ZURICH

A risk management guide to prevent embezzlement and theft

Protect against inside moves

Contents

Published by

Zurich Services Corporation
1400 American Lane
Schaumburg, Illinois 60196-1056

Zurich has been a leading specialist in providing bond and insurance protection for financial institutions for over 110 years. As such, we are acutely aware that employee dishonesty is one of the most serious hazards to which your institution is exposed.

This booklet is published by Zurich Services Corporation as a service to the management of financial institutions. The guidelines were written with the assistance of Ernst & Young and Linda Conrad of Zurich's risk engineering group.

Introduction

The environment in which financial institutions conduct their business is changing dramatically. Deregulation promoted increased competition both within the industry and from nonfinancial institutions, while technology has allowed for a significant expansion in the scope of services that financial institutions can offer. In addition, financial institutions face an increasing array of laws and regulations imposed by state and federal authorities. These are just a few of the many developments that have affected financial institutions. Each new development presents management with greater challenges.

These challenges have intensified the focus on an institution's ability to adapt to changes in today's highly competitive environment and to optimize asset performance. Increased attention has been placed upon the reliability and timeliness of the financial information and management's ability to make informed decisions in a timely manner. Management has placed increasing reliance upon effective systems of internal control to meet these demands and to continue serving the fiduciary responsibilities of the institution.

Due to the large volume of transactions processed and the highly liquid nature of money and negotiable instruments, financial institutions require effective systems of internal control to a greater extent than most other industries. When properly structured, such a system can provide for prompt discovery of discrepancies and irregularities, reduce the opportunity for errors and fraud, and enhance protection against misappropriation of assets. Without adequate internal control, the risk exists that the institution's financial data may become unreliable, thereby undermining management's ability to make informed decisions.

This booklet provides information on financial crime, guidelines on internal control for financial institutions, and a checklist for assessing the adequacy of your internal control system. The following discussion treats the application of the most significant elements of internal control within the major operating areas of a financial institution. These controls, divided into general preventive measures and specific procedures for each area, are designed to lessen the risk that assets may be misappropriated or diverted for an unauthorized use. They are by no means deemed to represent an all-inclusive list of preventive measures, but solely address the most important internal control considerations. Finally, no system of internal controls, no matter how pervasive, can effectively safeguard against all acts of fraud or theft, especially those involving collusion among employees.

Financial crime

Embezzling means "to appropriate fraudulently to one's own use money or property entrusted to one's care." Embezzlement implies the elements of intent and personal gain. Fraud of one type or another occurs in almost every business today, costing American businesses approximately 6 percent of revenues or $600 billion annually, according to a recent report of the Association of Certified Fraud Examiners (ACFE). Financial institutions are particularly vulnerable to fraud, as the total check fraud perpetrated against banks' accounts has doubled over the last two years surveyed by the American Bankers Association. The latest survey also revealed that losses are expanding from superregional/money center banks into smaller regional banks. This increase in fraud is attributable to many factors, including easy access and technology improvements in counterfeit check production, the growth in identity theft cases, and the sophistication of organized crime. Common types of embezzlement are described below.

- Fictitious and unauthorized fraudulent loans
- Overdrawn accounts/kiting
- Employee loans and overdraft accounts
- Expense overstatement
- General ledger theft
- Fraudulent funds transfers
- Computer manipulation
- Thefts of cash, jewelry, collateral, bearer bonds

To manage these types of embezzlement and fraud, the financial institution must create a "perception of detection." In other words, the organization should create an environment that is hostile to theft, which involves establishment of a fraud policy and effective internal control systems. It is important to practice careful employee hiring (including reference checking), provide thorough internal controls training and demonstrate a commitment to punish the guilty.

The FBI estimates that financial institutions may lose three times as much money from embezzlement and fraud as from robbery. Embezzlement is the most popular financial crime in the nation and is a significant factor in the failure of all types of businesses.[1]

Losses attributed to acts of embezzlement are more significant than losses attributed to all other types of business crimes combined. These crime risks are often difficult to quantify, and controlling these risks will rely heavily on evaluation of operational structure and adherence to safety and organizational procedures. Adequate security and a system of checks and balances will be essential for proper loss management to mitigate the extensive overall crime exposure present for financial institutions. Employee dishonesty exposure may be great, as tempting opportunities abound and banks can have a high turnover rate. Banks typically have a great deal of cash, and other valuables on the premises, and employees may have access to credit or the funds transfer system. Therefore, financial institutions require a strategic approach to investigating and reducing losses from both internal and external embezzlement crimes.

How does the financial institution protect itself from becoming a victim of embezzlement, fraud and internal crime? In order to mitigate this significant internal crime exposure, it is necessary to investigate whether the organizational structure provides checks and balances that will minimize the opportunities to a potentially dishonest employee to embezzle money or obtain funds for personal gain. Prevention of internal crime will rely heavily on evaluation of carefully documented operational structure and adherence to those organizational procedures. The quality and commitment of management, training, supervision and internal/external communications may affect loss potential. For example, are managers watching for behavioral changes or schedule modifications in their employees? Are pre-employment references checked thoroughly and background investigations performed to uncover possible criminal involvement? Has a system of duty cross-checks and surprise audits been established to catch fraud?

