ABOUND RESOURCES™
Goals Achieved. Guaranteed.

Sample Financial institution

Risk Management Policy

2011

Contents

Risk Management Program

The Board of Directors ("Board") and Management of Sample Credit Union (the "Credit Union") recognizes that the credit union industry is experiencing significant and rapid change, including increased competition from other credit unions, the commercial banking industry and from non-bank financial services firms. The industry is also subject to volatile interest rate changes, changes in banking laws and regulations and technological advances. The Board of Directors and Management further recognize that a comprehensive program is essential to effectively manage the Credit Union's risks.

This document describes the internal control and risk management program of Sample Credit Union. It also describes the management structure, through which the Credit Union will identify, measure, monitor and control risk throughout the Credit Union's operations and in its various products and lines of business.

Internal Control and Risk Management

An effective internal control and risk management program is the foundation of safe and sound banking. When properly designed and consistently enforced, an effective system of internal control will help management safeguard the Credit Union's resources, produce reliable financial reports, and comply with laws and regulations. It will also reduce the possibility of significant errors and irregularities, as well as assist in their timely detection when they do occur. Sample Credit Union's enterprise risk management program is based on the COSO II ERM model, as illustrated in Appendix 1.

General Control Environment

The General Control Environment sets the tone of an organization and influences the control consciousness of its people. It is the foundation for all other components of the system of internal control, providing both discipline and structure. The hallmark of an effective general control environment is the commitment by the Board of Directors and senior management, as evidenced by a number of criteria, including:

- The integrity, ethical values and competence of the organization's people;
- The attention of the Board of Directors, especially the audit and risk management committees, to whether controls are working properly;
- The manner and timeliness in which the Board and management respond to regulatory and audit recommendations and address deficiencies;
- Direction provided by the Board of Directors;
- Assignments of organizational authority and responsibility with a view to maintain appropriate segregation of functional responsibilities;
- The manner in which the Credit Union hires and develops employees;

- Management’s risk assessment, planning and oversight processes;
- Information systems that produce pertinent and timely information in a form that enables employees to carry out their responsibilities;
- Comprehensive, risk-based internal and external audit, compliance and loan review programs; and
- Strong physical and information security programs

A strong General Control Environment is essential to provide a foundation for the management of risk. Without a strong General Control Environment, the effectiveness of specific controls, such as transaction and approval requirements, is diminished. The degree of the organization and Management’s control consciousness is also integral to the success of specific control procedures.

Specific Internal Control Environment

Once a strong General Control Environment has been developed, specific control procedures must be established to manage the frequency and severity of potential losses. These specific controls can be divided into two primary types: Preventive and Detective.

Preventive Controls are designed to provide assurance that only valid transactions are processed and include, as examples, controls like:

- Authorized transaction limits;
- Supervisory approval of transactions;
- Separation and rotation of duties;
- Scheduled and unscheduled transaction review and testing; and
- Password procedures to restrict access to computer systems and information.

Detective Controls are designed to provide reasonable assurance that errors or irregularities are discovered and corrected. They include, for example, controls like:

- Reconciling subsidiary and general ledger balances
- Accounting for the use of prenumbered forms, such as checks and deposit forms
- Reviewing file maintenance and transaction results
- Inventorying cash and negotiable items
- Comparing period-to-period financial results, budgeted-to-actual results and rate-volume analyses

Risk Assessment

An effective internal control program cannot be structured without an understanding of the Credit Union's risks and exposures and an effective risk management process. Risk management is defined as the ability of the Credit Union to identify, measure, monitor and control risks. The Credit Union, through its Board, management and staff, must be able to respond to changing circumstances and to address risks that might arise from changing business or economic conditions, a decline in the effectiveness of internal controls; the initiation of new business activities or the offering of new products and services.

It is important to the success of the Credit Union's risk management efforts that risks be defined consistently throughout the Credit Union in accordance with the following definitions.

