DBF SUP 21-005

DBF GUIDANCE FOR GEORGIA STATE-CHARTERED BANKS, BANK HOLDING COMPANIES, CREDIT UNIONS, AND TRUST COMPANIES

TO:	Supervision Staff
CC:	Georgia State-Chartered Banks and Credit Unions
FROM:	Melissa Sneed Deputy Commissioner for Supervision
SUBJECT:	DEVELOPMENT OF POLICIES BY FINANCIAL INSTITUTIONS
DATE:	May 24, 2021

Policy formulation is a fundamental activity for all newly chartered financial institutions prior to opening for business, as well as established financial institutions. This commentary is designed to help management articulate sound flexible written policies to govern areas critical to a financial institution's success. The suggested areas of coverage for each policy discussed represent <u>minimum recommended coverage</u> for the policy. In all cases, financial institutions will want to expand coverage in the policy to tailor the policy to the unique needs of the institution. <u>Also, the policies included in this commentary are not and should not be considered as the only policies that an institution needs to operate effectively.</u> This statement is a starting point for policy formulation.

Members of the Board of Directors (Board) have a fiduciary responsibility to formulate a set of rules for their organization through written policies. The formulation of written policies offers a financial institution's directors and officers the opportunity to consider and develop basic objectives and to determine the desired institutional direction. It is the Boards' responsibility to review and revise, as necessary, approved, written policies when the strategic plan changes, when the overall condition of the institution changes, when the risk appetite changes, and periodically, but no less frequently than annually.

Creating written policies allows the Board and senior management an opportunity to reconsider the basic objectives of the financial institution as well as emphasizing to financial institution personnel the priority that the Board and senior management give to policy areas. Therefore, the formulation of sound written policies is important. However, implementation, adherence, and regular review of the written policies are critical to the success of the financial institution's safety and soundness.

The adoption of written policies does not guarantee the financial institution's success. Financial institutions operating in a financial services environment must have sound overall strategic planning supported by flexible written policies and capable management to succeed in a highly competitive environment. These guidelines for policy development are one element of support to develop a healthy and successful operation.

LOAN POLICY

A primary purpose of a written loan policy is to provide a framework of standards and points of reference within which individual lending personnel can operate with confidence, relative uniformity, and flexibility. Loans comprise a major portion of the asset structure of most financial institutions and it is the asset category which ordinarily presents the greatest credit risk and, therefore, potential loss exposure. A written loan policy can greatly assist management in the maintenance of proper credit standards, avoidance of unnecessary risks, and proper evaluation of new business opportunities. The lending policy should be tailored to fit the financial institution's specific needs, staff, and objectives. The financial institution's objectives for the lending function should include the generation of appropriate yields relative to the credit risk assumed, prudent underwriting standards that prevent excessive loan losses, prudent risk limits and risk management practices over lending concentrations, and loan terms that control interest rate risk.

Establishment of a lending policy is particularly important in newly organized financial institutions where management and staff are often unacquainted with each other or unfamiliar with the operations of the financial institution. The actual drafting of the policy may be delegated to the chief executive officer and the lending staff, but the Board should have a role in the process, either by reviewing and approving the policy once formulated or by direct participation at critical points in the drafting process. While it is not suggested that the written loan policy should actually be written by the Board, it should be approved by them, and not in a cursory or perfunctory manner, but rather after careful explanation, consideration, and discussion.

A constructive starting point in establishing a written loan policy is the careful evaluation and coverage, at a minimum, of the following points:

1. A description of the general fields of lending in which the financial institution shall engage, the type of loans and collateral considered desirable, and the types of loans and collateral considered undesirable.

2. An identification of the geographical trade area from which financial institution loans should be generated and circumstances under which loans outside the trade area may be granted.

3. The financial institution's legal lending limits and other legal constraints should be set forth to avoid inadvertent violations of financial institution laws and regulations. In determining compliance with the bank’s legal lending limits, the policy should address debt that should be combined and attributed to the same individual, including, but not limited to, continuing obligations for Other Real Estate Owned, overdrafts, cash items in process of collections, loan balances that are guaranteed by the individual, and other recourse obligations.

4. The responsibility of the Board in reviewing and approving loans and periodically reviewing major lines of credit.

5. The lending authorization limits (secured and unsecured) of a loan or executive committee, if any, and each loan officer. These authorities should be approved at least annually, for each individual by written resolution of the Board and kept current at all times.

6. The guidelines under which unsecured loans will be granted.

7. The guidelines for rates of interest and terms of repayment for (i) unsecured loans and (ii) secured loans.

8. Loan-to-value (LTV) requirements for secured loans and identification of the supporting documentation necessary to ensure that appropriate security and lien perfection are taken on the collateral pledged.

9. The maintenance and review requirements for complete and current credit and collateral files on each borrower.

10. Appropriate and adequate collection procedures, including but not limited to, the action to be taken against borrowers who fail to make timely payments.

11. Risk limitations for the maximum amount of loans by collateral type and industry measured against capital levels. Additionally, guidelines establishing limitations on the maximum dollar volume of loans in relation to types of funding sources. This includes assets or deposits of the financial institution based on seasonal demands and loan mix or an established level of loans by type; i.e., commercial, consumer, term, etc. Also, the policy should establish risk management practices that will be used to identify, measure, monitor, and control concentration exposures, as well as strategies that will be used to reduce and mitigate concentration exposures when necessary.

12. Specific guidelines governing loans to employees, officers, and directors of the financial institution, including a prohibition against recurring overdrafts or cash items held against deposit account of the employees, officers, directors, or other insiders of the financial institution (see prohibition of Federal Reserve Regulation O).

13. Appropriate limitations on the extension of credit through overdrafts.

14. A prohibition against (a) the addition of uncollected interest on the unpaid balance of any loan on which such interest is due, (b) the acceptance of a separate note for uncollected interest due on any loan unless supported by additional tangible

collateral which adequately and completely secures the loan, (c) the continuation of accrual of interest on any loan delinquent in principal or interest payments 90 days or more, or (d) any other device that essentially avoids recognition of overdue loans and/or artificially inflates the income of the financial institution.

15. The guidelines under which uncollectible and seriously past due loans will be charged-off.

16. Establishment of an allowance for loan and lease losses (ALLL), or Current Expected Credit Losses, (CECL) if applicable, by the Board which will be maintained against the reasonable risk inherent in the lending operation based on a quarterly review of the loan portfolio and the financial institution's loan volume.

17. Guidelines that address how policy exceptions will be identified, approval requirements of policy exceptions, and ongoing measurement and monitoring of the volume and trend of policy exceptions.

18. Guidelines for when credit memorandums should be created and periodically updated. Guidelines should also address the minimum information that credit memorandums should contain.

19. Guidelines that address the types of financial statements on borrowing entities and guarantors that are required for each loan type and the frequency that financial statements will be acquired.

20. Guidelines for obtaining, ordering, and reviewing appraisals and internal evaluations, when needed. Also, guidelines for content and analysis that should be included in internal evaluations.

21. Guidelines addressing the financial institution's loan review and grading system ("Watch list").

22. Plans to create, produce, and review related debt reports that aggregate all obligations of a single borrower to the financial institution including personal and business debt, obligations remaining from Other Real Estate Owned, overdrafts, cash items in process of collection, full and limited guarantees, and recourse obligations.

23. Guidelines for underwriting requirements and limitations for participation loans purchased.

24. Guidelines for when loan covenants will be required, when appropriate.

After adoption of a written loan policy, the administration of the policy is the responsibility of the Board. Procedures should be implemented to determine compliance with the loan policy. It is most important that the loan policy be adaptable to changing economic conditions, balance sheet management considerations, the financial institution's financial position, and competitive conditions.

Credit Grading Systems

Accurate and timely credit grading is a primary component of an effective loan review system and should be thoroughly addressed in the loan policy. Credit grading involves an assessment of credit quality, the identification of problem loans, and the assignment of risk ratings. An effective system provides information for use in establishing valuation allowances for specific credits and for the determination of an overall ALLL or CECL level.

Credit grading systems often place primary reliance on loan officers for identifying emerging credit problems. Given the importance and subjective nature of credit grading, a loan officer's judgement regarding the assignment of a particular credit grade should generally be subject to review. Reviews may be performed by peers, superiors, or loan committee(s), or by other internal or external credit review specialists. Credit grading reviews performed by individuals independent of the lending function are preferred because they often provide a more conservative assessment of credit quality. A credit grading system should, at a minimum, include the following:

1. A formal credit grading system that can be reconciled with the framework used by regulatory authorities;

2. An identification of loans or loan pools that warrant special attention;

3. A mechanism for reporting identified loans, and any corrective action taken, to senior management and the Board; and

4. Documentation of an institution's credit loss experience for various components of the loan and lease portfolio.

A tool used in this regard is the establishment of loan review and grading systems.

Loan Review Policy and System

Management should maintain written policies and procedures governing the loan review system. These should be reviewed and approved at least annually by the Board. The term loan review system refers to the responsibilities assigned to various areas such as credit underwriting, loan administration, problem loan workout, independent and ongoing credit review, or other areas. The complexity and scope of a loan review system will vary based upon an institution's size, type of operations, and management practices. Although, smaller institutions may not be expected to maintain separate loan review departments, it is essential that all institutions maintain an effective loan review system.

Regardless of its complexity, an effective loan review system is generally designed to address the following objectives:

- To promptly identify loans with well-defined credit weaknesses that warrant the special attention of management so that timely action can be taken to minimize credit loss;

- To provide essential information for determining the adequacy of the ALLL;

- To identify relevant trends affecting the collectability of the loan portfolio and isolate potential problem areas;

- To evaluate the activities of lending personnel;

- To assess the adequacy of, and adherence to, loan policies and procedures, and to monitor compliance with relevant laws and regulations;

- To provide the Board and senior management with an objective assessment of the overall portfolio quality as well as actions taken by management; and

- To provide management with information related to credit quality that can be used for financial and regulatory reporting purposes.

The loan review policy should include a written description of the overall credit grading process and establish responsibilities for the various loan review functions. Loan review may be implemented by a qualified external party, auditor, loan review officer, or a loan review committee who should report directly to the Board. The nature, scope and structure of loan review and grading systems will vary with the size and complexity of each financial institution; however, the loan review policy should generally address the following items:

1. Qualifications of loan review personnel: Qualifications should be based on level of education, experience, and extent of formal training. In addition, they should be knowledgeable of pertinent laws and regulations that affect lending activities, sound lending practices, and their own institution's specific lending guidelines.

2. Independence of the review personnel: Management should ensure that all loans that are included in the loan review are reviewed by individuals that are independent of the loans under review, including the underwriting, administration, and approval processes.