1 International Association of Financial Crimes Investigators (IAFCI) Conference in Boston, MA, September 2002.

The elements of internal control

Internal controls in financial institutions can be segregated into five elements. None of these measures alone, or in conjunction with one another, can completely eliminate the risk of embezzlement or collusion among employees. However, the likelihood of fraud or theft should be significantly reduced. These elements of internal control are:

- Defining and periodically reviewing authorization to commit the institution's financial resources
- Safeguarding negotiable assets
- Accurate and timely recording of transactions
- Segregating those duties which, in order to have affective internal control, are incompatible
- Proper valuation of reported balances

1. Defining authorization to commit the institution's financial resources

The financial commitments that an institution enters into are done so in accordance with management's authorization and executed in conformity with management's intentions. Authorizations may be general or specific. General authorizations apply to a large number of similar transactions and are granted by establishing policies such as officer lending limits, customer credit limits or review policies. Specific authorizations may be required over and above the general authority determined by management. For example, management may decide to approve lending on officer approval to a specified dollar limit, and credit committee approval for loans in excess of that amount.

2. Safeguarding negotiable instruments

Direct physical access to assets must be limited to designated personnel (e.g., tellers) and indirect access (approval to initiate the transfer of the institution's assets) limited to those who are properly authorized by management. Safeguarding is also achieved through physical precautions (e.g., locked file cabinets for unused bank drafts and burglar resistive and fireproof vaults for the protection of currency and securities). Know who approves and authenticates the

collateral taken in support of loans. There should be a system in place to prevent employees from benefiting from the unauthorized sale or purchase of securities and to protect securities from loss. Document how such collateral transactions are authorized.

3. Accurate and timely recording of transactions

All transactions are to be recorded in the correct amounts, in the period they were executed and in the appropriate account. The physical evidence of recording includes documents (e.g., cash and general ledger tickets, bank notes and drafts, etc.) and records (e.g., subsidiary ledgers, proof recap, general ledger) in which the transactions are entered and summarized. These documents and the procedures used to post transactions should be designed to limit the possibility that a transaction will be recorded incorrectly, recorded more than once, or omitted from the records. For example, a document might include preprinted numbers, instructions for preparing and routing, and space for designated authorization or approval. Procedures might incorporate duplicate data entry, check digits and reconciliation of account balances to physical balances. In reconciliation of account balances, accounting records are compared with related assets, documents or control accounts (e.g., periodic reconciliation of investment securities to detail records and control accounts). The nature and amount of any differences are identified and investigated and the account balances adjusted, as necessary.

4. Segregating those duties, which, from the perspective of effective internal control, are incompatible with one another

Those duties, which are incompatible with one another from an internal control standpoint, should be segregated among different employees. This segregation is structured to avoid one person having complete responsibility for the process, such as the initiation of the entry, processing of the transaction and reconciliation of the reported balances. In addition, the financial institution should not allow one individual control over both physical assets and the accounting records. For example, negotiable instruments should not be maintained by the same employee who has record-keeping responsibility.

5. Proper valuation of reported balances

This control addresses whether recorded amounts are properly reviewed for impairment in value, reserved or adjusted as necessary to conform with generally accepted accounting principles and regulatory guidelines. Allowances for possible loan losses should be reviewed quarterly and adjusted for any impairments in the value of the loan portfolio. Collateral values and other bank assets marked-to market should accurately reflect their true value on the balance sheet.

Internal control within operations

Defining the authorization to commit the institution's financial resources

Control over authorization to commit the institution's financial resources is accomplished primarily through the structure of the organization and establishing, communicating and monitoring the institution's policies and accounting procedures. The most important control features in this regard are:

- A formal organizational structure that clearly defines the level of authority and commensurate reporting responsibilities associated with each level.
- Clearly defined written policies and procedures.
- An accounting system that provides accurate and timely information concerning the level of outstanding commitments.
- Periodic audit reviews and, if an institution's size permits, a well-trained internal audit staff that reports directly to senior management and the board of directors.
- Authorization of all cash adjustments to assure that cash differences are identified at an appropriate level and that proper action is taken to resolve differences.
- Authorization of noncash transactions (i.e., account debits and credits) to prevent misappropriation of cash assets through the posting of noncash transactions.
- Authorization of withdrawals against uncollected, attached or pledged funds to lessen the potential exposure to outside fraud.
- Authorization of substitute documents prepared for rejected proof-transit items.
- Electronic funds transfer policies that include identification requirements (passwords, call backs), restrictions on the amount of funds employees can transfer and policies that reclude transfers against uncollected funds.

- Authorization limits restricting the amounts employees and officers can disburse and a requirement that countersignatures be obtained for disbursements in excess of a given amount.

- The centralization of administrative expenditures, to the extent possible, to ensure these disbursements receive the proper amount of scrutiny and approval at the proper level of management. This feature also facilitates account reconciliation.

Safeguarding negotiable assets

An important objective of internal control is safeguarding negotiable assets. In addition to cash (the most negotiable asset), there are many other highly negotiable items handled on a daily basis. These items include bearer bonds held as bank-owned securities and as assets of trusts administered by a bank, collateral on secured loans which may be in the form of stocks or bonds accompanied by "powers of attorney" signed in blank by the owner, cosigned traveler's checks, cosigned U.S. Savings Bonds and official bank checks.