1. ***Credit Risk.*** Credit risk is the most recognizable risk associated with banking. Essentially, credit risk is the risk to earnings and capital arising from an obligor's failure to meet the terms of any contract with the Credit Union, or otherwise fail to perform as agreed. This definition, however, encompasses more than the traditional definition associated with lending activities. Credit risk is found in all activities where success depends on counter-party, issuer, or borrower performance. Any time Credit Union funds are extended, committed, invested, or otherwise exposed through actual or implied contractual agreements, whether recorded on the Credit Union's balance sheet or off the balance sheet, the Credit Union is exposed to credit risk. Credit risk may also arise where the performance of guarantors is required. In addition, credit risk arises in conjunction with a broad range of non-lending activities, including selecting and purchasing portfolio investments and processing and settling investment transactions with counter-parties.
2. ***Interest Rate and Market Risk*****.** Interest Rate and Market risk are those risks to a financial institution earnings and asset quality and valuation resulting from adverse movements in market rates or prices, such as interest rates, foreign exchange rates or equity prices. This type of risk focuses on the economic scenarios relative to the value of the Credit Union in the current interest rate environment, and the sensitivity of that value to changes in interest rates. Market risk occurs due to: (1) differences between the timing of rate changes and the timing of cash flows (repricing risk); (2) changing rate relationships among different yield curves affecting Credit Union activities (basis risk); (3) changing rate relationships across the range of maturities (yield curve risk); and (4) interest-related options embedded in Credit Union products (options risk). Valuation of interest rate risk must also consider the potential effect of complex, illiquid hedging strategies, and also the potential effect on fee income, which is sensitive to changes in interest rates. Changes in interest rates may have a significant effect on other areas of risk. For example, market risk can impair the Credit Union's liquidity position. It also potentially affects earnings if the Credit Union is unable to meet its obligations when they come due without incurring unacceptable losses (i.e., liquidating investments that declined in value due to rising interest rates). This type of risk affects the Credit Union's ability to establish new

relationships or services or to continue servicing existing relationships. This risk can expose the Credit Union to litigation, financial loss, or damage to its reputation.

3. ***Liquidity Risk.*** Liquidity risk is the risk to earnings or capital that arises from a Credit Union's inability to meet its obligations when they come due without incurring unacceptable losses. Liquidity risk includes the inability to manage unplanned decreases or changes in funding sources. It also arises from the Credit Union's failure to recognize or address changes in market conditions that affect the ability to liquidate assets quickly and with minimal loss in value. Liquidity risk exposure is present in various funding situations, but primarily deposit and lending activities. Again, interest rate and market risks affect the Credit Union's liquidity position. This type of risk may affect the Credit Union's ability to establish new relationships or services or to continue servicing existing relationships, and can expose the Credit Union to litigation, financial loss, or damage to its reputation.

4. ***Transaction Risk.*** Operational risk arises from the potential that inadequate information systems, operational problems, breaches in internal controls, fraud or unforeseen catastrophes will result in unexpected losses. Operational risk includes both transaction and strategic risk. Transaction risk is the risk to earnings or capital arising from problems with service or product delivery and may include potential financial losses from human error or fraud, incomplete information, and related decision-making or operational disruption. The risk is a function of the adequacy of internal control and information systems, employee integrity, management policies and operating processes. Transaction risk may exist in all products and services. This type of risk ultimately affects the Credit Union's ability to establish new relationships or services or to continue servicing existing relationships, and may result in damage to the Credit Union's reputation.

5. ***Compliance and Legal Risk***. As a publicly chartered institution operating as a major community business organization, the Credit Union, its directors, management, and staff must operate in compliance with a myriad of laws, rules and regulations. Compliance risk arises from violations of or nonconformance with those laws, regulations, or prescribed practices which govern the Credit Union's activities. Legal risk arises from the potential that unenforceable contracts, lawsuits, or adverse judgments can disrupt or otherwise negatively affect the operations or condition of a banking organization. Legal risk also arises from violations of or nonconformance with laws, regulations, prescribed practices or industry standards, or ethical standards. Compliance and legal risks may potentially subject the Credit Union and its directors and officers to fines and civil money penalties by regulators and result in lawsuits by customers and others. Exposure to compliance and legal risks can also dramatically affect the Credit Union's reputation, strategic alternatives, and operations.

6. ***Reputation Risk.*** Reputation risk is the potential that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions, often as a result of poor earnings, regulatory censure, significant fraud or litigation and failure to provide services or products in conformity to the local market. This type of risk affects the Credit Union's ability to establish new relationships or services or to continue servicing existing relationships.