3. Frequency of reviews: The loan review function should provide feedback on the effectiveness of the lending process in identifying emerging problems. Reviews of significant credits should be performed annually, upon renewal, or more frequently when factors indicate a potential for deteriorating credit quality. Additionally, a

sampling of loans with balances below the significant credits should be reviewed in tiers throughout the year to assess the quality of other segments of the loan portfolio, specifically addressing weak or negative trends that may be pervasive throughout a particular loan type.

4. Scope and depth of reviews: The scope and depth of the review should include not only a review of specific loans, but also a review of the entire credit administration process. The annual review program should cover significant loans and other loans to result in a percentage of the loan portfolio that can be reasonably extrapolated to capture the overall risk exposure of the loan portfolio. The scope should include analysis of credit quality, the sufficiency of credit memoranda and collateral documentation, completeness of the lien perfection, appropriateness of and compliance with internal policies and procedures as well as applicable laws and regulations, the accuracy and timeliness of assigned credit grades, and the effectiveness of the institution's internal controls, approval processes, tickler systems, and exception tracking reports.

5. Review of findings and follow-up: Loan review findings should be reviewed with appropriate loan officers, department managers, and members of senior management. Any existing or planned corrective action should be elicited for all noted deficiencies. All deficiencies that remain unresolved should be reported to senior management and the Board.

6. Maintenance of workpapers: Workpapers for loans reviewed should consist of documentation supporting assigned ratings and findings.

7. Board reporting: Timely reports should be prepared and submitted to the Board that summarizes the results of the loan review. Deficiencies should be addressed and remedied in a prompt manner.

<u>Environmental Risk and Lender Liability Program</u>

A growing area of potential risk associated with lending is the potential for liability under various environmental laws and claims of lender liability by borrowers, and possibly other creditors and shareholders. The potential adverse effect of environmental contamination on the value of real estate collateral and the potential for liability have become important factors in the evaluation of real estate transactions and making loans secured by real estate. The Environmental Protection Agency (EPA) has responsibility for enforcement authority of environmental laws. The EPA may be contacted for information or exemptions available to financial institutions regarding liability and cleanup of contaminated property. Legislation and the authority of the EPA are still evolving regarding liability of financial institutions as lenders holding a security interest in contaminated property. In order to minimize the financial institution's exposure when holding a security interest in real or personal property that may be in violation of Federal or State environmental laws, and when making loans to borrowers who engage in a potentially environmentally sensitive business, the following should apply to all real estate loans in which the financial institution has a security interest or owns outright through foreclosure, with the exception of single family residences:

1. Procedures: When taking a loan application from the borrower, the loan officer should make a determination as to whether or not the borrower is involved in any way with the use of hazardous substances. The financial institution should develop and maintain a list of such businesses which may engage in a potentially environmentally sensitive activity. The financial institution should establish guidelines for actions to be taken when a borrower is suspected to engage in a business that uses hazardous substances. The history of the property and whether the property has been used for hazardous substances in the past and whether any remediation is needed should also be considered and documented.

2. Risk Assessment: If it is determined that the borrower may be involved in a potentially hazardous industry or business, the loan officer should follow established procedures such as a Preliminary Environmental Risk Review. After completing the assessment, a determination must be made as to whether or not an environmental risk audit by an outside firm should be ordered and performed prior to making the loan to the potentially hazardous business.

3. Documentation: When closing a loan which is secured by real property of a potentially hazardous business, the customer should execute an indemnity and hold harmless covenant. This document should be attached to the Security Deed.

4. Managing the Loan: Under existing Federal and State laws, the financial institution may have an exemption from environmental liability as the holder of a security interest in the real property collateral as long as the financial institution's actions involved with the customer do not constitute "participating in the management" of the business. The financial institution should not exercise any decision-making control over the borrowers' environmental compliance obligations. Also, the financial institution should not take any responsibility for all, or substantially all of, the operational aspects of the borrower’s enterprise.

<u>Lender Liability Risk Management</u>

Financial institutions should address procedures in the written loan policy to manage the risk of lender liability through file documentation and loan administration practices. Claims of lender liability usually involve problem workout and collection loans. Memoranda in the loan file should detail the various terms of the credit and any agreements reached with potential borrowers. Management must be consistent in its handling of the borrower. Files should be cleansed free of extraneous materials and care should be exercised in file maintenance. The conduct of loan officers should be professional and oral agreements of any kind should be avoided, or if one is made, it should be confirmed in writing with the borrower, with a copy to the loan file. Participation by the loan officer in management of the borrowers' business or interference in its day-to-day affairs should be avoided. All management activities should be carried out in good faith, consistently apply fair dealings, and in accordance with the terms of the loan agreement.

Subprime Lending Program

For purposes of this guidance, "subprime lending" is defined as extending credit to borrowers who exhibit characteristics indicating a significantly higher risk of default than traditional lending customers as defined in Interagency Guidance on Subprime Lending, March 1, 1999, and the Interagency Expanded Guidance for Subprime Lending Programs. January 31, 2001. Institutions often refer to subprime lending by other names such as the nonprime, nonconforming, high coupon, or alternative lending market.

The term "subprime" refers to the credit characteristics of the borrower at the loan's origination, rather than the type of credit or collateral considerations. Subprime borrowers typically have weakened credit histories that include payment delinquencies, and possibly more severe problems such as charge-offs, judgments, and bankruptcies. These borrowers may also display reduced repayment capacity as measured by credit scores, debt-to-income ratios, or other criteria.

Financial institutions should have comprehensive written policies and procedures, specific to each subprime lending product, that set limits on the amount of risk that will be assumed and address how the institution will control portfolio quality and avoid excessive exposure. Policies and procedures should be in place before initiating the activity. Acceptable origination channels, dealers, brokers, correspondents, and marketing firms, for subprime loans should be included in written policies. Additionally, minimum regulatory capital requirements will not apply to an institution's portfolios that exhibit substantially higher risk profiles that exist in subprime loan programs. Subprime lenders should retain additional capital support consistent with the volume and nature of the additional risks assumed. These institutions are expected to establish procedures for quantifying the amount of capital needed to offset the additional risk in subprime lending activities, and for fully documenting the methodology and analysis supporting the amount specified.

Subprime lending should only be conducted within a comprehensive lending program that employs strong risk management practices to identify, measure, monitor, and control the elevated risks that are inherent in this activity. If risks associated with subprime lending activities are not properly controlled, subprime lending may be considered an unsafe and unsound practice.

The Board's decision to engage in subprime lending programs should be based on the institution's overall business strategy and risk tolerances, and with a full knowledge of all business risk issues. When establishing subprime lending programs, management should proceed slowly and cautiously. The following items are essential components of a risk management program for subprime lending:

Planning and Strategy: Prior to engaging in subprime lending, the Board and senior management should ensure that all involved parties have properly addressed critical business risk and issues including:

1. Evaluated costs associated with attracting and retaining qualified personnel, and investment in the technology necessary to manage a more complex portfolio.
2. Developed a clear solicitation and origination strategy that allows for after-the-fact assessment of subprime portfolio performance.
3. Established appropriate feedback and control systems.
4. Developed a risk assessment process that extends beyond credit risk and appropriately incorporates operating, compliance, market, liquidity, reputation, and legal risks.
5. Implemented a periodic Strategic Plan performance analysis to detect adverse trends or circumstances and take appropriate action in a timely manner.

Management and Staff: Prior to engaging in subprime lending, the Board should ensure that senior management and staff possess sufficient expertise to appropriately manage the risks in subprime lending and that staffing levels are adequate for the planned volume of activity. Generally, it is not sufficient to have the same staff responsible for both subprime and prime loans. Staffing challenges include:

1. Subprime lending requires specialized knowledge and skills that many financial institutions do not possess.
2. Marketing, account origination, collections strategies, and techniques often differ from those employed for prime credit.
3. Servicing and collecting subprime loans can be very labor intensive and requires a greater volume of staff with smaller caseloads.
4. Compensation programs should not depend primarily on volume or growth targets; any targets used should be weighted towards factors such as portfolio quality and risk-adjusted profitability.

Profitability and Pricing**:** A key consideration for lenders in the subprime market is the ability to earn risk-adjusted yields that appropriately compensate the institution for the increased risk and costs assumed. The institution must have a comprehensive framework for pricing decisions and profitability analysis that considers the following for each product:

1. Origination, administrative/servicing, expected charge-offs, funding, and capital.
2. Fees - including the extent they are recurring and a viable source of revenue.
3. Profitability projections should be incorporated into the operating budget and business plan.
4. Method of tracking actual performance against projections regularly and a process for addressing variances.

Loan Review and Monitoring: The Board should adopt and implement a comprehensive analysis and information system that identifies, measures, monitors, and controls the risks associated with subprime lending.

1. The analysis must promote understanding of the portfolio and early identification of adverse quality/performance trends.

2. Systems employed must possess the level of detail necessary to properly evaluate subprime activity.
3. Analysis should take into consideration the effects of portfolio growth and seasoning, which can mask true performance by distorting delinquency and loss ratios.
4. Liquidity and funding sources for subprime lending should be reviewed and assessed periodically.
5. Management should monitor customer behavior and credit quality and take proactive measures to avert potential problems.

Concentrations in non-owner occupied Commercial Real Estate lending and Acquisition, Development and Construction Lending

Generally, an asset concentration is a significantly large volume of economically-related or collateral-related assets that an institution has advanced or committed to a person, entity, affiliated group, or industry. These assets may in the aggregate present a substantial risk to the safety and soundness of the institution. Adequate diversification of risk allows the institution to avoid the excessive risks imposed by credit concentrations. Concentrations add a dimension of risk which the Board should consider when formulating plans and policies. Elevated concentration levels require additional capital support commensurate with risk taken.

In formulating policies, management should, at a minimum, address goals for portfolio mix and limits within the real estate acquisition, development and construction (ADC) loan category, and the non-owner occupied commercial real estate (CRE) loan category. Management should consider the need to track and monitor the economic and financial condition of specific geographic locations, industries, and groups of borrowers in which the financial institution invests heavily.

The degree of risk in real estate loans depends primarily on the loan amount in relation to collateral value, the interest rate, and most importantly, the borrower's ability to repay in an orderly fashion. Financial institutions can jeopardize their capital structure by a concentration in ADC and non-owner occupied CRE loans. Adverse economic conditions could result in a decline in realty values. Additional risks in concentrated ADC and non-owner occupied CRE lending include: granting real estate loans without consideration of normal or even depressed realty values during periods of great demand and inflated price structure, lending to the maximum debt and paying capacity of borrowers, granting loans that lack adequate guarantor support, and failure to reasonably restrict real estate loans for projects that are not economically viable.

