

## The Changing Nature of Risk

**Audit control procedures are part of a kind of detective control, designed to determine whether preventive controls are working.**

The concept of risk management is not new to credit unions. Traditionally, credit unions and other financial service providers have addressed the challenges posed by risk on an exposure-by-exposure basis within each functional area. The loan department, for example, is backed up by a loan policy that helps to evaluate credit risk. Before granting a loan, the loan officer evaluates the chance it will be repaid.

In the past, loans were made or denied based on the character of the borrower and an evaluation by the credit committee. As fields of membership became larger and new tools became available to assess the likelihood of repayment, many credit unions turned to credit scoring and risk-based lending programs to assist in the evaluation process.

On the investment side of the operation, financial officers making decisions on behalf of the credit union analyze the risk associated with each investment opportunity before committing member funds. In a typical scenario, the credit union's investment professionals use the SLY principle to assess the risks an investment presents. SLY is an acronym for:

- Safety;
- Liquidity; and
- Yield.

Investment managers first consider the safety of the investment, then the liquidity it offers, and finally the yield. (It is generally conceded that the best investment a credit union can make in

terms of safety, liquidity, and yield is a loan to a member.)

Operational management is responsible for making sure tellers and other employees are well trained so that errors or omissions that result from transaction risk will be adequately managed. Because new accounts are a major source of forgeries, employees need to be trained in detection measures, and new account procedures need to be in place to determine the eligibility of potential new members. When employees verify membership eligibility as well as the potential member's identification, and record the information used to verify the new member's identity, fraud is deterred.

Use figure 3.1 as a quick reference for preventing new member fraud.

The internal audit department, with the oversight of the supervisory or audit committee, examines internal controls within the credit union's processes and procedures to identify any weaknesses that may increase risk. Internal controls are part of the credit union's **preventive** control system; they are designed to anticipate and avert problems. Audit control procedures are part of a kind of **detective** control, designed to determine whether preventive controls are working. Revising policies and procedures when a weakness is discovered is part of the corrective control, to strengthen the internal control process.

And the credit union security department is responsible for physical

**Figure 3.1****New Member Tips****Simple steps to avoid risk of new member fraud**

- Require a picture ID for member identification.
- Review all information on the new account application for accuracy.
- Verify identification with the primary family member before allowing new members to join.
- Ask for previous financial institution references or verify employment and telephone numbers.
- If the credit union allows accounts to be opened by mail, develop additional checks for those accounts.
- Be wary of new members who ask questions about funds availability and other teller procedures.
- These checks and procedures can prevent serious problems later by verifying the qualifications of new members in advance.

protection—making sure that the physical plant is adequately protected against burglary or robbery by having locks on the doors, good alarm systems, and safes.

### New Concepts in Risk Assessment and Management

While traditional methods continue to play an important role in maintaining the safety and soundness of the credit union and its assets, risk assessment and management has changed in the post-Enron, Sarbanes-Oxley era. Legislators, regulators, and risk managers have all realized that additional safeguards are needed to enhance traditional risk management procedures. Weakness in one area of the credit union can severely impact another area, and many emerging factors now influence risk.

Credit unions have always had to deal with the inherent risk of conducting a financial services business—making loans, accepting deposits, and maintaining branch offices to serve members—and this hasn't changed. But credit unions now must consider

risk from external sources, risks that are relatively new, such as those that follow.

**Threats from terrorism** have affected the way the organization handles money and enrolls new members. It has become increasingly clear that the financial services industries need to adopt new strategies, tactics, and technologies to protect against the potential expenses involved in terrorist attacks.

The events of September 11, 2001 forever changed the world. Our knowledge of terrorism has substantially increased, and we have begun to take countermeasures to protect virtually all aspects of business, government, and society. The economic impact of terrorist attacks often exceeds the direct costs associated with the events. While no one can truly put a price on the human losses, the financial impact can be measured. Methods, approaches, and techniques used to create programs that address risks are in place in most organizations today. However, these techniques have not been modified to adapt to the risks associated with terrorism.

A new approach to risk management must be developed that includes private intelligence in order to reduce or mitigate exposure.

In order to assist organizations in this undertaking, the federal government conducted research and published numerous guides that assist in planning. The Federal Emergency Management Agency (FEMA) offers a series of guides for protecting buildings against terrorist attacks. In the new era of corporate risk, technology plays an even more important role. A new approach to risk management must be developed that includes private intelligence in order to reduce or mitigate exposure. Combining core technologies such as intelligence and location technology provides the foundation necessary to achieve these goals.