Reputation risk exposure is present throughout the organization and is driven to a large extent by the Credit Union's actions to manage compliance, strategic, credit, interest rate and other risks.

7. ***Strategic Risk***. Strategic risk results from adverse business decisions or the improper implementation of those decisions. This risk is a function of the compatibility of an organization's strategic goals, the business strategies developed to achieve those goals, the resources deployed to support achievement of those goals, and the quality of implementation. Strategic risk includes the misalignment of business and technology strategic plans, the failure to achieve economies of scale in "scale" driven businesses (e.g., mortgage loan servicing, credit card account servicing, etc.) or improper market positioning (e.g., retail delivery strategies, geographic positioning, etc.) and pricing of products and services.

Properly managing these risks is not only critical to the conduct of safe and sound banking activities, but also crucial to the success of the Credit Union.

Enterprise Risk Assessment and Risk/Control Self Assessment

Annually, the Credit Union will prepare an assessment of its business risks. This assessment will begin with an evaluation of "inherent risk." Risks in the seven categories described previously will be evaluated throughout the Credit Union. These risks will be rated as High, Medium or Low. Among factors considered in this assessment of risk will be the inherent level of such risk in the specified business activity, the trend of risk in that activity (e.g., increasing, decreasing or stable), the adequacy of risk measurement and monitoring processes and tools, and the quality of risk management practices and controls in place to control such risks.

The risk control self assessment will be completed by the Risk Officer, Internal Auditor and appropriate business unit managers and will include specific risk issues, identification of the risk category, specific risk mitigating controls and information about these controls, such as where is the requirement of control procedure documented, who performs the control procedure, how often is it performed, where is the result documented, etc. The assessment should identify the most significant, or key, controls and include an opinion about the effectiveness of the design of the control in mitigating the related risk.

Compliance Risk Assessment

Annually, the Credit Union will prepare an assessment of its compliance risks. This assessment will begin with an assessment of the risk associated with those regulations the Credit Union is required to comply with, based on its operations, products and services. The risk assessment will be used as the basis for developing the compliance monitoring, testing and audit program and allocating compliance resources.

Operational / Audit Risk Assessment

The Internal Auditor shall annually prepare an assessment of the inherent risk of the Credit Union and submit and review this assessment with the Audit and Risk Management Committee of the Credit Union. The results of the inherent risk assessment will also be provided to other members of the risk management team, such as the Compliance Officer, Loan Review Supervisor or Credit Administration Officer, so that the scope of their work can be modified accordingly.

Annually, the Internal Auditor will develop, based on the understanding of the Credit Union's business activities and its assessment of risks, management, organization and accounting and internal controls, a comprehensive audit plan. This risk assessment will be documented in the Internal Auditor's Permanent File in the manner of internal control questionnaires, analyses of transaction volumes, notes from interviews with management, operational narratives or work process flow charts. A summary of the risk assessment, including those areas determined to be of high, moderate and low risk, will be reviewed annually with the Audit and Risk Management Committee of the Credit Union.

Product Risk Assessment

The Risk Management Department is responsible for completing an annual review of product line risk. Respective business unit managers will compile the necessary information to prepare this risk assessment. Product and line managers, in connection with Information Technology and Compliance, are also responsible for assessing risks associated with the offering of new products and services, or making substantial changes to existing products and services. These risk assessments will be documented and submitted to the appropriate parties for approval.

Vendor Risk Assessment and Due Diligence

The Information Security Officer is responsible for completing an annual assessment of risks associated with the use of third-party vendors. The ISO will prepare a ranking of all vendors in accordance with criteria for information security risk and operational risk. In particular, the Information Security Officer will assess information security risks and controls of those vendors who have custody of or access to the Credit Union's customers' non-public personal financial information. These risk assessments will be reviewed with the Audit and Risk Management Committee of the Credit Union. Further, the ISO will prepare an inventory of information assets throughout the Credit Union and an assessment of risk at each location.

BSA/AML Risk Assessment

Annually, the BSA/AML Officer will prepare appropriate assessments of: BSA/AML Inherent and Residual Risk, (2) OFAC Inherent and Residual Risk, (3) Product Risk, (4) Geographic Risk, (5) Customer/CIP Risk and (6) Effectiveness of BSA/AML risk controls.