When real estate lending concentrations exist, the Board should adopt policies that address the following factors, at a minimum:

- Maximum amount that may be loaned on a given property, in a given category, i.e. subdivision;
- Required appraisals (professional judgments of the present and/or future value of the real property);

- Guidelines for guarantor requirements;
- Minimum requirement for initial equity investment;
- Guidelines for support of draw requests with inspections;
- Periodic monitoring of concentrations of credit;
- Information systems that provide reports by loan type or repayment source for industry concentrations which include dollar volume/amount and percentages for funded and unfunded totals measured against the sum of Tier 1 Capital and the ALLL;
- Limitation for specific ADC and non-owner occupied CRE concentrations, such as applicable sub-groups of ADC and CRE lending; and
- Limits on the number of speculative and pre-sold construction home loans granted to each builder and in each development.

LIQUDITY AND FUNDS MANAGEMENT POLICY

Liquidity represents the ability to efficiently and economically accommodate decreases in deposits and other liabilities as well as fund increases in assets. Liquidity is essential in all financial institutions to compensate for expected and unexpected balance sheet fluctuations and provide funds for asset growth. Because liquidity is critical to the ongoing viability of any financial institution, liquidity management is among the most important activities that a financial institution conducts.

The Board should understand the nature and level of the institution's liquidity risk, establish the institution's tolerance for liquidity risk, and approve significant policies related to liquidity and funds management. The Board, or a duly elected committee of the Board, should also ensure that senior management takes the necessary steps to monitor and control liquidity risk within the parameters of Board-approved policies. Liquidity and funds management is generally the function of the Chief Financial Officer, who manages the liquidity risk in consultation with the Board or an authorized Asset Liability Management Committee (ALCO).

In institution should establish a funding strategy that provides effective diversification in the sources and tenor of funding. In general, management should avoid funding concentrations, as undue over reliance on any one source of funding increases liquidity risk and can be considered an unsafe and unsound practice. Funding diversification allows management to maintain access to different funding lines and provides flexibility in selecting the appropriate funding source. Also, an institution will likely benefit from a diversified funding base in times of financial distress.

Effective analysis and management of liquidity requires management to measure the liquidity position of the financial institution on an ongoing basis and to examine how funding requirements are likely to evolve under various scenarios, including adverse conditions. The formality and sophistication of funds management depends on the size and sophistication of the financial institution, as well as the nature and complexity of its activities. The objectives and guidelines of funds management should encompass the following:

1. Planning for funding gaps (cash flow planning)

2. Maintaining ample amounts of unencumbered liquid asset reserves

3. Establishing risk tolerances for individual and aggregate limits on all potentially volatile funding sources

4. Addressing funding concentrations or excessive reliance on any single source of funding

5. Managing Net Interest Margin

6. Maintaining access to continency funding sources
7. Performing balance sheet planning (asset mix, liability mix)
8. Planning short-, medium-, and long-term funding

These objectives are integral parts of a funds management policy and should include appropriate risk tolerance benchmarks as established by the Board. Benchmarks and limitations should align with the institution's short- and long-term planning objectives in consideration of the risk profile of the institution, including support from earnings and capital as well as the current economic environment.

Developing forward looking assumptions through intelligent forecasting, as opposed to speculation, is essential to liquidity planning. Management must consider the effect future events are likely to have on funding requirements as well as the probability of such events occurring. All financial institutions are affected by changes in the economic climate, but sound financial management can minimize negative changes and maximize positive ones.

The Board should understand the nature and level of the institution's liquidity risk, establish the institution's tolerance for liquidity risk, and approve significant policies related to liquidity management. The Board, or ALCO, should also ensure that senior management takes the necessary steps to monitor and control liquidity risk.

Determination of the adequacy of a financial institution's liquidity position depends upon:

1. An analysis of the current liquidity position;
2. Historical funding requirements;
3. Anticipated future funding needs; and
4. Options for reducing funding needs or attracting additional funds.

A liquidity and funds management policy should generally provide guidance for forecasting liquidity needs while considering the unique characteristics of the financial institution, the Board's goals regarding asset and liability mix, desired earnings, and margins necessary to achieve desired earnings. The policy should provide guidance to identify anticipated funding needs and authorize the means available for management to meet those needs. The policy should establish responsibility for liquidity and funds management decisions and provide a mechanism for necessary coordination between the different departments of the financial institution. Strategies should be based on sound, well-deliberated projections. The Board should be satisfied that the assumptions used in the projections are valid and the strategies employed are consistent with projections.

Contingency funding plans are essential to liquidity planning. Despite senior management's efforts to provide for liquidity needs, events may unfold that negatively impact available resources. Senior management should consider the limitations of maintaining the current, or planned, liability structure if certain funding strategies become unavailable. For example, rate restrictions resulting from deterioration in the overall condition of the institution could eliminate some funding sources. Also, funding resources from Federal agencies may be curtailed and/or eliminated based on deterioration of the overall condition of the institution and/or deterioration in qualifying assets eligible to serve as collateral. Senior management should monitor the financial condition of liquidity resources for financial deterioration to determine if correspondent institutions can be reasonably expected to provide funding. Contingency plans must be developed in consideration of both internal and external funding restraints the financial institution may encounter.

Based upon the foregoing elements of liquidity, the development of a liquidity and funds management policy should include the establishment of guidelines for the following topics:

1. Periodic review of the financial institution's deposit structure, including the volume and trend of total deposits and the volume and trend of the various types of deposits offered, the maturity distribution of time deposits, rates being paid on each type of deposit, rates being paid by trade area competition, caps on large time deposits, public funds, out-of-area deposits, and any other information needed. Management should consider maturity and repricing balance sheet mismatches, anticipated funding needs, and economic and market forecasts in its liquidity planning.

2. Conveys the Board's risk tolerance and establishes target liquidity ratios such as loan-to-deposit ratio, loan-to-asset ratio, long-term assets funded by less stable funding sources, individual and aggregate limits on potentially volatile funds by type and source, liquidity ratio, or a minimum limit on the amount of short-term investments.

3. Processes to monitor cash flow projections to identify potential cash flow mismatches and gaps over specified future time horizons under both expected and adverse business conditions.

3. An adequate system of internal controls that ensures the independent and periodic review of the liquidity management process, and compliance with policies and procedures and liquidity strategies. Monitoring compliance should include adherence and limits for managing and monitoring liquidity to ensure adequate liquidity is maintained at all times. This process should also include monitoring internal and external factors and events that could have a bearing on the institution's liquidity.

4. A contingency plan that addresses alternative sources of funds if initial projections of funding sources and uses are incorrect or if a liquidity crisis arises. This plan should

include scenarios of changing overall financial conditions and for varying resources available for each situation, particularly changes to capital categories for Prompt Corrective Action as certain funding sources automatically become unavailable for certain categories.

5. Establishment and periodic testing of correspondent institution lines of credit including both unsecured and secured lines. Diversification reduces dependence on any one supplier. The financial institution should not exceed its capacity to borrow in any one area or market. A limit should be set for each category of borrowing.

6. Long-range investment strategy with regard for liquidity needs includes maintaining adequate liquidity levels while at the same time minimizing the cost of those funds. If the financial institution experiences cyclical loan demand or deposit fluctuations, educated predictions can be made for funding requirements and investments can be purchased with those needs in mind.

7. Liquidity plans must consider changes in cash flow due to interest rate changes. The degree of interest rate risk exposure will affect liquidity due to the cash flow changes that result from interest on rate-sensitive assets and liabilities.

8. In conjunction with the financial institution’s investment policy, a determination must be made regarding the types of investments permitted, the desired mix among those investments, the maturity distribution and the amount of funds that will be available, and reviews of pledging requirements. A maturity ladder in the investment portfolio which is consistent with the liability structure of the financial institution should coincide with both the sources and uses of funds.

9. Periodic stress testing of contingency funding plans under satisfactory, deteriorating, and unsatisfactory overall conditions to assess adequacy of plans at varying degrees of stress from both internal and external pressures.

10. Adequate Board or ALCO review of policy compliance and evaluating the current and projected liquidity position is necessary so that immediate remedial action can be taken to correct imbalances and avoid illiquid conditions. Where noted changes in the financial institution's environment affect management's predictions concerning anticipated liquidity needs, periodic review of the Policy and the financial institution's planned liquidity position can be fine-tuned to meet the liquidity needs due to the uncontrolled changes in the marketplace.

11. Approval procedures for exceptions to policies, limits, and authorization should be defined. Exceptions should be discussed by the Board or ALCO and documented in the minutes.

Once anticipated and potential needs have been determined, management must decide how those needs will be met through funds management. Every financial institution should carefully consider the reasonable options to establish optimum liquidity management operations.

INVESTMENT POLICY

Management of a financial institution's investment portfolio requires the adoption of a defined investment policy. The uncertainty and volatility of the bond and other investment markets of the past underscore the need for sound investment portfolio administration to achieve the desired goals of high profitability, optimum liquidity, and acceptable quality. It is the responsibility of the Board to develop the investment policy. To ensure that the directorate does not delegate policy decisions, a financial institution's investment policy must provide details and encompass minimums and maximums rather than a philosophical description of objectives. The policy should be in written form, reviewed periodically by the Board and revised as needed in view of changing circumstances and the needs of the individual financial institution. By establishing clarity of direction, a written investment policy should provide the basic foundation upon which effective portfolio strategy can be developed.

Each financial institution, regardless of size or its unique characteristics, should consider at a minimum the following major factors in formulating a written investment policy:

1. A Statement of the Objectives of the Investment Portfolio: Such objectives should include the following:

    (a) To provide an investment medium for funds which are not needed to meet loan demand or deposit withdrawal;

    (b) To optimize income generated from the investment account consistent with the stated objectives for liquidity and quality standards;

    (c) To meet regulatory standards;

    (d) To provide collateral which the financial institution is required to pledge against public monies;

    (e) To provide an investment medium for funds which may be needed for liquidity purposes;

    (f) To provide an investment medium which will balance market and credit risk of other assets and the financial institution's liability structure; and

    (g) Other objectives (as deemed appropriate for the specific financial institution).

2. Assignment of Responsibilities: Responsibilities of the Board, investment officer(s), and Investment Committee should be detailed.

3. Listing of Acceptable Investments: Acceptable investments may include U.S.

Treasury securities, Federal Agency securities, municipal obligations, certificates of deposits of other financial institutions, financial institution acceptances, collateralized mortgage obligations, etc. All investments should conform to applicable Sections of the Code of Georgia Annotated and the Rules of the Department.

4. Investment Portfolio's Composition and Investment Limitations: The policy should define responsibility for establishing minimum and maximum amounts to be invested in the various acceptable investments. Proper diversification in the investment portfolio will avoid unfavorable concentrations in obligations of a single issuer or in the types of investments whose quality depends largely upon the same set of circumstances. Appropriate geographic distribution in municipal investments should be established. Factors to be considered in establishing investment limits should include regulatory requirements and constraints, liquidity needs, tax position, and collateral and pledging requirements.

5. Acceptable Maturity Ranges: A soundly planned maturity schedule will take into consideration the financial institution's invested position, prevailing and anticipated loan demands, and the stability of mixed funding sources.