Important procedures in this area should include the following:

- Each teller's cash supplies should be separated from one another to allow for designation of individual responsibility. In addition, each teller's cash assets should be proven on a daily basis to an independent control, with over/short cash supplies cleared on a regular basis. This procedure will allow for timely identification of cash variances and diminish exposure to cash losses.

- Cash reserves should be maintained under dual control, including a procedure allowing for independent verification of cash transfers and the dual custody of cash assets, thereby diminishing the exposure to cash losses. Dual control is the authorization, approval or action of two individuals to complete a transaction. It should be exercised over vault cash, vault supplies of traveler's checks, night depository mail and ATM items. Securities and negotiable collateral held in any capacity, whether in the commercial banking department or the trust department, should be under dual control. Dual control procedures should also pertain to the custody and control of dormant accounts and notes which have been charged-off.

- Checks should be cleared daily from the teller funds to ensure timely deposit and prevent the withholding of checks and possible lapping of funds.
- Check cashing policies should include identification requirements, approval limits and should preclude the cashing of checks payable to corporations, partnerships and other organizations.
- Verification procedures should be required to assure authenticity of wire transfer requests that include verification of signatures on mail requests, call back procedures on verbal requests and sufficient controls (i.e., code book, test keys) on electronically transferred requests.
- Verification of signatures on in-clearing checks over specified dollar limits to lessen the exposure to fraudulent and forged checks.
- Restricted access to unissued checks, check-signing machines and signature plated and wire transfer equipment.
- Accounting controls over the sequence in which checks are issued, the retention of bonded checks and the release of checks for payment.

Accurate and timely recording of transactions

Wire transfer procedures should include:

- Written confirmation of customer-initiated transactions (subject to amount limitations).
- Tape recording for incoming verbal requests and call back verification.
- Prenumbered transfer request forms; numerically accounted for and logged with access restricted to a limited number of authorized personnel.
- Independent verification of request form usage and sequence.
- Daily reconciliation of requests to transactions actually processed (for amount, payee, etc.).
- Retention of wire transfer documents and historical records (for an established time period).

Proof-transit procedures should include:

- Use of predetermined batch control totals and independent verification of control totals computed by external sources
- Use of a batch receipt log to control production through the department

Accounting procedures should include:

- Daily reconciliation of department transactions with batch control total balances
- Independent review of substituted or rejected documents
- Periodic reconciliation of reported balances to physical assets

Segregation of duties within the operations functions

- Tellers and proof-transit employees should be prohibited from performing functions in other departments. An employee, independent of the teller operations, should be responsible for issuing new account documents and assigning account numbers.
- The physical custody of cash should be segregated from the posting of accounting transactions and from the reconciliation of account balances.
- Officers' and employees' accounts should be segregated by assignment of a designated series of account numbers and should be reviewed periodically for unusual activity.
- Transactions to dormant accounts should be reported separately and reviewed periodically by employees independent of the teller or bookkeeper functions.
- Account statements should be mailed to customers on a regular basis. All customer inquiries should be handled by employees independent of the teller and accounting functions.
- Responsibility for originating, processing and reconciling wire transfers should be segregated.

- Proof-transit responsibility for batch control processing, transaction encoding and the reconciliation of control totals should be segregated.
- Responsibility for initiating administrative expenditures, preparing negotiable instruments and reconciling transactions should be segregated.
- Administrative expenditures should be disbursed from a separate operating account and segregated from normal bank transactions.

Internal control within lending functions

A financial institution should be aware of the various types of loan fraud such as revolving or term loans, employee loans, overdraft account fraud, and plastic card outstandings. Typically, the largest types of fraud losses that a financial institution may incur relate to loan losses, where an employee has created fictitious loans, loans made based on fraudulent documents, or made loans that violated the bank's internal procedures to cause a loss to the bank and obtain a personal gain. To audit for fraudulent loans, the financial institution should use a checklist to review the files to ensure that the loan was issued within policy, and that all documentation and collateral is in place. The financial institution should also trace to share and loan trial balances. Characteristics of loan fraud include frequent refinances, signature or vehicle loan, and an address that is a P.O. Box (not a "warm" address). To test for fraudulent revolving or term loans, it is advisable to have the computer generate a list of loans with the following characteristics: not on payroll deduction, original balance the same as current balance (no paydown), due dates more than 60 days in the future, and/or no payments for 60 days. Below are red flags that may indicate fictitious or unauthorized loan fraud:

Statements/Trial Balance	In Loan Files
- Unexpectedly high balances	- Missing, incomplete, or altered documents
- Missing or inadequate payments	- Missing approval signatures
- Inadequate amortization	- Missing collateral
- Principal only payments	- Large number of extension agreements
- Interest rate discrepancies	- Inconsistencies in terms, rates, amounts
- Unusual due dates	- Missing files

It is essential that the financial institution have an accurate list of employee accounts and loans, including board members and committees. Beginning with known accounts, you can then cross-reference to search for other outstandings through SSN, joint ownership, address, maiden names, and account transfers. It is also beneficial to let employees know you are watching by developing a "perception of detection" within the organization. Some characteristics of fraudulent employee loans are shown below.