FACT Act Risk Assessment

Annually, the Compliance Officer will prepare appropriate assessments of FACT Act risk, include the identification of covered accounts, risks associated with those accounts, red flags associated with ach account type and remediation actions for each rd flag.

Risk Management and Internal Control Responsibilities

The ultimate responsibility for risk management rests with the Board of Directors. Management and staff of the Credit Union also have clearly defined responsibilities for risk management.

Board of Directors Responsibilities

It is the responsibility of the Board, in conjunction with Management, to determine those risks which are warranted and acceptable, based on the Management's ability to: (1) identify and understand such risks, (2) measure the degree of exposure to such risks, (3) monitor the changing nature of the risk and related exposure, and (4) develop and implement processes and procedures to control such risks.

The Board and Management will define risk tolerances (i.e., limits) in the policies of the Credit Union. The Board and Management will ensure that periodic reports are provided to Directors that permit them to measure Management's compliance with risk limits and to gauge the changing nature of risk inherent in the Credit Union's chosen lines of business and operations and as a result of changing factors within the Credit Union, such as Management and personnel changes, technology changes, etc. To aid them in fulfilling their risk management responsibilities, the Board has established a number of risk oversight committees. These Committees include:

- The **Risk Management Committee** meets quarterly to review risk and compliance issues. Members include two outside Directors, the Chief Executive Officer, the Chief Financial Officer, Chief Lending Officer, Chief Technology Officer and the Internal Auditor. This Committee will become the key Committee regarding the broad seven categories of risk, as well as information technology and related security risk issues. Reports to this Committee will include Key Risk and Performance Indicator Dashboards, supported by risk indices (i.e., reputational risk, supported by an index measuring customer satisfaction, account churn, charitable contributions, advertising dollars spent, complaints, etc.) and specific, targeted risk assessments (i.e., BSA, GLBA, FACTA, IT, etc.)
- The **Supervisory Committee** of the Board, which meets quarterly, is responsible for reviewing the audit risk assessment and internal audit program and plan. The Internal Auditor of the Credit Union reports functionally/directly to this committee. The Chief Risk Officer also reports functionally to this committee. Other members of the risk management group, including Loan Review Officer, Compliance Officer, Information Security Officer, Security Officer and BSA Officer also submit reports to and meet with the Committee.
- **Credit Committee** is responsible for approving loans in excess of dollar limits specified in the Credit Union's Loan Policy. All loans presented to the Committee must first be approved by the Credit Union Loan Committee (i.e., Pre-Credit

Committee). Membership of the Executive (Board) Loan Committee includes three non-officer Directors and two executive officers of the Credit Union. The Committee meets as required, typically weekly and no less often than monthly and approves significant credits, as required by lending policies, and monitor all classified loans.

- **Investment Committee** is responsible for the management of interest rate/market risk, liquidity and funding risk, and capital adequacy levels of the Credit Union. The Committee will meet at least quarterly to review the overall balance sheet structure of the Credit Union and its compliance with asset and liability management, liquidity and investment policies, interest rate risk guidelines and capital guidelines. Reports of the Committees work, including minutes, will be provided to the full Board of Directors.

Management Responsibilities

Management is charged with employing personnel with the appropriate skills and experience to identify, measure, monitor and control risks within the areas of their expertise. To aid them in fulfilling their risk management responsibilities, Management has established a network of oversight committees. Key committees and their risk management roles are summarized below:

- The **ALCO Committee's** principally responsibility is to review the Credit Union's level of interest rate risk and determine if there should be recommendations to change the pricing of the Credit Union's loans or deposits.
- The **Executive (Directors) Loan Committee** are responsible for the overall management of the credit risk of the Credit Union, underwriting standards, lending practices, and the collection process. These Committees meet as required, typically weekly and no less often than monthly and approves significant credits, as required by lending policies, and monitor all classified loans.
- **Problem Loan Committee** is a management committee responsible for reviewing the status of identified problem loans. This Committee includes the Manager of Loan Review, Chief Risk Officer, Chief Credit Officer and Senior Loan officer. The Committee meets at least monthly.
- The **Information Technology Committee** - Responsible for the overall information technology environment of the Credit Union, including the preparation and update of technology plans, the identification of any new technologies that the Credit Union should implement and oversight of on-going relationships with technology vendors (i.e. monitoring service level agreements). The Committee is also responsible for monitoring progress of technology implementation and other project progress.
- The **Compliance Committee** - Responsible for identifying, assessing, and managing compliance risks related to the products offered by the Credit Union, any new products to be offered by the Credit Union and any changes to the products that should be considered due to changes in applicable regulations. The Compliance Committee is responsible for the implementation of policies, procedures, and training programs for compliance issues and

for the review of compliance and internal audit findings to ensure that the exceptions noted are effectively eliminated and proper internal controls established.