6. Acceptable Quality of Investments: Investments whose quality is reflective of speculative or substandard elements should not be purchased. Investment purchases should be restricted and purchased only after proper credit documentation has been analyzed to determine investment quality.

7. Acceptable Lot Sizes: Minimum and maximum lot sizes should be established for purchases.

8. Acceptability of Trading Securities: Trading is a day-to-day operation of buying and selling securities that requires easy access to the securities market. Trading requires experience and an expertise not available to most financial institutions. Gains and/or losses should be considered in light of the financial institution's earnings, tax, and capital positions.

9. Pledging Practices and Requirements: Investments should be adequate to secure deposits which by statute are required to be secured.

10. Accounting and Recordkeeping: Guidance on the accounting and reporting for securities should be based on generally accepted accounting principles.

11. Internal Controls: Internal controls over investment activities should be commensurate with the volume and complexity of the investment activity conducted by the institution and should be as independent as practical from related

operations. The policy should emphasize separation of duties between the individuals who execute and account for investment activities.

12. Credit Risk: Management should be restricted to investment quality instruments. Guidelines on credit analysis and due diligence suitability analysis should be performed to determine if instruments are suitable for purchase relative to the financial institution's tolerance for credit risk, asset liability position, sensitivity to market risk, and liquidity exposure.

13. Pre-purchase Analysis Requirements: The institution's pre-purchase analysis should clearly document the due diligence process and quality analysis required before a security is purchased. While the analysis may contain information provided by the party selling the security, the purchase decision should be independent from the organization selling the investment product. Pre-purchase analysis should document management's understanding of the risk associated with the product purchased, how the investment fits within the current balance sheet structure, and comparison to established policy limits and strategies.

14. Exceptions to Policy: Approval procedures for exceptions to policies, limits, and authorization should be defined. Exceptions should be discussed by the Board or designated committee and documented in the minutes.

Securities activities by financial institutions may be affected by internal factors such as a slackening of loan demand and a decline in net interest margins which may prompt some financial institutions to look more closely at the investment portfolio as a source for improving profitability. Certainly, this should always be a consideration; however, there are certain boundaries that should always be observed. Investments can have a profound impact on an institution's performance. Some of these activities are encouraged by securities dealers whose primary motivation is commission income and not the safety and soundness of the financial institution system. The following points should always be observed to help alleviate problems:

1. Written investment policies which discourage speculative trading activity should be adopted by the Board and followed by appropriate financial institution management.

2. The financial institution should adhere to specific limits on individual security issues contained in its investment policy.

3. Appropriate vendor management practices should apply to securities dealers with whom the financial institution regularly does business.

4. Comparison pricing should be considered when purchasing securities.

5. The investment officer should ascertain that the securities to be purchased are, in fact,

permissible investments in conformity with the Official Code of Georgia Annotated and comply with Rules of the Department.

6. The investment officer should review a stress test before purchasing a Collateralized Mortgage Obligation, or similar investment, in order to ensure that the investment is not a "high-risk" security. Stress tests should be reviewed periodically in an assessment of the suitability and investment eligibility of the security. Stress tests are required on at least an annual basis, but during times of rapid interest rate movements, should probably be performed on a quarterly basis.

7. Management needs to be aware of the accounting treatment for the designation of "Held to Maturity," "Available for Sale," or "Trading" under accounting standards may have a significant impact on earnings and/or capital.

SENSTIVITY TO MARKET RISK POLICY

All financial institutions are expected to have a comprehensive Board-approved policy governing all aspects of the interest rate risk (IRR) management process. The policy should ensure that the institution's strategies, products, and business activities are integrated into the IRR management process. Established earnings and capital exposure limits that are commensurate with the risk tolerance of the Board should be articulated from a short- and long-term perspective. The policy should also identify strategies, instruments, and activities that may be used to manage IRR risk exposure.

The frequency and methods for measuring and monitoring IRR should be established. All institutions should have a measurement system or model to measure IRR exposure that corresponds with the size and complexity of the institution. The contents of the policy and the complexity of the model should be comprehensive and encompass the risk authorized by the Board, the actual on- and off-balance sheet risk, anticipated changes from implementation of strategic changes, and challenges related to the overall condition of the institution in the economic environment.

The development of policies and procedures governing IRR should include the following topics:

1. Responsibility and authority for establishing and maintaining an effective IRR management program that identifies, measures, monitors, and controls IRR within Board-approved limits should be clearly outlined. Most Boards will choose to delegate oversight authority to the ALCO, which meets on a periodic basis no less than quarterly. The ALCO will oversee the model results to determine if daily management has appropriately controlled interest rate risk within the Board's authorized risk tolerance. Additionally, the ALCO will review the model's assumptions, inputs, and independent evaluation of the mechanics of the model as well as sufficiency of the overall process. Generally, an institution will also have a daily management committee to perform the following functions:

   A. Monitor business conditions, financial markets, and regulatory changes on a continuing basis;

   B. Manage the mix of rate sensitive sources and uses of funds over interest rate cycles; and

   C. Evolve key loan, deposit, investment, and funds management strategies consistent with profit planning and longer-range goals and objectives.

2. Stress testing that includes both scenario and sensitivity analysis is an integral component of IRR management. The policy should outline the frequency and types of scenario stress testing the Board expects to be conducted. Risk tolerances should be established

for each stress scenario run in order for management to compare results with Board expectations. Additionally, proper management of IRR requires reasonable assumptions that align with on- and off-balance sheet risks and customer behaviors. Management should ensure that key assumptions are identified by periodic stress testing of assumptions to help determine those that have the most influence on model output.

3. Guidelines for overseeing the implementation and maintenance of management information and measurement systems that identify, measure, monitor, and control IRR should be incorporated into the policy. Management information and measurement systems should be flexible and tailored appropriately to meet the institution's needs. As an institution grows in asset size and/or the complexity of the risk exposure changes, the model should be reassessed to determine if it is appropriate to capture the risks relevant to the strategic direction of the institution.

4. An adequate system of internal controls must be present and ensure the independent and periodic review of the IRR management process, models, and compliance with policies and procedures. The review should encompass compliance with policies, procedures, and interest rate strategies. The scope of the review should involve and assessment of the reasonableness of the assumptions used in the model, the process in determining those assumptions, and the backtesting of assumptions and results. The review should occur regularly and whenever a material change is made to the process or strategic direction. Additionally, model validations to ensure mechanics and mathematics of the IRR model are functioning as intended must be obtained.

5. Approval procedures for exceptions to policies, limits, and authorization should be defined. Exceptions should be discussed by the Board or designated committee and documented in the minutes.

The Board should consider taking advantage of features of the model that are designed to assist with balance sheet planning. Most models can be configured for a static balance sheet or a dynamic balance sheet. The features that produce dynamic results are useful for both budgeting, strategic planning, and stress testing. Certain data and assumptions are input into the model to project "what if" scenarios to produce reports for executive analysis.

The Board should control interest rate exposure by managing the entire balance sheet, both assets and liabilities, to result in a reasonable level of interest rate risk exposure in consideration of the condition of the institution and support available from earnings and capital. Each institution has a unique set of risks, which results in varying degrees of authorized risk. The Board controls this risk through the risk limitations and activities authorized in its policies.

AUDIT POLICY

Each financial institution is required to have an adequate audit program. One of the primary tools to be used by the Board of a financial institution to facilitate the implementation of an adequate audit program is the development and maintenance of a written policy on audit considerations. Such a policy would allow the Board to target and direct the audit program of the institution, thereby having a direct influence to ensure that the audit program is tailored to the needs of the institution. The policy allows the Board to consider the specific needs of the institution while giving proper consideration to the bookkeeping system being employed, the qualifications of the audit staff, the audit reporting system, and the satisfaction of legal requirements when establishing the audit program.

The management of each financial institution must decide the most effective audit technique which best fits their overall management plan. Every financial institution shall have an audit of its books and records performed in accordance with the requirements contained in the Official Code of Georgia Annotated and the Rules of the Department. It is the Board’s responsibility to contract and appoint with independent audit firms. The audit policy should address the independence of the internal and external audit functions. An internal auditor or audit liaison must be appointed by the Board and charged with implementation of the financial institution's internal audit program. Some management teams may choose to use a qualified in-house internal auditor, while others may choose to employ the services of an independent CPA firm to perform the duties of the internal auditor. Whichever method is utilized, legal restrictions contained in the Official Code of Georgia should be reviewed in detail to ensure complete technical compliance with the provisions contained therein.

When establishing a formal audit program, the following are basic goals which the program should attain:

1. The audit program should provide assurance that the records are being posted (by whatever means employed) in an accurate, timely, safe, and sound manner;

2. The audit program should have provisions which help monitor the operating procedures being practiced;

4. The audit program should ensure that there is proper adherence to all management policies and established procedures as well as all applicable laws and regulations; and

5. The audit program should establish a robust tracking report that includes all findings and exceptions from internal audits, external audits, regulatory findings, and third party review findings. The tracking report should detail expected time frames for corrective action, personnel responsible for corrective action, and ongoing reporting requirements to the Board.

Specific elements of the internal audit function should include:

Risk Assessment: A risk assessment identifies the institution's business activities and their associated risks. These assessments typically analyze the risks inherent in a given business line, the mitigating control processes, and the resulting residual risk exposure of the institution. They should be updated regularly to reflect changes to the system of internal control or work processes, and to incorporate new lines of business. The risk assessment is a key component to develop the audit scope.

Audit Plan: An internal audit plan is based on the control risk assessment and typically includes a summary of key internal controls within each significant business activity, the timing and frequency of planned internal audit work, and a resource budget.

Audit Program: An internal audit program describes the objectives of the audit work and lists the procedures that will be performed during each internal audit review.

Audit Report: An audit report generally presents the purpose, scope, and results of the audit, including findings, conclusions, and recommendations.

Workpapers: Workpapers that document the work performed and support the audit report should be maintained or the financial institution should have contractual access to the documents.

Staff Expertise and Resources: The internal audit function should be competently supervised and staffed by people with sufficient expertise and resources to identify the risks inherent in the institution's operations and assess whether internal controls are effective.

Organizational Structure: The Board should determine the organizational structure that will oversee the internal audit program. The Board is strongly encouraged to establish an audit committee, consisting of outside directors. The audit committee, if established, should oversee the internal audit function, evaluate performance, and report to the Board. The organizational structure should be positioned so that the internal audit function is independent from undue management influence.