- Failure to obtain proper approval, and rush or custom loans
- Granting loans outside loan policy

- Unauthorized refinances
- Preferential interest rates
- Failure to secure collateral
- Unauthorized file maintenance charges
- Unexpectedly high balances or inconsistent amounts
- Missing, inadequate or principal-only payments
- Unusual due dates, amortization schedules, or extension agreements

To perform an overdrawn account audit, the financial institution should review accounts for negative balances, obtain copies of employee statements, and review a sample of nonsufficient funds (NFS) rejection listings for any employee activity. Verify that overdrafts were handled and repaid in accordance with policy.

Defining authorization to commit the institution's financial resources

A review of the institution's lending policies should be made, at least annually, to address:

- Loan authorization limits and credit policies
- Compliance with industry/secondary market guidelines
- Appraisal criteria and list of approved appraisers
- Compliance with regulatory lending guidelines

Loan documentation procedures should be sufficient to ensure that:

- Separate files are maintained for each loan and reviewed independently for completeness. The files should contain a checklist of loan documents and a separate credit file.

- The application review procedures are documented clearly in the file.
- Adjustments, renewals and extensions are indicated clearly on the loan documents.

The following should be monitored on at least a quarterly basis:

- Concentrations of loans within particular industries or geographical areas
- Delinquent loans
- The adequacy of the allowance for loan losses
- Investments in foreclosed property
- Loan officer delinquency rate

Verification of loan balances should be performed annually, on at least a sample basis, by an external audit firm or, if the institution's size permits, an internal audit staff that reports directly to senior management and the board of directors.

Safeguarding negotiable assets

- Adequate physical control should be maintained over loan documents.
- Loans should not be funded in cash.
- Repossessed assets should be secured adequately and protected against diminution in value.
- Repossessed assets held by third parties must be inspected and inventoried on a regular basis.
- Ensure that unissued letters of credit are secured physically to prevent unauthorized access.

- Acceptance/release of collateral should be receipted on prenumbered forms; release of collateral must have officer approval.
- Construction loan disbursements should be made only after evidence of completed work is reviewed.
- Floor plan inventory must be verified physically on a regular "surprise" basis.

Segregating duties within the lending function

The functions that should be performed by individuals independent of the lending function are:

- Credit reviews
- Property appraisals
- Disbursements of loan proceeds
- Processing of loan payments
- Preparing delinquent loan lists
- Disposals of repossessed collateral
- Adjustments to employee loans

An independent loan officer should review any adjustments, renewals and extensions to the loan application.

The completeness of loan files should be reviewed by an independent person prior to disbursing loan proceeds.

Lending officers should not have access to the accounting records or be allowed to post entries without appropriate officer approval.

Loans that have been charged-off should be segregated and maintained under separate accounting control.

Detailed statements of the loan balances, including charge-offs and pledged collateral, should be mailed at least annually. Any exceptions to those balances must be resolved by employees outside the lending functions.

Internal control within the investments and trust areas

Defining authorization to commit the institution's financial resources

Investments and Trust areas of financial institutions can incur large losses. An investment committee of the board of directors should set investment strategies for the institution that may include:

- Statement of investment
- Expertise requirements
- Authorization levels and limits for investment commitment transactions
- Limits on concentration by type and industry
- Limitations on positions (amounts and holding periods)
- Monitoring of correspondent relationships
- Monitoring portfolio vs. trading accounts
- Monitoring of investment transactions, including all security gains and losses

Purchases and sales, transfers between portfolio and trading accounts, investment gains and losses, and composition of the investment portfolio should be regularly reviewed by the board of directors, preferably by an investment committee.

Market value of investments should be independently verified and regularly reviewed by management.

Safeguarding negotiable assets

Securities held by the institution should be held under dual control, segregated from fiduciary securities and independently verified on a regular basis.

Investment transactions under a trust agreement must be reviewed periodically to ensure that the transactions are within the authorization of the trust agreement and that the fiduciary responsibilities, as set forth in the trust agreement, are being properly followed (e.g., authorization is being obtained from a trustee when required by the trust agreement).

Segregation of duties within the investment and trust functions

The balance of fiduciary securities is to be reconciled to a control total by an individual who is independent of the investment department.

Trust statements should be periodically mailed to the parties of interest for verification.

Policies and procedures should be established to govern systems development, management of data processing applications, physical security of data processing equipment, and data integrity.

Computer manipulation and data processing

Computer manipulation and abuse

Nielsen//NetRatings reports that people with access to the internet via a home PC increased from 531 million people in 1Q2002 to 553 million in 2Q2002. The United States has 30 percent of the global internet population, followed by Europe with 24 percent and the Asia/Pacific region with 14 percent of the total. This growth in internet and computer use has led to an increase in unauthorized file maintenance, which can result in loan manipulation (changing balance, etc.), reversal of fees, advanced due dates (extended repayments), creation of fictitious accounts, and unapproved reissues/address changes. Computer fraud also includes identity theft and plastic card fraud, where hackers or skimmers obtain account numbers and sell them over the internet. The financial institution should check postings periodically to ensure credits/debits are posted to proper customer accounts instead of employee or phantom accounts. Unauthorized supervisory overrides should also be checked because they permit employees to process sensitive transactions. With online banking, there should be monitoring of activity at odd hours and manipulation of personal customer accounts. With regard to ATMs, care should be taken around third-party processing companies. Financial institutions should watch for false PIN pads, which are secretly added to ATM machines to capture data streams and produce forged cards, later used to get cash.