As time passes after 9/11, there is a tendency to relax and lower one's guard. Risk assessment has taken on a whole new meaning after the events of September 11. In the new era of corporate risk, technology is playing an ever more important role. New approaches to risk management, such as private intelligence, must be developed to reduce or mitigate exposure within an organization or to an entire industry. Combining core technologies such as

intelligence and location technology provide the foundation necessary to properly manage risks associated with terrorism.

**Plastic card fraud** has forced credit unions to reexamine the ways that they administer these programs. Card fraud has become one of the most prevalent forms of theft from financial institutions, with losses totaling in the billions of dollars annually. CUNA Mutual Group reports that insurance claims on card fraud are rising at an alarming rate.

The bulk of the losses come from compromised accounts, sometimes referred to as "counterfeit skimmed" accounts. In the past, counterfeit skimming involved the compromise of one card at a time. For example, a dishonest merchant employee using a hand-held skimmer stole a customer's credit or debit card data. More recently, merchant breaches involved millions of compromised cards. In these cases, merchants violated Visa® and MasterCard® operating rules and regulations, which prohibit storing full magnetic stripe data after the authorization has been approved. One merchant originally said compromised card data affected 140,000 accounts, but later revised that estimate to 1.4 million credit card accounts and 96,000 checking accounts.

When criminals hack into merchant databases and steal card account information, they re-encode the magnetic stripes of stolen cards on what is called "white plastic," which is plastic with magnetic stripes, and create new forged cards. A financial institution name is placed on the

### Case Study: Merchant Computer Data Breach

A breach into the computer system of a New England supermarket chain resulted in the theft of up to 4.2 million customer credit and debit card numbers from more than 200 stores in several states. The chain said data was accessed illegally from the company's computer systems during the card verification transmission process in transactions.

The stolen data were credit and debit card numbers and expiration dates. The company said it could not send letters directly to the potentially affected customers because it did not have their names and addresses. The breach was among the largest retail breaches ever experienced. The data breach was not contained until a full three months after investigators discovered it.

**A neural network generates an alert whenever a cardholder uses a card for purchases outside the norm.**

front, and the card appears genuine.

Most of these cards wind up overseas, as credit unions find fraudulent transactions coming from foreign countries. Credit unions most at risk are those with large numbers of cards outstanding, and with a card base that is unusually active.

To defend itself against counterfeit skimmed cards, the credit union can initiate three practices:

- Name mismatch;
- Neural networks; and
- Monitor daily authorization reports.

The first is to use a security feature called “name mismatch.” This feature compares the cardholder’s name as it appears on the card’s magnetic stripe to the cardholder’s name stored in the card processor’s database. If these two names do not match, the transaction should be declined, and the card should be blocked.

Credit unions also need to look at the effectiveness of what is known as “neural networks.” This is a fraud monitoring service provided by the organization’s card processor (FAL-

CON, by Fair Isaacs, is one of the better-known neural networks). A neural network generates an alert whenever a cardholder uses a card for purchases outside the norm.

A third line of defense is to monitor daily authorization reports received from the card processor summarizing the day’s transactions. The credit union can copy the authorization report into an Excel spreadsheet and sort the transactions in a variety of ways to reveal suspicious activity. For example, criminals often test counterfeit skimmed cards to make sure they will work. If the credit union sorts its charges by dollar amount in ascending order, it can quickly find suspicious activity on a card. A charge of one dollar at a pay-at-the-pump gas station, followed quickly by another larger dollar authorization is a red flag.

In short, today it is easy for identity thieves to defraud the credit union without ever setting foot inside. They can do everything electronically.

The NCUA also recognizes that plastic card fraud and the resulting losses are affecting ATM, debit, and credit card programs in an increasing number of credit unions. Failure to protect plastic card operations is a significant safety and soundness concern, according to the agency.

**Electronic commerce.** The different types of fraud that occur over the Internet have forced credit unions to look at how they can control these risks and protect their members at the same time. Technology has required credit unions to rethink some of their business models, their core strategies, their service delivery, and their target

### Case Study: ATM Fraud

An ATM hack attack at a (former credit union recently converted to a) bank charter spread to members at other financial institutions, including credit unions. Members who used their debit cards at ATMs owned by the bank reported unusual activity on their accounts to their credit union. When one affected credit union first received reports of suspicious activity, it reissued members new cards. It also checked the unusual activity for common denominators and found that the affected members had used the bank’s ATMs. About 50 members of the credit union reported suspicious activity. The apparent cause of the breach was that the bank stored information it was not supposed to, so when the data system was hacked into, the hackers were able to use cardholders’ information to make purchases.