Outsourcing Considerations: Even when outsourcing vendors provide internal audit services, the Board is responsible for ensuring that both the system of internal control and the internal audit function operate effectively. In any outsourced internal audit arrangement, the Board must maintain ownership of the internal audit function and provide active oversight of outsourced activities. When negotiating the outsourcing arrangement, an institution should carefully consider its current and anticipated business risks in setting each party's internal audit responsibilities. The outsourcing arrangement should not increase the risk that a breakdown of internal control will go undetected. To clearly distinguish its duties from those of the outsourcing vendor, the institution should have a written contract, often taking the form of an engagement letter. If the same firm is used to perform internal and external audit work, the audit committee and/or the Board should document both that it has pre-approved the internal audit outsourcing to its external auditor and has considered the independence issues associated with the arrangement.

The responsibility for the quality of an audit program ultimately rests with the Board. The Board must periodically review and make determinations concerning the qualifications of the auditor, the scope of the audit, the frequency of the various audit functions, and the techniques to be utilized. It is very important that the financial institution audit be reported directly to the Board or a committee thereof. This point should be stated in the audit policy to provide the audit independence needed to be effective and ensure the Board is fully informed.

CONFLICTS OF INTEREST POLICY

The primary purpose of a written conflicts of interest policy is to manage potential risk and liability from the conduct of the affairs of the financial institution. This risk is usually manifested in the conduct of directors, officers, and employees in discharging their duties and responsibilities in the management of the affairs of the financial institution. The Board of Directors should adopt a policy to avoid even the appearance of a conflict of interest by its directors, officers, and employees when performing their fiduciary duties of care and loyalty to the financial institution. The Conflict of Interest Policy shall address the following situations or circumstances which should be avoided and/or reported by directors, officers, employees, and/or principal stockholders to the Board:

1. Personal interest, direct or indirect, in any assets, real or personal, owned by the financial institution, either purchased from or sold to the financial institution without the prior approval of the Board.

2. Report ownership interest held in the form of "business trusts" or other entities including disclosure of the identity or personal guarantees of the principals.

3. Loans or other transactions in which the officer, director, or principal stockholder (or immediate family member of each) of the financial institution receives or holds a beneficial interest.

4. Loans or other transactions in which the officer, director, or principal stockholder (or immediate family member of each) of another depository institution receives or holds a beneficial interest.

5. Loans or other transactions at any depository institution in which an officer, director, or principal stockholder (or immediate family member of each) holds a beneficial interest, either direct or indirect.

6. Loans or other transactions at any depository institution in which an officer, director, or principal stockholder (or immediate family member of each) has no direct interest but which involve parties with whom an insider has other partnership or business associations.

7. Loans extended personally by officers, directors, or principal stockholders (or immediate family member of each) to parties who are also borrowers from the financial institution or loans extended personally by any borrowing customers to an officer, director, or principal stockholder of the financial institution.

8. Written procedures for notification to the Board or any committee when asked to review a loan approval request or other transaction in which an officer, director, or

principal stockholder may be involved.

9. Prohibition for directors and officers to make or participate in voting on a loan or other transaction where there is a financial interest in the transaction.

10. At least annually directors, officers, and principal shareholders shall disclose their business interests and individuals and customers that they also do business with.

11. Directors, officers, principal stockholders, and their related interest shall conduct all transactions with the financial institution in compliance with State law and Federal law, including Regulation O of the Federal Reserve Board.

12. Directors, officers, employees, principal stockholders, and their related interest will not engage in activities in competition with the financial institution.

13. Establish procedures and practices designed to prevent conflicts of interest and self-dealing by directors, officers and employees, with respect to using confidential or other inside information in making investment decisions; using voting power as a shareholder; and authority of their position when exercising their duties in the conduct of affairs of the financial institution.

The above practices and procedures should be adopted to limit any exposure, to avoid losses and to prevent violations of civil and criminal laws while conducting the affairs of the financial institution.

INTERBANK LIABILITY POLICY

The Board should adopt written policies and procedures to prevent excessive exposure to any individual correspondent financial institution in relation to the condition of the correspondent, and to monitor the financial condition of those entities. Federal Reserve Regulation F is made applicable to state nonmember financial institutions by Section 18(j) of the FDIC Act. Policy consideration should include:

- Standards for selection correspondent financial institutions;
- Periodic review of the financial condition of correspondent financial institutions;
- Reliance on another party, such as a financial institution rating agency or the financial institution's holding company, to assess the financial condition of correspondence financial institutions, provided the financial institution's Board has reviewed and approved the general assessment used by that party;
- Establish internal limits on exposure to the correspondent financial institution;
- Transactions shall be structured with the correspondent financial institution to monitor exposure to the correspondent;
- Establish appropriate procedures to address compliance with internal limits; and
- Establish procedures for periodic review and approval of policies by the Board.

ELECTRONIC BANKING POLICY

Electronic Banking (e-banking) is defined as the automated delivery of new and traditional banking products and services directly to customers through electronic, interactive communication channels. E-banking includes the systems that enable financial institution customers, individuals, or businesses, to access accounts, transact business, or obtain information on financial products and services through a public or private network, including the Internet. Customers access e-banking services using an intelligent electronic device. While the risks and controls are similar for various e-banking access channels, this policy focuses specifically on Internet-based services due to the Internet's widely accessible public network. The Board of Directors (Board) and senior management should develop policies and procedures that mitigate the risks of e-banking. The extent of the financial institution's risk management program should be commensurate with the complexity and sophistication of the activities in which it engages.

Websites

Informational Websites

Informational websites provide customers access to general information about the financial institution and its products or services. Management should have policies and procedures that identify the risk management issues of informational websites. The issues may include the following:

- Potential liability and consumer violations for inaccurate or incomplete information about products, services, and pricing presented on the website;
- Potential access to confidential financial institution or customer information if the website is not properly isolated from the financial institution's internal network;
- Potential liability for spreading viruses and other malicious code to computers communicating with the institution's website; and
- Negative public perception if the institution's on-line services are disrupted or if its website is defaced or otherwise presents inappropriate or offensive material.

Transactional Websites

Transactional websites provide customers with the ability to conduct transactions through the financial institution's website by initiating banking transactions or buying products and services. Banking transactions can range from something as basic as a retail account balance inquiry to a large business-to-business funds transfer. E-banking services, like those delivered through other delivery channels, are typically classified based on the type of customer they support.

Since transactional websites typically enable the electronic exchange of confidential customer information and the transfer of funds, services provided through these websites expose a financial institution to higher risk than basic informational websites. Wholesale e-banking systems typically expose financial institutions to the highest risk per transaction, since commercial transactions usually involve larger dollar amounts. In addition to the risk issues associated with informational websites, management should consider the following risk issues:

- Security controls for safeguarding customer information;
- Authentication processes necessary to initially verify the identity of new customers and authenticate existing customers who access e-banking services;
- Liability for unauthorized transactions;
- Losses from fraud if the institution fails to verify the identity of individuals or businesses applying for new accounts or credit on-line;
- Possible violations of laws or regulations pertaining to consumer privacy, anti-money laundering, anti-terrorism, or the content, timing, or delivery of required consumer disclosures; and
- Negative public perception, customer dissatisfaction, and potential liability resulting from failure to process third-party payments as directed or within specified time frames, lack of availability of on-line services, or unauthorized access to confidential customer information during transmission or storage.

E-Banking Components

E-banking systems can vary significantly in their configuration depending on a number of factors. Financial institutions should choose their e-banking system configuration, including outsourcing relationships, based on four factors:

- Strategic objectives for e-banking;
- Scope, scale, and complexity of equipment, systems, and activities;
- Technology expertise; and
- Security and internal control requirements.

E-Banking Support Services

In addition to traditional banking products and services, financial institutions can provide a variety of services that have been designed or adapted to support e-commerce. Management should understand these services and the risks they pose to the institution. Some of the most common support services are weblinking, account aggregation, electronic authentication, website hosting, payments for e-commerce, and wireless banking activities. Management should develop policies and procedures that address e-banking support services.

Weblinking

A weblink is a word, phrase, or image on a webpage that contains coding that will transport the viewer to a different part of the website or a completely different website by clicking the link. While weblinks are a convenient and accepted tool in website design, their use can present certain risks. Generally, the primary risk posed by weblinking is that viewers can become confused about whose website they are viewing and who is responsible for the information, products, and services available through that website.

Account Aggregation

Account aggregation is a service that gathers information from many websites, presents that information to the customer in a consolidated format, and, in some cases, may allow the customer to initiate activity on the aggregated accounts. The information gathered or aggregated can range from publicly available information to personal account information (e.g., credit card, brokerage, and banking data). Aggregation services can improve customer convenience by avoiding multiple log-ins and providing access to tools that help customers analyze and manage their various account portfolios. Some aggregators use the customer-provided user IDs and passwords to sign in as the customer. Once the customer's account is accessed, the aggregator copies the personal account information from the website for representation on the aggregator's site (i.e., "screen scraping"). Other aggregators use direct data-feed arrangements with website operators or other firms to obtain the customer's information. Generally, direct data feeds are thought to provide greater legal protection to the aggregator than does screen scraping.

Financial institutions are involved in account aggregation both as aggregators and as aggregation targets. Risk management issues management should consider when reviewing aggregation services include:

- Protection of customer passwords and user IDs - both those used to access the institution's aggregation services and those the aggregator uses to retrieve customer information from aggregated third parties - to assure the confidentiality of customer information and to prevent unauthorized activity;
- Disclosure of potential customer liability if customers share their authentication information (i.e., IDs and passwords) with third parties; and
- Assurance of the accuracy and completeness of information retrieved from the aggregated parties' sites, including required disclosures.

Electronic Authentication

Verifying the identities of customers and authorizing e-banking activities are integral parts of e-banking financial services. Since traditional paper-based and in-person identity authentication methods reduce the speed and efficiency of electronic transactions, financial institutions have adopted alternative authentication methods, including:

- Passwords and personal identification numbers (PINs);
- Digital certificates using a public key infrastructure (PKI);
- Microchip-based devices such as smart cards or other types of tokens;
- Database comparisons (e.g., fraud-screening applications);
- Multi-factor authentication; and
- Biometric identifiers.

The authentication methods listed above vary in the level of security and reliability they provide and in the cost and complexity of their underlying infrastructures. As such, the choice of which technique(s) to use should be commensurate with the risks in the products and services for which they control access.

Website Hosting

Some financial institutions host websites for both themselves as well as for other businesses. Financial institutions that host a business customer's website usually store, or arrange for the storage of, the electronic files that make up the website. These files are stored on one or more servers that may be located on the hosting financial institution's premises. Website hosting services require strong skills in networking, security, and programming. The technology and software change rapidly. Institutions developing websites should monitor the need to adopt new interoperability standards and protocols such as Extensible Mark-Up Language (XML) to facilitate data exchange among the diverse population of Internet users.