- The **Risk Management Committee** - The Committee is responsible for the overall assessment and management of risks throughout the Credit Union. The committee shall also be charged with proposing ways to mitigate or manage risk of the Credit Union.

Officers Responsible For Risk Management

In addition to the previously described committee structure, certain organizational units are charged with risk management responsibilities.

- The **President and Chief Executive Officer** is primarily responsible for the management of strategic business and strategic technology risk. This objective is fulfilled in conjunction with the Budget and Planning Committee of the Board of Directors and through the annual preparation/update of a strategic business plan and strategic technology plan.

- The **Chief Financial Officer** - Responsible for ensuring the accuracy of general ledger accounting information and the internal and external financial reports provided to the Board of Directors, Management and regulatory authorities. To fulfill this responsibility, the Chief Financial Officer and the Controller will be primarily responsible for ensuring the monthly completion of the general ledger certification program. The CFO is also responsible for evaluating and taking the lead in managing liquidity risks and interest rate risks, as well as evaluating credit risk in the Credit Union's investment portfolio. In this regard, the CFO will be responsible for maintaining and reporting results of interest rate risk/shock, liquidity forecasting and stress testing and capital models. Reports from these models and results of on-going risk assessments will be reported to the Management ALCO Committee and to the Investment Committee and to the Board of Directors.

  The CFO is primarily responsible for obtaining insurance. Insurance purchased and the specific coverage and features of each policy will, as appropriate, incorporate risk tolerances (i.e., retention, deductibles and limits) commensurate with the Credit Union's risk appetite and established guidelines. All insurance coverage will be reviewed annually with the Board of Directors.

- The **Information Security Officer -** Responsible for information technology risk management, including information technology security. The **Information Security Officer** is aided in this effort by the Credit Union's primary technology vendor, who provides certain data processing and data security services, including maintenance of the Credit Union's Internet firewalls and intrusion detection systems.

- The **Security Officer** - Responsible for ensuring that: (1) appropriate security procedures have been established and physical security devices installed, commensurate with the identified risk exposures and in compliance with the Credit Union Protection Act, (2) employees are properly trained in the execution of security procedures and use of security devices and (3) losses are appropriately investigated.

- The **Internal Auditor** - Responsible for ensuring the adequacy of and coordinating the overall risk management and internal control processes of the Credit Union. The **Internal Auditor** is responsible for ensuring that Management has established a framework of specific internal controls, accounting controls and operating procedures, commensurate with exposures to risk and to ensure compliance with the overall guidance of Board-approved policies and applicable regulations. The efforts of the Internal Auditor are augmented through the use of audit resources obtained from third-party vendors in the area of information technology.
- The **Compliance Officer** - Responsible for ensuring that: (1) the Credit Union maintains an appropriate compliance program and organizations, including chairing the Compliance Committee, and (2) that comprehensive tests of compliance are performed to assess the adequacy of compliance and identify and correct compliance errors. The **Compliance Officer** is also responsible for ensuring that: (1) changes in regulations are disseminated to the appropriate business units, (2) that business unit managers maintain procedures and systems to ensure that regulations and guidelines are followed, and (3) Directors, managers and staff are knowledgeable of laws and regulations which apply to the Credit Union's business through ongoing training programs, and (4) libraries of compliance and policy reference material are maintained. The resources of Compliance are augmented, as required, through the use of resources obtained from third-party vendors.
- **Chief Credit Officer** - Responsible, in conjunction with the Senior Lending Officer, lending officers and credit administration staff, for: (1) working with senior management, the Board of Directors and credit officers to develop appropriate credit policies, (2) developing appropriate reporting mechanisms and tools and monitoring compliance with lending policies, (3) evaluating and monitoring the overall quality of the total loan portfolio, (4) identifying credit exposure trends and (5) evaluating the credit quality of individual loan relationships and rating credit risk. The Chief Credit Officer, through credit administration, will be responsible for implementing and maintaining credit quality stress tests. The **Chief Credit Officer** will also report periodically to the Executive Loan Committee on the quality of loan portfolio, concentrations of credit and credit trends.
- **Loan Review Manager** - Responsible for performing periodic reviews of specific loan relationships, including evaluating the quality of the loan and Management's risk rating. The objective is to evaluate 65% of the total dollar value of the loan portfolio on an annual basis. The scope of the Loan Review Program will also include all classified and "watchlist" credits. In addition, Loan Review will evaluate specific loan segments, including concentrations of credit, and prepare evaluations of industry trends.
- **BSA/AML Officer** – Responsible for ensuring the Credit Union's compliance with Credit Union Secrecy and Anti-Money Laundering guidelines and managing the staff and systems responsible for the BSA/AML program.
- **Sarbanes-Oxley Compliance Officer** – Primarily responsible for maintaining and updating Sarbanes-Oxley Section 404 compliance information, including financial statement mapping, risk assessments, results of testing and remediation efforts.