Electronic theft

Internet banking and computer use has significantly increased the risk of electronic theft. This exposure will likely expand with the growth of the electronic funds transfer system and a cashless society. The Computer Security Institute has estimated that 90 percent of all financial institutions have had some type of computer security breach, 80 percent have had financial losses as a result, and 40 percent have suffered losses over $450 million. Financial institutions must protect themselves against the threat of electronic theft by devising an organizational structure with checks and balances that will minimize their exposure. Computer operations employees should work with the bank's auditors to ensure that the systems and audit trail are sufficient, and that usage logs are checked. With regard to internal computer usage, employees should be subject to a formal division of labor and lines of accountability that are clearly delineated in writing.

As with other types of internal crime, periodic random checks should be performed to verify functionality, particularly with those who have access to credit accounts or funds transfer. It is also important that dismissed employees have their passwords and access disabled to prevent information dissemination.

Internet banking liability

As with electronic theft, the growth of the electronic funds transfer system and the cashless society has also significantly increased the risk of exposure to internet banking liability. Directors, officers and employees must protect themselves and the financial institution for losses arising from "wrongful internet/electronic banking acts." Such acts would be defined as any actual or alleged act, error or omission, misstatement, misleading statement, neglect or breach of duty committed in connection with the provision of internet banking services. First-party protection can be provided through a Financial Institution Bond enhanced by the addition of an Electronic/Computer Systems Rider, which provides protection against loss resulting directly from the fraudulent transfer of funds initiated through the bank's computer systems. Zurich's E-RiskEdge® Policy provides coverage under the following insuring agreements: Business Income Loss, Intellectual Property Loss, and three events of Business Loss: business interruption, public relations expense, and cyber/network extortion.

The financial institution may also want to consider the following optional Fidelity Bond coverages that address risks that are more specific to certain banking activities and services. These optional endorsements are: Electronic/Computer Systems Rider, Fraudulent Mortgages Rider, Unauthorized Signature/Alteration Insuring Agreement, and Trading Loss Rider. All of these risks could be associated with embezzlement.

Internet banking intrusions

Recently, there were at least two intrusions into the systems of major internet banking service providers. In each scenario, the internet vendor took the server down for several days and notified the banks involved. In the first intrusion, it appeared that over 100 banks allegedly had their account information hacked. While no immediate use of the information was immediately detected, there is

now malicious activity arising from the confidential information obtained during the hacks nearly eleven months ago. The hackers are now ordering checks drawn on customers' accounts, requesting PIN code changes and creating counterfeit checks. This delayed loss experience is similar to credit card fraud whereby fraudulent account information does not surface for 6 to 12 months or longer from the time of intrusion. During this lag time, an opportunity existed for the banks to notify customers, change account numbers and passwords, and reprint checks. However, some banks did not disclose the intrusion for fear of negative publicity and loss of customer confidence. Those banks that did not notify customers and change data suffered losses, and exposed themselves to liability suits, rather than mitigating the potential risk. Those banks that were upfront with customers were less likely to sustain later loss and were less exposed to allegations of fraud, breach of duty or punitive damages.

The intrusion at the second internet provider resulted in funds being immediately wire-transferred from one bank to an out-of-state bank and out of the country. In the wake of this hack, some banks have received extortionate e-mails, threatening to expose the hack to the bank's customers and publish confidential account information (attached to the e-mail) unless some money was paid. Lists of account numbers are easily sent via the internet to other states or exported overseas, where they are used to make duplicate cards and obtain cash advances. Criminals are also using debit cards to buy U.S. Postal Money Orders and cashing them out.

Hackers and viruses

The computer system is vulnerable to electronic theft by hackers who gain access to a network, either legally or illegally for the purpose of stealing data. Often, these hackers are internal employees or network administrators who have easier access to passwords and clearances. Similarly, the computer system may be attacked by viruses that are installed by employees to invade and disrupt the system.

Electronic barriers — or firewalls — should be present on all computer networks that interface with the internet to prevent uninvited access by hackers proficient at breaching password protection systems. When inspecting the internet banking system, the type of online identification that is required of customers should be

investigated. internet banking users should be provided with unique PINs or passwords to prevent unauthorized entry into the system. Measures should be used to safeguard the customers' personal information. All sensitive financial and proprietary information should be encrypted, with access restricted to those in possession of frequently changed passwords. There should also be an employee designated to monitor system usage logs.

Business contingency planning

Many banks rely on their internet service vendors to ensure that security is adequate to protect the integrity and assets of the institution, and to mitigate impact on operations. Actually, the bank itself should regularly monitor transactions and exception reports to identify any suspicious account activity. The bank's internet banking implementation and review process should include a cohesive disaster recovery plan, which addresses all contingencies in the event of an internet banking intrusion. This recovery plan should consider the potential cost of negative publicity and resultant public relations expense, loss of customers' confidence, costs to communicate with customers, and expenses to change account numbers, checks, passwords, etc. It is imperative that a bank continues operations as quickly as possible, because the principal time element exposure for banks is extra expense resulting from loss of data/funds processing capabilities. Hence, a Loss of Use Endorsement to the Electronic Data Processing coverage may be necessary to address the business interruption from hackers and viruses, or from denial of service and router problems. It is critical that the flow of incoming and outgoing funds not be interrupted. The financial institution should have systems in place that back up crucial data on a daily basis. Listed below are some e-commerce risk issues that can arise from disruption of a financial institutions' computer systems.