Risk issues management should consider when reviewing website hosting services include damage to reputation, loss of customers, or potential liability resulting from:

- Downtime (i.e., times when website is not available) or inability to meet service levels specified in the contract;
- Inaccurate website content (e.g., products, pricing) resulting from actions of the institution's staff or unauthorized changes by third parties (e.g., hackers);
- Unauthorized disclosure of confidential information stemming from security breaches; and

- Damage to computer systems of website visitors due to malicious code (e.g., virus, worm, active content) spread through institution-hosted sites.

Payments for E-Commerce

Many businesses accept various forms of electronic payments for their products and services. Financial institutions play an important role in electronic payment systems by creating and distributing a variety of electronic payment instruments, accepting a similar variety of instruments, processing those payments, and participating in clearing and settlement systems. However, increasingly, financial institutions are competing with third parties to provide support services for e-commerce payment systems. Among the electronic payments mechanisms that financial institutions provide for e-commerce are automated clearing house (ACH) debits and credits through the Internet, electronic bill payment and presentment, electronic checks, e-mail money, and electronic credit card payments.

Most financial institutions permit intrabank transfers between a customer's accounts as part of their basic transactional e-banking services. However, third-party transfers - with their heightened risk for fraud - often require additional security safeguards in the form of additional authentication and payment confirmation.

Wireless E-Banking

Wireless banking is a delivery channel that can extend the reach and enhance the convenience of Internet banking products and services. Wireless banking occurs when customers access a financial institution's network(s) using cellular phones or other similar devices through telecommunication companies' wireless networks. Wireless banking services in the United States typically supplement a financial institution's e-banking products and services.

As institutions offer wireless banking services to customers, they should consider the risks and necessary risk management controls to address security, authentication, and compliance issues.

E-Banking Risks

E-banking has unique characteristics that may increase an institution's overall risk profile and the level of risks associated with traditional financial services. E-banking policies and procedures should consider the applicable risk that derive from operational risk, liquidity risk, market risk, legal risk, strategic risk, and reputation risk.

Transaction/Operations Risk

Transaction/Operations risk arises from fraud, processing errors, system disruptions, or other unanticipated events resulting in the institution's inability to deliver products or services. This risk exists in each product and service offered. The level of transaction risk is affected by the structure of the institution's processing environment, including the types of services offered and the complexity of the processes and supporting technology.

Liquidity, Interest Rate, Price/Market Risks

Funding and investment-related risks could increase with an institution's e-banking initiatives depending on the volatility and pricing of the acquired deposits. The Internet provides institutions with the ability to market their products and services globally. Internet-based advertising programs can effectively match yield-focused investors with potentially high-yielding deposits. However, Internet-originated deposits have the potential to attract customers who focus exclusively on rates and may provide a funding source with risk characteristics similar to brokered deposits. An institution can control this potential volatility and expanded geographic reach through its deposit contract and account opening practices, which might involve face-to-face meetings or the exchange of paper correspondence. The institution should modify its policies as necessary to address the following e-banking funding issues:

- Potential increase in dependence on brokered funds or other highly rate-sensitive deposits;
- Potential acquisition of funds from markets where the institution is not licensed to engage in banking, particularly if the institution does not establish, disclose, and enforce geographic restrictions;
- Potential impact of loan or deposit growth from an expanded Internet market, including the impact of such growth on capital ratios; and
- Potential increase in volatility of funds should e-banking security problems negatively impact customer confidence or the market's perception of the institution.

Compliance/Legal Risks

Compliance and legal issues arise out of the rapid growth in usage of e-banking and the differences between electronic and paper-based processes. E-banking is a new delivery channel where the laws and rules governing the electronic delivery of certain financial institution products or services may be ambiguous or still evolving. Specific regulatory and legal challenges include:

- Uncertainty over legal jurisdictions and which state's or country's laws govern a specific e-banking transaction;
- Delivery of credit and deposit-related disclosures/notices as required by law or regulation;
- Retention of required compliance documentation for on-line advertising, applications, statements, disclosures and notices; and
- Establishment of legally binding electronic agreements.

Laws and regulations governing consumer transactions require specific types of disclosures, notices, or record keeping requirements. These requirements also apply to e-banking, and federal banking agencies continue to update consumer laws and regulations to reflect the impact of e-banking and on-line customer relationships.

Strategic and Reputation Risk

A financial institution's Board and management should understand the risks associated with e-banking services and evaluate the resulting risk management costs against the potential return on investment prior to offering e-banking services. Poor e-banking planning and investment decisions can increase a financial institution's strategic risk. Early adopters of new e-banking services can establish themselves as innovators who anticipate the needs of their customers, but may do so by incurring higher costs and increased complexity in their operations. Conversely, late adopters may be able to avoid the higher expense and added complexity, but do so at the risk of not meeting customer demand for additional products and services. In managing the strategic risk associated with e-banking services, financial institutions should develop clearly defined e-banking objectives by which the institution can evaluate the success of its e-banking strategy. In particular, financial institutions should pay attention to the following:

- Adequacy of management information systems (MIS) to track e-banking usage and profitability;
- Costs involved in monitoring e-banking activities or costs involved in overseeing e-banking vendors and technology service providers;
- Design, delivery, and pricing of services adequate to generate sufficient customer demand;
- Retention of electronic loan agreements and other electronic contracts in a format that will be admissible and enforceable in litigation;
- Costs and availability of staff to provide technical support for interchanges involving multiple operating systems, web browsers, and communication devices;
- Competition from other e-banking providers; and
- Adequacy of technical, operational, compliance, or marketing support for e-banking products and services.

Board and Management Oversight

The Board and senior management are responsible for developing the institution's e-banking business strategy, which should include:

- The rationale and strategy for offering e-banking services including informational, transactional, or e-commerce support;

- A cost-benefit analysis, risk assessment, and due diligence process for evaluating e-banking processing alternatives including third-party providers;
- Goals and expectations that management can use to measure the e-banking strategy's effectiveness; and
- Accountability for the development and maintenance of risk management policies and controls to manage e-banking risks and for the audit of e-banking activities.

Managing Outsourcing Relationships

The Board and senior management must provide effective oversight of third-party vendors providing e-banking services and support. Effective oversight requires that institutions ensure the following practices are in place:

- Effective due diligence in the selection of new service providers that considers financial condition, experience, expertise, technological compatibility, and customer satisfaction;
- Written contracts with specific provisions protecting the privacy and security of an institution's data, the institution's ownership of the data, the right to audit security and controls, and the ability to monitor the quality of service, limit the institution's potential liability for acts of the service provider, and terminate the contract;
- Appropriate processes to monitor vendor's ongoing performance, service quality, security controls, financial condition, and contract compliance; and
- Report Monitoring and establishing expectations including incidence response and notification.

Information Security Program

E-banking introduces information security risk management challenges. Financial institution directors and senior management should ensure the information security program addresses these challenges and takes the appropriate actions.

- Ensure compliance with the "Guidelines Establishing Standards for Safeguarding Customer Information" as issued pursuant to section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLBA).
- Ensure the institution has the appropriate security expertise for its e-banking platform.
- Implement security controls sufficient to manage the unique security risks confronting the institution. Control considerations include:
    - Ongoing awareness of attack sources, scenarios, and techniques;
    - Up-to-date equipment inventories and network maps;

    - Rapid identification and mitigation of vulnerabilities;
    - Network access controls over external connections;
    - Hardened systems with unnecessary or vulnerable services or files disabled or removed;
    - Use of intrusion detection tools and intrusion response procedures;
    - Physical security of all e-banking computer equipment and media; and
    - Baseline security settings and usage policies for employees accessing the e-banking system or communicating with customers.
- Use verification procedures sufficient to adequately identify the individual asking to conduct business with the institution.
- Use authentication methods sufficient to verify individuals are authorized to use the institution's systems based on the sensitivity of the data or connected systems.
- Develop policies for notifying customers in the event of a security breach effecting their confidential information.
- Monitor and independently test the effectiveness of the institution's security program.

Administrative Controls

E-banking presents new administrative control requirements and potentially increases the importance of existing controls. Management must evaluate administrative controls to maximize the availability and integrity of e-banking systems. E-banking information can support identity theft for either fraud at the subject institution or for creating fraudulent accounts at other institutions. The institution’s policy and procedures should consider the adequacy of the following controls:

- Segregation of e-banking duties to minimize the opportunity for employee fraud;
- Dual-control procedures especially for sensitive functions like encryption key retrieval or large on-line transfers;
- Reconcilement of e-banking transactions;
- Suspicious activity reviews and fraud detection with targeted review of unusually large transaction amounts or volumes;
- Periodic monitoring to detect websites with similar names, possibly established for fraudulent purposes;

- Error checks and customer guidance to prevent unintentional errors;
- Alternate channel confirmations to ensure account activity or maintenance changes are properly authorized; and
- Business disruption avoidance strategies and recovery plans.

Legal and Compliance Issues

E-banking limits face-to-face interaction and the paper-based exchange of information with customers and therefore, introduces new compliance or legal risks. The following legal and compliance issues should be addressed:

- Clearly identify the official name of the financial institution providing the e-banking services;
- Properly disclose customer privacy and security policies on websites; and
- Ensure that advertisements, notices, and disclosures are in compliance with applicable statutes and regulations, including the E-Sign Act.

Additional Guidance can be found in the FFIEC IT Handbook

RETAIL PAYMENT SYSTEMS

Retail payments usually involve transactions between two consumers, between consumers and businesses, or between two businesses. Wholesale payments are typically made between businesses. Although there is no definitive division between retail and wholesale payments, retail payment systems generally have higher transaction volumes and lower average dollar values than wholesale payment systems. This policy provides background information on payments typically classified as retail payments. The following are examples of typical retail payments. These retail payments may involve the use of various retail payment instruments or access devices (e.g., checks, ACH, card, phones, etc.).

Retail Payment Systems Risk Management

Financial institutions engaged in retail payment systems should establish an appropriate risk management process that identifies, measures, monitors, and limits risks.

Management and the Board should manage and mitigate the identified risks through effective internal and external audit, physical, and logical information security, business continuity planning, vendor management, operational controls, and legal measures.

Risk management strategies should reflect the nature and complexity of the institution's participation in retail payment systems, including any support they offer to clearing and settlement systems. Management should develop risk management processes that capture not only operational risks, but also credit, liquidity, strategic, reputational, legal, and compliance risks, particularly as they engage in new retail payment products and systems. Management should also develop an enterprise wide view of retail payment activities due to cross-channel risk. These risk management processes should consider the risks posed by third-party service providers.

Financial institutions should tailor their risk management strategies to the nature and complexity of their participation in retail payment systems, including any support they offer to clearing and settlement systems. Financial institutions must comply with federal and state laws and regulations, as well as with operating rules of clearing houses and bankcard networks. From the initiation of a retail payment transaction to its settlement, financial institutions are exposed to certain risks. For individual retail payment transactions, risks resulting from compliance issues and potential operational failures including fraud are always present. Operational failures can increase costs, reduce earnings opportunities, and impair an institution's ability to reflect its financial condition accurately. Participation in retail payment systems may expose financial institutions to credit, liquidity, and operational risk, particularly during settlement activities. In addition, a financial institution's credit, liquidity, and operational risks may be interdependent with payment system operators and third parties.

