Rating:		
Profit Planning & Control Component Rating:		
Interest Rate Risk Mgmt. Component Rating:		
Liquidity Risk Mgmt. Component Rating:		
Credit Risk Management Component Rating:		
Board Oversight, Audit & Compliance Component Rating:		
Operations Component Rating:		

Corporate Credit Union:
Effective Date:

Empirical Capital Component Rating:	**EXAM**	**COMMENTS**
Retained Earnings Ratio:		
Core Capital Ratio:		
Total Capital Ratio:		
Capital Trends:		
Ratio:		
Dollars:		
Other Factors:		

	EXAM	**COMMENTS**
Capital Accumulation Planning Component Rating:		
Reasonableness of Capital Accumulation Plan:		
Other Evaluation Factors:		

	EXAM	**COMMENTS**
Earnings Component Rating:		
NI Level:		
Trends:		
Composition:		
Gross Income:		
Cost of Funds:		
Fee Income:		
Operating Expenses:		
Other Factors:		

	EXAM	**COMMENTS**
Profit Planning & Control Component Rating:		
Budgeting and Reporting:		
Relation to Capital Plans:		
Cost Accounting Systems:		
Product Profitability:		
Pricing Strategies:		
Other Factors:		

Corporate Credit Union:
Effective Date:

	EXAM	COMMENTS
Interest Rate Risk Exposure Component Rating:		
NEV Base Ratio:		
NEV Exposure Measure:		
NEV Volatility Measure:		
Other Evaluation Factors:		

	EXAM	COMMENTS
Interest Rate Risk Mgmt. Component Rating:		
Robustness of NEV Model:		
FAS 115 Classifications:		
Additional NEV and Stress Testing:		
Modeling Process / Internal Control:		
ALCO Documented Strategies:		
Compliance Program:		
Third Party Validation:		
Policies/Procedures:		
Other Evaluation Factors:		

Corporate Credit Union:
Effective Date:

	EXAM	COMMENTS
Liquidity Risk Exposure Component Rating:		
Asset/Liability Concentrations:		
Core Funds Determination:		
Cash Budgeting:		
Other Factors:		

	EXAM	COMMENTS
Liquidity Risk Mgmt. Component Rating:		
Policies/Procedures:		
Objectives:		
Contingency Plans:		
Alternative Funding Sources:		
Development:		
Maintenance:		
Testing:		
Commercial Paper:		
Repurchase:		
FAS 115 Classifications:		
Disintermediation Plan:		
Early Withdrawal Penalties:		
Compliance/Monitoring:		
Other Factors:		

Corporate Credit Union:
Effective Date:

	EXAM	COMMENTS
Credit Risk Component Rating:		
Concentration by Invest. Type:		
Concentration by Issuer:		
Concentration by Sector or Industry:		
Diversification by Credit Rating:		
Concentrations of Loans, Commitments, and Guarantees:		
Other Factors:		

	EXAM	COMMENTS
Credit Risk Management Component Rating:		
Quality of Policies:		
Quality of Written Procedures:		
Loan Underwriting Practices:		
Credit Administration, Documentation and Reporting (Investments):		
Asset Quality:		
Other:		

Corporate Credit Union:
Effective Date:

	EXAM	COMMENTS
Board Oversight, Audit & Compliance Component Rating:		
Overall Strategic Planning:		
Succession Planning:		
Ability to Attract and Retain Staff:		
Quality of Policy Making:		
Quality of Infrastructure:		
Effectiveness of Board:		
Effectiveness of Committees:		
Effectiveness of Senior Mgmt:		
Independence and Effectiveness of Compliance Function:		
Responsiveness to Supervision:		
Accounting & Financial Reporting:		
Internal Audit Function:		
External Audit Function:		
Cross Training & Backup:		
Continuing Education:		
Legal Issues and Management:		
Use of Consultants:		
Vendors & Outsourcing of Services:		
Other Factors:		

	EXAM	COMMENTS
Operations Component Rating:		
Completeness and Effectiveness of Documented Procedures:		
Adequacy of Operational Internal Controls:		
Adequacy of Management of MIS Systems Risks including LAN, Wire, ACH, and Item Processing Controls:		
Other Factors as Applicable:		