Banks
- Hackers/viruses access
- Customer account info
- Funds transfer problems
- Contingency planning
- "Denial of service"
- Internet retailer credit card fraud
- Customer legal liability
- Public relations
- Expense to rework accounts
- Internal posting/drawdown fraud
- Business interruption

Internet Service Providers
- Router problems
- Hacker intrusions
- Legal liability to users
- Virus
- Data backup

Customers
- Identity fraud
- Lack of funds access
- Fraudulent withdrawal/draw down/posting
- Plastic card fraud

Defining authorization to commit the institution's financial resources

- An overall priority plan for system development and maintenance
- Formal documentation procedures (all program changes should be documented in writing)
- Formal user testing procedures for the implementation of new system software and systems maintenance
- Review and approval guidelines for systems development, including user participation. The work of independent software contractors should be subjected to the same standards as those of in-house programmers.

Physical security

- Data access and security standards, including employment policies covering issuance and return of employee security codes as well as policies concerning hiring and terminating employees (e.g., confidential background checks, etc.).
- Responsibility for security violations should be clearly detailed and imparted to all employees.

- Data processing facilities should be secured through the use of both physical controls, such as locks, security guards, badges and access cards; and electronic controls, such as magnetic card readers, access codes and passwords that restrict access to the system.

- Management of data security systems should include periodic revision of security codes of terminated employees. In addition, background checks should be performed on all new employees.

- System documentation and files should be restricted to authorized personnel through the use of restricted access features, user logs, etc.

- Access to remote terminals and communication lines, especially those connected to a communications network, should be restricted.

- Access to confidential data and critical features of software programs should be controlled, monitored and evaluated periodically. The system should also incorporate features to document repeated system access attempts, and to logoff users after a specified period of inactivity.

- Backup and recovery features for software and data files should ensure that all information can be restored in the event of data loss, damage or the introduction of errors and/or contamination of data files. These features should also ensure that the integrity of the software and data is adequately maintained during the recovery process and that alternate procedures exist to operate critical transactions in the event of a disaster or system failure.

- Rejected transactions should be corrected on a timely basis and re-entered promptly into the production process, subject to the same controls as the original data. This procedure limits the exposure to transactions circumventing the normal production process and the associated controls.

- Critical master file transactions should be supported by written documentation and reconciled to that documentation by an individual independent of the data processing (DP) department or by supervisory personnel within the department with no access to data production. Run-to-run batch control goals, or similar controls, should also be employed to ensure that all file changes are authorized.

Segregation of duties within the data processing function

- Segregation of data processing personnel, both within the department (i.e., segregation of systems development and application personnel) and within the institution.
- Changes to master files should be initialed by authorized user personnel.
- Access to identification codes for ATM accounts and electronic funds transfers should be controlled, preferably by individuals outside the data processing department.
- The identification and resolution of errors and the reconciliation of batch control totals should be segregated from the systems applications.
- Systems development and programming personnel should not have access to customer files nor have any responsibilities for resolution of customer discrepancies.
- Computer applications personnel should not be allowed to implement program changes.
- The management and reconciliation of batch control totals should be segregated from both application processing and systems programming.
- The library of computer programs should be closely controlled and monitored, with all program changes documented and approved prior to implementation.
- A separate group, either within the data processing department or a user group, should control the input and output and verify batch control totals.

Account fraud

Identity fraud prevention strategies

The Federal Trade Commission (FTC) recently registered a 300 percent increase in identity theft. Identity theft, also called account takeover fraud or true name fraud involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number, and mother's maiden name, in order to impersonate them. This information enables the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, establishing cellular phone service, purchasing automobiles, applying for loans/plastic cards/social security benefits, renting apartments and establishing services with utility and phone companies. Technology has aided criminals in obtaining false identifications, as well as educated them on how to commit check fraud. A trip on the internet quickly illustrates the ease with which criminals can obtain false documents used to defraud financial institutions and other organizations. Therefore, technology must also be one of the tools in a financial institution's arsenal to combat check and loan fraud. It is helpful to utilize a name-search software program to compare given name with address, driver's license information and Social Security number. Technological solutions and tools like inkless fingerprints should become an integral part of the new account/loan process to achieve the goal of "Know Your Customer."

While identity theft may be the nation's fastest-growing crime, police funding shortages and turf battles have prevented it from becoming a top crime-fighting priority a General Accounting Office report said. "Because identity theft is still a non-traditional crime, some police departments may be unaware of the importance of taking reports of identity theft, much less initiating investigations," said the GAO study requested by Rep. Sam Johnson (R-Texas). The study also found that identity theft victims often have trouble filing a police report. In fact, about 35 percent of victims who contact the Federal Trade Commission had tried and failed to file a report with local police. Since identity theft cases often cross state and other jurisdictional lines, "law enforcement agencies sometimes tend to view identity theft as being someone else's problem," the report said. With the police perception that identity theft is someone else's problem, the burden to disrupt account takeover fraud falls upon the affected individuals and financial

institutions. By catching the identity theft prior to the establishment of accounts or credit, financial institutions can reduce potential charge-offs and improve profitability.