Retail Payment Instrument Specific Risk Management Controls

Specific retail payment instruments introduce risks that require effective internal controls and adherence to the relevant clearing house, association, interchange, and regulatory requirements. Financial institutions should address these risks in their Information Security Policy and business continuity planning programs.

Checks

Financial institutions manage the risk exposure to check payment processing by establishing appropriate account opening and monitoring controls. Account opening controls that incorporate information from credit bureau services may mitigate credit risk exposure to criminals and to customers with a history of financial problems. Such screening is also the basis for customer verification in support of BSA/AML compliance and for qualifying customers for Remote Deposit Capture (RDC). Institutions should perform a credit assessment of those customers for whom they collect large dollar volumes of checks.

Financial institutions use a variety of monitoring tools during check processing as a means of identifying potential fraudulent activity or for early detection of kiting. These automated tools are typically available from major vendors. Institutions should monitor the payment activity of their customers and take appropriate action when credit limits are exceeded or when their business practices may indicate possible fraud or money laundering activity. Institutions that offer commercial customers services for RDC should make such arrangements under contracts that clearly state the liability of the commercial customer in the event of a dispute over the imaged checks.

Automated Clearing House

ACH operations pose a variety of risks including credit, liquidity, and operational. NACHA and the two national ACH operators (the Reserve Banks and EPN) have clear expectations that financial institutions will manage these risks, particularly when the institutions engage in riskier ACH activities. In recent years, the ACH operators have begun to offer a variety of risk management tools to help control ACH risks. Financial institutions should employ those tools that are commensurate with the risks taken.

The risk of fraud can be mitigated through proper due diligence for all originating customers and strict adherence to ACH and credit policies. Additional mitigation can be achieved by adequately assessing high risk businesses and customers. Limits should be appropriate for the risks of each customer and the use of pre-funding arrangements or reserves can be effective in controlling losses. Management should review monitoring reports offered by the ACH operators that can assist in early detection of unauthorized ACH transactions.

Third-Party ACH Processing

While a financial institution's responsibilities do not change with the use of a technology service provider for ACH processing, its risk exposure may increase as a result of the servicer's direct access to an ACH operator. A Technology Service Provider (TSP) may transmit ACH transactions directly to an ACH operator using the ODFI routing number. However, it is the ODFI that warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized all entries. To reduce risk to all parties, the financial institution should establish controls over TSP operations, and the ODFI should maintain control over its settlement accounts.

The financial institution should review and assess all audits of its service provider's internal controls. NACHA rules also require the ODFI to have contractual agreements with third-party senders specifying that the third-party sender is in compliance with NACHA rules and applicable laws and regulations. NACHA rules further require the ODFI to have an agreement with a TSP that has direct access to an ACH operator. NACHA specifies that the agreement sets out the rights and responsibilities of all parties, including:

- A requirement that the third-party service provider obtain the prior approval of the ODFI before originating ACH transactions for originators under the ODFI routing number. ODFI approval of each originator should be contingent upon the creditworthiness of the originator and the execution of an originator and ODFI agreement.

- ODFI dollar limits for files that a TSP deposits with the ACH operator. The service provider should notify the ODFI of any file exceeding established dollar limits before depositing the file at the ACH operator so that the ODFI can either approve it as an exception or hold it until the next business day.

- A provision that restricts the TSP's ability to initiate corrections to files already transmitted to the ACH operator. The ODFI should restrict correction capability. If the TSP has the ability to make file corrections, the ODFI should authorize and approve any changes to the file totals before the ACH operator releases the file for processing.

- A requirement that a third-party sender who enters into an agreement with an ODFI establish the identity of each originator using commercially reasonable methods, warrant that the originators will assume their responsibilities under NACHA rules, and warrant that it will assume the liabilities of the ODFI. The lack of a direct relationship between the ODFI and the originator poses a risk to the ODFI. The ODFI should conduct proper due diligence, establish exposure limits, and employ other monitoring procedures to ensure that the business practices of the third- party sender and its merchant clients do not create an undue risk to the ODFI. The ODFI should be able to substantiate that the third-party sender has sufficient creditworthiness to back the warranties it makes relative to the risk, nature, and volume of ACH transactions; the underlying originators; and the exposure duration.

NACHA also requires participating financial institutions to conduct annual audits of their ACH operations to assess compliance with NACHA rules.

Credit Cards

Credit and fraud losses are two of the most significant credit card-related risks to a financial institution. Credit card charge-offs represent many credit losses due to contractual delinquency and bankruptcy. Fraud includes unauthorized use of lost or stolen cards, fraudulent applications, counterfeit or altered cards, and the unauthorized use of a cardholder's credit card number for card-not-present transactions.

A control method financial institutions use to reduce risk is the authorization process to approve the credit transaction. The institution should also implement preventative controls to deter fraud and detective controls to identify and respond to fraud once it has occurred. Employing the appropriate underwriting, account management, monitoring, and collection practices can mitigate credit risk. By setting standards that reduce the probability of delinquency and fraud, financial institutions can more effectively control credit losses.

Debit/ATM Cards

A significant risk with PIN or signature-based debit or ATM cards is that unauthorized individuals will obtain them and make fraudulent transactions. Financial institutions and their technology service providers should mitigate these risks by executing financial institution-merchant and financial institution-customer contracts that delineate each party's liabilities and responsibilities. Institutions should also establish adequate physical safeguards including the installation of surveillance cameras and access/entry control devices.

ATM stand-in arrangements, which enable EFT/POS networks to authorize transactions if a card issuer or processor is unable to authorize and process transactions, also increase the potential for fraud since normal credit limit and authorization procedures are not in effect. Stand-in authorization arrangements should include reasonable credit limits and defined terms of duration to limit potential financial loss.

Card/PIN Issuance

Financial institutions also assume certain fraud-related risks when issuing credit, debit, and ATM cards either in-house or under contract to third parties. Inadequate internal controls or ineffective card and PIN issuance procedures may result in fraudulent customer transactions. Inappropriate separation of duties that allow employees access to both customer account and PIN information expose the institution to potential employee fraud.

Merchant Acquiring

Merchants that accept card association-branded credit card sales payments must be sponsored by an acquiring bank that is a member of the credit card association. Merchants may maintain a settlement account with their acquiring bank, or settle via ACH transactions between the acquiring bank and the merchant's bank. Acquiring banks typically do not process their merchants' transactions directly so this function may be outsourced to a third-party service provider (merchant acquirer) that performs the data processing functions of authorization and clearing and settlement. Some merchant banks may also engage the services of an ISO or Member Service Provider (MSP) to solicit and sign up merchants and merchant transaction processing services. Regardless of the presence of such third parties, the credit card networks expect the acquiring bank to be the risk-controlling entity throughout the credit card process.

The credit card associations require acquiring banks to ensure that their merchants and third-party service providers comply with the Payment Card Industry Data Security Standards (PCI DSS). For third-party service providers and large merchants, PCI DSS compliance validation must be performed annually by a Qualified Security Assessor that has been approved by the PCI Security Standards Council. Smaller merchants must validate compliance annually through completion of a self-assessment questionnaire. It is not uncommon within the industry for a large number of merchants, and even some third-party service providers, to be in noncompliance with PCI DSS, potentially exposing their acquiring bank to reputation risk and financial loss from fraud, lawsuits, and fines. Additionally, issuing banks that use third-party service providers for transaction processing are required by the card associations to ensure that their providers are in compliance with PCI DSS.

EFT/POS and Credit Card Networks

Financial institutions should have accurate audit trails for all transactions at each network switch point. The audit trails should identify the originating terminal and destination. To ensure accurate transaction posting, the financial institutions should have adequate procedures in place to control transaction activity if the EFT/POS network becomes inoperable. Also, financial institutions should document and monitor procedures for balancing and settling transactions to ensure that they adhere to interchange policies. Each participant in the switch should receive adequate transaction journals and exception reports necessary to facilitate final settlement for the institution.

A financial institution should establish stand-in processing arrangements with peer financial institutions as part of its disaster recovery and business continuity plans to ensure availability of the service. Additionally, adequate oversight and contract provisions for all outsourced services to ensure continuity of expected service levels should be implemented. Agreements between switch or network participants should delineate each party's liabilities and responsibilities. The agreements should detail basic control items concerning normal and contingency processing and assign responsibility for corrective action. Grievance procedures and arbitration policies are also an important part of participant agreements.

Other Payment Channels

Internet and Telephone-Initiated ACH

Financial institutions originating ACH debit entries through the Internet should ensure they are in compliance with NACHA requirements. NACHA rules establish a WEB standard entry class (SEC) code for Internet-initiated ACH debit entries to which a number of requirements apply. The rules apply to originators and also affect the ODFI and its service providers. Under these rules, financial institutions must use the WEB SEC code to identify all ACH debit entries to consumer accounts that a receiver authorizes through the Internet. This code applies to both recurring and single entry ACH debits. In addition, an ODFI that transmits WEB entries must warrant that its originators have met certain NACHA standards.

Financial institutions offering TEL origination services on behalf of their customers are exposed to substantial risk from merchants that may be engaged in fraudulent or deceptive business practices. Therefore, these institutions should adopt applicable NACHA risk management practices.

Online Person-to-Person (P2P), Account-to-Account (A2A) Payments and Electronic Cash

Electronic payments include person-to-person, account-to-account, electronic cash, and electronic benefit transfers. These payment instruments are usually associated with an established consumer deposit account and facilitate consumer access to recurring or one-time debit and credit transactions and a variety of federal, state, and local government benefit programs.

Contactless Payment Cards, Proximity Payments and Other Devices

Contactless cards and key fobs have an embedded computer chip with financial and personal information used for payment transactions, and they employ RFID technology for payment transmission. The contactless cards include a microcontroller (or equivalent intelligence) and internal memory and have the ability to secure, store, and provide access to data on the card. The microcontroller also supports the use of improved security features including authenticated information access and information privacy.

Proximity payments are POS transactions made with a mobile device like a cellular telephone, smart card, or virtually any device that can house a microchip. Many of these transactions use the same credit/debit card network, and provide lower costs to institutions and to merchants.

Mobile Financial Services

Mobile financial services (MFS) are the products and services that a financial institution provides to its customers through mobile devices. The mobile channel provides an opportunity for financial institutions of all sizes to increase customer access to financial services and decrease costs. Although the risks from traditional delivery channels for financial services continue to apply to MFS, the risk management strategies may differ. As with other technology-related risks, management should identify, measure, mitigate, and monitor the risks involved and be familiar with technologies that enable MFS.