**The world of consumer finance is moving at lightning speed, and credit unions need to keep pace to stay viable.**

markets. Technology, and more specifically the Internet, is changing the way credit unions do business in substantial ways. For many credit unions, this has already taken place. The Internet has brought the world to our fingertips as consumers, and we're ready to take advantage of that world. Financial service providers now have a number of delivery channels available to them: person-to-person, the mail, the telephone, and the Internet.

Today, the typical U. S. household has multiple computers. In a relatively short time, many of those households have come to expect, even to demand, doing their financial business on the Internet. And credit unions need to be prepared to compete in this new marketplace. Members need to be able to access their credit union at any time, day or night, weekday or weekend and use any of the credit union's services immediately. Quick answers are essential for success on the Internet. Service requests must be fulfilled within seconds, loan decisions within a minute or two of application submission, and answers by e-mail, mail, and phone as rapidly as members expect them. Speed

is a factor that creates new levels of risk.

Consumers want their loans delivered better and faster. Our society may be moving a bit too fast, but there's no time to stop and reflect on the implications of technology. The world of consumer finance is moving at lightning speed, and credit unions need to keep pace to stay viable. The object is to deliver technology to members without losing the personal touch, and to control the risks associated with the process.

As Internet availability of financial services becomes ever more commonplace, credit unions need to enable a broad array of services online to meet their members' sophisticated technological needs. And credit unions must also be aware of the pitfalls of electronic commerce, most notably the risk of fraud and identity theft, and ensure that software and origination practices are in place to avoid losses in this area.

**Expectations of future members.** Young people entering the financial services arena have ever-increasing expectations. They want more products and higher quality, and this leads to more risk. Not meeting members' expectations can have a significant impact on the credit union's viability.

The next generation of members comprises the savers and borrowers of the future. Research shows these members are more technically savvy, more demanding of quick service, but extremely loyal to those who meet their needs. Credit unions that find a way to meet their needs will have great success with this demographic.

Credit unions need to examine their younger members to determine what

### Case Study: Member Online Gambling

Many credit unions have seen the impact of online gambling on members and the credit union. Gambling can create a burden for staff members in watching for telltale signs of online gambling abuse. One New England credit union CEO says: "If our members go to a casino or an online site, we certainly don't want to make moral judgments about them getting access to their money. At the same time, we want to protect both the credit union and our membership." In an uncertain environment for online credit card gambling, credit unions need to carefully assess business risks and then decide whether to block transactions. Credit unions should work closely with their credit card companies, their data processors, and their insurance companies to assure the safety and soundness of their card programs.

**Insurance is a safety net, not a substitute for sound business judgment.**

sorts of services they are likely to need in the future, and to develop services aimed specifically at them. Of special interest are young adults just entering the market for loans. Analysts at CUNA suggest that the average credit union stands to lose \$14 million in loans over the next decade if it does not increase loan penetration among 18- to 24-year-olds. These are future borrowers, and attracting them is critical to the long-term success of the enterprise. In short, credit unions cannot ignore the importance and the market power of their young adult members and potential members.

**Business failure.** As we discussed in chapter 1, legislators and regulators are giving increased accounting scrutiny to financial statements as a result of recent business failures. Many new regulations have been mandated. Credit unions now have to deal with legislation such as the Bank Secrecy Act and rules for consumer identification and protection of member information, all of which carry risks.

To protect the National Credit Union Share Insurance Fund (NCUSIF) and assure the continued safety and soundness of credit unions, the NCUA continues to develop and

refine its regulatory policies. To access current information on NCUA rules and regulations, as well as proposed changes in regulations, the agency's Web site is an excellent resource. The site is at [www.ncua.gov](http://www.ncua.gov) and includes links that provide the latest information on everything from the Federal Credit Union Act to Special Reports, Regulatory Alerts, Interpretive Rulings and Policy Statements, and a host of other subjects.

Another excellent resource for legislative and regulatory information is CUNA's Web site at [www.cuna.org](http://www.cuna.org). Click on the regulatory advocacy category to find information on advocacy, status reports, a guide to federal laws and regulations, compliance materials, and a research database.

**Insurance.** One of the biggest changes in risk management is the role that insurance is expected to play. Directors may have noticed the difference in the pricing of credit union insurance policies, the amount of coverage available, the deductibles, and the ability to get reimbursement for the bond claims filed. Insurance gives the credit union a way to transfer or limit liability. However, insurance is not a supplement to sound business policies and regular board and staff education sessions. Insurance is a safety net, not a substitute for sound business judgment. It protects the credit union from totally unanticipated or catastrophic events, not from inattention, inaction, or fraud.

Next we'll look at a relatively new concept in assessing and managing credit union risks, enterprise risk management.