Expense theft

Expense theft involves altered checks or payment of personal items through the financial institution's checking account/accounting function. Through the checking account, employees may alter the check, issue a check to a bogus vendor or pay for personal items with a financial institution check. Through corporate cards, expense theft can also take the form of "double dipping" — charging excessive meals/entertainment or personal items. To audit expenses, the financial institution should begin by reviewing its policy and board minutes. A sample should be selected from the transaction register/general ledger to be compared with supporting documentation and cash expenses paid. Financial institutions should obtain corporate credit card statements and physically inventory large purchases.

Check kiting

A kite is a check or draft drawn against uncollected funds for the purpose of creating false balances by taking advantage of the time lapse required for collection. Kiting is a continuous movement of worthless checks that take advantage of early funds availability in the check clearing system. A quasi-neural network can be used to mine account data patterns to track the kiting. Kiting can occur by exchanging checks for cash, single-handedly or with collusion, within the same account or between two or more financial institutions. Note that kiting can also occur between an account and a line of credit or credit card, or through an ATM by making fake deposits (empty envelopes or NSF checks) and real withdrawals. It is for this reason that financial institutions may want to verify that check cashing and withdrawal policies preclude the cashing of checks payable to third parties, corporations, partnerships and other organizations. Financial institutions may want to restrict the withdrawal of uncollected, attached or pledged funds by placing holds on the checks to the extent permitted by law.

Neural networks

While every check kite involves withdrawals against uncollected funds, not all withdrawals against uncollected funds involve check kites. A neural network can recognize inconsistencies in a checking account, and examine the account for patterns of fraud that may indicate possible kiting activity. When the neural network system is installed, account histories for all accounts of the bank are downloaded. The network will then run in real-time and can be tied into teller stations. The neural network model will not only detect signs of fraud on items written on that account, but can also detect deposit patterns of fraud for that account. For "on us" items, the neural network database also contains digitized check images for the account in question, as well as a digitized signature database. It will also determine whether a particular check number is out of an acceptable numerical range. The neural network is also designed to detect suspicious amounts on checks as well as suspicious digit combinations. The theory is that people favor certain digits when making up random numbers, and are not very adept at creating random number sequences. Note that, if your financial institution is outsourcing its processing, you should inquire as to whether the processor has such a neural network in place, as part of your vendor due diligence.

Neural networks operate by focusing on predicting what we do not know. There are also rules-based systems that focus on what we do know about fraud patterns to exclude certain transaction types. In combination, these two types of analysis programs can be very effective in disrupting fraud and embezzlement.

Plastic card fraud

Financial institutions lost over $1 billion in plastic card fraud last year. To review for fraudulent plastic card facilities, select a sample from new accounts, requested limit increases, overlimits, change of address or name, and reissues (for lost/stolen card). These loans can be verified by telephone. The financial institution must be cautious of "bust outs" in which credit cards are repaid with "booster" checks or NSF checks — then an increase in limit is quickly obtained before the NSF is discovered. More funds are immediately drawn down and deliberately never repaid. These bust outs can occur at the individual or merchant level, and funds are often used to purchase gold coins that are easily held or resold.

Plastic card losses continue to escalate, leaving financial institutions to absorb much of the cost of these fraudulent transactions through higher deductibles and consumer chargebacks. Financial institutions should be cautious issuing multiple cards to the same individual because they may be sharing or selling the extra card to an unauthorized party. In addition, financial institutions should be alert for any round dollar transactions. Approval amounts ending in $.00 should be redflagged for further scrutiny, as service/merchandise sales rarely end evenly and may be a cash advance by an unauthorized user.

It is preferable that a neural network be put in place to help detect plastic card fraud by examining accounts for possible patterns of fraud or fraudulent transactions. A neural network will also help prevent fraudulent plastic card transactions by subjecting each transaction to multiple screening parameters before issuance of an approval code. Financial institutions should not allow any transactions to be approved by an internal employee outside this neural network (for example, bypassing the network and using manual approvals if the network is slow/down) because security may not be as thorough and fraudulent charges may get cleared in error.

Other concerns

ATM controls

The use of ATM machines presents several additional concerns:

- Access to the customer PIN numbers should be restricted from employees who have access to customer account numbers.
- ATM transactions should be settled daily and all customer discrepancies resolved promptly.
- Customer statements should note ATM transactions clearly and address procedures that the customer should follow to notify the institution of any discrepancy.
- Restrictions should be built into the system to prevent the withdrawal of funds prior to the collection of deposits. The institution should establish a strict funds availability policy.

The use of a service bureau

The use of a service bureau does not fundamentally change the internal control structure necessary to assure that transactions are processed in an accurate and timely manner. The effectiveness of the internal control procedures that a service bureau uses for controlling data are basically the same as those used for in-house processing. These are normally evaluated in a third party review report issued by the bureau's independent auditors. These reports provide information about data processing controls and detection of any internal control weaknesses.