WHOLESALE PAYMENT SYSTEMS

This policy provides guidance for financial institution management regarding the risks and risk-management practices when originating and transmitting large-value payments. There are two primary networks for interbank, or large-value, domestic funds transfer payment orders. The first, Fedwire Funds Service, is operated by the Federal Reserve Banks, and is an important participant in providing interbank payment services, as well as safekeeping and transfer services for U.S. government and agency securities, and mortgage-backed securities. Funds Service and the Federal Reserve's National Settlement Service (NSS) are critical components used in other payment systems' settlement processes. The Clearing House Interbank Payments Company L.L.C. (CHIP Co.) operates the second, the Clearing House Interbank Payments System (CHIPS).

Fedwire Funds Service

Fedwire Funds Service is a real-time gross settlement system (RTGS) enabling participants to transmit and receive payment orders between each other and on behalf of their customers. Real-time gross settlement means that the clearing and settlement of each transaction occurs continuously during the processing day. Payment to the receiving participant (payee) over Fedwire Funds Service is final and irrevocable when the Federal Reserve Bank either credits the amount of the payment order to the receiving participant's Federal Reserve Bank reserve account or sends notice to the receiving participant, whichever is earlier.

CHIPS

CHIPS is a privately operated, real-time, multilateral, payments system typically used for large dollar payments. CHIPS is owned by financial institutions, and any banking organization with a regulated U.S. presence may become an owner and participate in the network. The payments transferred over CHIPS are often related to international interbank transactions, including the dollar payments resulting from foreign currency transactions (such as spot and currency swap contracts) and Euro placements and returns. Payment orders are also sent over CHIPS for the purpose of adjusting correspondent balances and making payments associated with commercial transactions, bank loans, and securities transactions.

Other Clearinghouse, Settlement, and Messaging Systems

National Settlement Service (NSS)

NSS is a multilateral settlement service owned and operated by the Federal Reserve Banks. It allows participants in private clearing arrangements to settle their net obligations with same-day finality using participant's reserve or clearing account balances maintained at the Federal Reserve Banks. NSS participants include local check clearinghouse associations, automated clearinghouse (ACH) networks, credit card processors, and automated teller machine (ATM) networks.

Society for Worldwide Interbank Financial Telecommunication (SWIFT)

International funds transfer operates differently from domestic large-value funds transfer. While the SWIFT operates as a messaging system, transmitting instructions to move funds, the domestic systems discussed above accomplishes the actual funds movement.

Operational Risk

Internal and Operational Controls

Management should consider implementing a variety of specific measures to mitigate or limit operational risks, such as authentication and encryption techniques to ensure the authenticity of the payer and payee as well as prevent unauthorized access to information in transit; and edit checks and automated balancing to verify the integrity of the information relative to the payment order and funds transfer transaction. Additional controls include the use of certified tamper resistant equipment, logical access controls to verify transactions, verification of account balances, and the logging of all transactions and attempts to make a transaction.
Additional internal control measures that management should employ to mitigate wholesale payment system risk include:

- Dual custody and separation of duties for critical payment transaction processing and accounting tasks;
- Payment data verification;
- Clear error processing and problem resolution procedures; and
- Confidential and tamper resistant mailing procedures for bankcards and other sensitive material.

The operational controls for funds transfer operations require clearly defined procedures establishing a control environment which provides for the authorization and authentication of transactions. Financial institutions should establish effective operational controls that identify and document:

- The original payment instructions from the corporate or individual customer to the financial institution and other pertinent information (e.g., account officer, branch manager, terminal entry identity, and automated interface identification);
- Every transfer point of data for each step of the manual process (e.g., account officer, message receipt, authentication, data entry, and payment release); and

- Every transfer point of data for each step of an automated process (e.g., SWIFT, message preparation, data entry, and payment release).

Basic internal controls should be in effect to maintain overall integrity for any funds transfer operation. However, depending on the complexity and volume of operations, certain steps may not be applicable for some institutions. Recommended control objectives for a wholesale funds transfer system include:

- Verifying the accuracy and completeness of the outgoing instruction;
- Protecting original instructions from loss or alteration;
- Authenticating the identity and authority of the sender;
- Ensuring collected balances are available and held for the outgoing payments;
- Ensuring the original unaltered outgoing instruction is entered into the internal accounting system;
- Maintaining a physically secure environment; and
- Maintaining appropriate separation of duties for employees involved in the payment process.

Financial institutions should have funds transfer policies and procedures addressing both the processing of funds transfer messages and the related standards for creating and maintaining source documents. Policies and procedures should include documentation describing all interfaces between the funds transfer application and other back office and customer-related banking processes, and should address the controls relating to crediting, debiting, and reconciling customer and institution account balances. Policies and procedures should also document institution specific compliance requirements to address federal and state regulations including OFAC verification procedures.

<u>Audit</u>

A financial institution's internal auditors should conduct periodic independent reviews of the funds transfer operation, including all pertinent internal policies and procedures. An external auditor can supplement internal audit procedures. Financial institution audits should verify the effectiveness of the funds transfer control environment and identify funds transfer deficiencies for correction.

<u>Information Security</u>

A financial institution's information security program should include an effective risk assessment methodology that includes an evaluation of risks relating to performing high-risk activities such as funds transfer and other payment-related activities. Management should use risk assessments based on a periodic review of high-risk activities to develop effective standards for adequate separation of duties, physical security, and logical access controls based on the concept of "least possible privilege."

Business Continuity Planning (BCP)

Financial institutions should recognize their role in supporting systemic financial market processes (e.g., inter-bank payment systems and key market clearance and settlement activities) and understand that service disruptions at their institution may significantly affect the integrity of key financial markets or customer transactions. Business Continuity Plans should by commensurate with the institution's funds transfer activities.

Vendor and Third-Party Management

Some financial institutions rely on third party service providers and other financial institutions for wholesale payment system products and services either to enhance the services performed in-house or to offer wholesale payment services that are otherwise not cost effective. Financial institutions should have adequate due diligence processes, appropriate contract provisions, and service provider monitoring procedures to ensure they conduct wholesale payment operations appropriately. Effective monitoring should include the review of select wholesale payment transactions to ensure they are accurate, reliable, and timely. The integrity and accuracy of wholesale payment transactions depend on the use of proper control procedures throughout all phases of processing, including outsourced functions.

Credit Risk

Customer Daylight Overdrafts

Financial institutions often permit their individual and corporate customers to incur intraday overdrafts by allowing customers to make payments without available balances. In most cases, overdrafts are eliminated with incoming funds transfers from other institutions (or outgoing securities transfers against payment) by the end of the business day.

Financial institutions engaging in this practice are extending credit to their customers. As such, they should monitor the credit position of individual customers; control the amount of intraday credit extended to each customer; and have guidelines to prevent exceeding approved intraday and overnight overdraft limits. These guidelines should include:

- Reviewing customer credit limits and the frequency and scope of internal credit reviews. In the absence of pre-authorized limits, institutions should have a process for management approval of daylight overdrafts. Authorization should be within the lending authority of approving officers and aggregate legal lending limits.

- Reporting and approval procedures for payments exceeding established credit limits to ensure officers with sufficient lending authority make approvals.
- Reviewing intraday overdrafts incurred for compliance with established limits as well as approval and reporting requirements.
- Reviewing arrangements/agreements regarding collateralization of credit exposures.

To the extent that these guidelines give consideration to projected incoming payments, the financial institution should be aware of the risk that expected payments may not be received when expected. Moreover, as described below, institutions should also consider whether such payments have been or are expected to be made with finality.

Since daylight overdrafts constitute an extension of credit (no matter the period of time involved), financial institutions' credit policies should include provisions for approving and monitoring intraday credit lines to customers. Daylight overdrafts have the potential to become overnight overdrafts or overnight loans, and institutions should also have procedures to determine limits on overnight overdrafts. Both sets of procedures should be similar to loan portfolio credit analysis. Credit policies and procedures should include:

- Analyzing worthiness of all borrowers with amounts outstanding in excess of the credit line.
- Reviewing reporting and approval procedures for overdrafts and settlement credits exceeding established limits.
- Assessing reporting and approval procedures for payments against uncollected funds.

Depending on the creditworthiness of the customer and the nature of the activity, a financial institution should consider requiring customers to advise the institution of anticipated incoming securities transfers. Financial institutions should also consider requiring the customer to pre-fund all such anticipated transfers, with the understanding that any transfers not pre-funded may be reversed. To further mitigate credit risk, management should consider requiring customers to collateralize intraday overdrafts.

Settlement Risk

In addition to the explicit provision of credit via daylight overdrafts, financial institutions also need to control their exposure to settlement risks incurred through the institutions' participation in interbank payment and settlement systems. In general, settlement risk is the possibility that the completion or settlement of individual transactions or settlement at the interbank funds transfer or securities settlement level more broadly, will not take place as expected. In addition to credit risk, settlement risk often includes elements of liquidity risk.

Liquidity Risk

Liquidity risk involves the possibility that earnings or capital will be negatively affected by an institution's inability to meet its obligations when they come due. Liquidity risk is the risk that the financial institution cannot settle an obligation for full value when it is due (even if it may be able to settle at some unspecified time in the future). Liquidity problems can result in opportunity costs, defaults in other obligations, or costs associated with obtaining the funds from some other source for some period of time. In addition, operational failures may also negatively affect liquidity if payments do not settle within an expected time period. Until settlement is completed for the day, a financial institution may not be certain what funds it will receive and thus it may not know if its liquidity position is adequate. If an institution overestimates the funds it will receive, even in a system with real-time finality, then it may face a liquidity shortfall. If a shortfall occurs close to the end of the day, an institution could have significant difficulty in raising the liquidity it needs from an alternative source.

To manage and control liquidity risk, it is important for financial institutions to understand the intraday flows associated with their customers' activity to gain an understanding of peak funding needs and typical variations. To smooth a customer's peak credit demands, a depository institution might consider imposing overdraft limits on all or some of its customers. Moreover, institutions must have a clear understanding of all of their proprietary payment and settlement activity in each of the payment and securities settlement systems in which they participate.

Legal (Compliance) Risk

Legal/compliance risk arises from an institution's failure to enact appropriate policies, procedures, or controls to ensure it conforms to laws, regulations, contractual arrangements, and other legally binding agreements and requirements. In particular, legal risks can result if a financial institution does not provide adequate attention to the operating circulars, procedures, and rules of the payment and settlement systems in which it participates. Similarly, an institution's contractual relationships with customers, counterparties, and vendors must be sound and appropriate to the relevant legal framework(s) such as payment and bankruptcy frameworks. Contracts, among financial institutions, their customers, and counterparties are also important to allocate risk-sharing responsibilities applicable to payments. Finally, an institution must ensure it is in compliance with all applicable Federal and State laws and regulations governing payments activity, including the Bank Secrecy Act, the USA PATRIOT Act, and laws regarding economic sanctions.