- **Marketing Officer** – The Credit Union’s Marketing Officer will be primarily responsible for managing and monitoring reputational risk and assembling information to be used in periodic assessments of potential reputation risk and reporting in risk dashboards.
- **Business Unit Managers** - Responsible for making risk management, including identifying and measuring risk exposures, selecting and implementing risk management strategies and establishing appropriate internal controls, a part of their daily job function.
- **Legal Counsel** of the Credit Union is responsible for assessing, managing, and mitigating legal risks faced by the Credit Union and reporting such risks on a timely basis to the Board of Directors. The Credit Union currently employees full-time, in-house legal counsel. The resources of in-house legal counsel are augmented, as required, through the use of resources obtained from outside attorneys.
- **Certified Public Accountants** - Responsible for ensuring the accuracy of published financial statements, including the accuracy of valuation accounts (i.e., allowance for loan and lease losses) and the preparation/accuracy of tax returns. They are also responsible for assessing the adequacy of internal accounting controls and compliance with generally accepted accounting principles and regulatory accounting guidelines.

Efforts of these individual members of the Credit Union’s risk management program may be supplemented through the periodic employment of outside consultants and specialists.

Risk Tolerances

The Board and Management desire to manage risks at a level that permits the Credit Union to grow and achieve its strategic business objectives, while conducting business in a safe and sound manner, complying with all applicable regulations, and provide a return to shareholders that meets or exceeds their expectations. The Board of Directors will set risk tolerance levels annually through several means. The overall risk environment of the Credit Union will be considered annually in conjunction with the strategic planning process of the Board of Directors and Management. In this regard, the Strategic Plan will include a Risk Appetite Statement. Specific levels of risk tolerance within key business units, such as credit/lending (i.e., concentration risk), interest rate and liquidity, will be set annually through the review, and if necessary, amendment of the Credit Union’s business programs related to those areas. Specific risk tolerance limits and guidelines will be included, as appropriate, in the Credit Union’s Policies.

Monitoring the Risk Management and Internal Control Program

The Internal Auditor is primarily responsible for ensuring adherence to the Risk Management Program and Policy. The Internal Auditor will monitor the conduct of the various committees to insure each committee functions in a manner that appropriately addresses risk issues facing the Credit Union.

Certification Program

To ensure the accuracy of general ledger accounting information, financial statements and management accounting reports and to assess compliance with key internal controls, the Credit Union will develop and maintain an "on-going "certification program". This program, monitored primarily by the **Chief Financial Officer and Controller**, will include: (1) periodic reconciliation of key general ledger accounts to the appropriate sub-ledger system (i.e., demand deposits, loans, investments, etc.), (2) periodic analyses of certain general ledger accounts (i.e., prepaid assets, allowance for loan and lease losses, etc.), (3) counts/inventorying of negotiable items (i.e., travelers checks, investments in safekeeping, etc.) and (4) monitoring/testing of key internal control and security procedures (i.e., security equipment testing, branch security procedures, etc.). Results of the certification will be tested periodically by **Internal Audit**.*