Third party reviews should be performed by a reputable and competent independent auditor and should address the controls during a specified period of time or as of a given date. The institution should inquire about any significant changes in the bureau's processing procedures if a significant period of time has elapsed since the review. If a third party review report identifies any internal control deficiencies or is unavailable for review, the institution should assure itself that its own internal controls are sufficient to ensure accurate processing or consider switching to another service bureau.

Fraud detection tools

As part of the verification and authentication process the financial institution may wish to utilize data analysis tools that allow them to sort, analyze, segment, sample and extract transactions that meet certain criteria. Many commercial brands of software can be interfaced with the account or loan opening procedures to cross-reference a name, address (P.O. Box or "warm" address), driver's license number and Social Security number. Some financial institutions are moving toward biometrics such as digital signature verification, retinal scan, voice print, facial recognition, and thumbprints (which are, regrettably, only held in file and not actually compared to any state database). Finally, it is helpful if financial institutions have neural networks in place to analyze for both plastic card fraud and check kiting schemes.

Management/officers

Initially, inquiry should be made of officers and directors about any circumstances, like outside business connections or close personal ties, that might present a conflict of interest or opportunity for collusion. Directors should monitor management, who should watch employees for changes in attitude, demeanor and attendance to detect if collusion, embezzlement or extortion may be taking place. As for lending officers, there should be established lending limits and formalized policies for the approval and processing of loans. Fraudulent loans can be a major source of loss for financial institutions where tasks such as loan processing, verification, and disbursement are not divided. The banks should arrange for credit authorization committees rather than singular approval capabilities, and multiple signatures should be required to fund a loan. Also, accurate record-keeping and careful loan documentation are essential.

The audit review

Auditing department

To discourage employees from embezzling funds, all accounting functions should be separated from funds transfer functions, with third-party managerial signatures and reporting required. Formal division of procedures and lines of accountability must be clearly delineated in writing, with periodic random checks performed to verify functionality. Internal and external audits should be performed. External auditors' reports, including those from state and federal agencies, should be subject to internal testing and review to ensure that control mechanisms are actually in place, and that any noted problems are dealt with adequately. The auditing department should be a separate entity, independent of other functions and operational segments, and controlled directly by the financial institution's board of directors. Any discrepancies reported by customers or fellow employees should be routed directly to the auditor's office. Arrangements and schedules for audits should not be disclosed, so that employees do not have a chance to hide or change any schemes. Employees, particularly those in accounting or funding functions, should be required to take vacations in at least one-week increments, to allow time for any discrepancies to surface during their absence.

The auditing area and management have many exception reports and red flag reports at their disposal to monitor employee/customer activity, including:

- File maintenance reports
- Supervisory override reports
- NSF rejection listing
- Excessive activity reports (ATM or plastic cards)
- Kiting detection systems report
- Dormant-to-active account change status
- Employee plastic card, loan and overdraft balances (beware of privacy issues)

Independent auditors can be helpful in evaluating an institution's internal control as part of an external annual audit or, if an institution's size permits, as part of an

ongoing internal audit function. Auditors take two approaches in the study and evaluation of an institution's internal control when performing an audit. One is to evaluate, test and rely on the control structure (i.e., the control environment, accounting systems and operating procedures). The other approach is to obtain an understanding of the control structure and then extensively test the account transactions without relying upon the system. The first approach generally is more efficient from an audit perspective but relies significantly on the presence of effective internal controls. Neither method provides complete assurance that an effective system of internal control exists.

Management may wish to have certain aspects of the internal control environment system reviewed in greater detail, especially those controls not directly related to the financial statements (e.g., access to sensitive customer information), despite receiving assurances from the independent auditor as to the effectiveness of the internal controls. These procedures may be performed by an internal audit department or as a separate external review.

Some questions management may consider in reviewing internal controls:

- Have any deficiencies in internal control been detected that may have a potentially significant impact upon the institution's operations? Do any conditions exist that warrant management's attention but are not considered significant?
- Have the comments on internal control from management letters, internal audit reports or regulatory examination reports been adequately addressed? What other areas should management address? Are there any areas of potential risks that were not addressed?
- Specifically, what are the institution's policies and procedures concerning questionable transactions and illegal payments? What steps have been taken to establish whether appropriate policies exist and are being followed?
- Has an adequate review of the institution's computer-related control functions (or service bureau's functions) been performed?
- What is the exposure to security breaches in computer operations?

- Are there adequate controls in place over the information processed on micro-computers (access to sensitive information on these systems and the existence of contingency plans for these operations)?

The internal auditor performs many of the same functions as the external auditor in larger financial institutions. The primary responsibility is to study, assess and test the system of internal control. Internal auditors also may assist in other areas outside the scope of an external audit review (e.g., evaluate compliance with management policies, perform analyses of operational efficiencies, conduct fraud reviews, etc.).

Objectivity is an important consideration in the work of internal auditors. Are the auditors able to perform their reviews without undue influence or restrictions by management?

How much internal control is enough?

The system of internal control should basically minimize — and ideally eliminate — intentional deviations from prescribed policies, theft and errors made by personnel performing their duties as they understand them.

Even if the system of internal control is well designed and operating as intended, human factors (e.g., employee boredom, personal problems or other distractions) can result in errors. While effective controls should detect significant errors, collusion among employees or an executive overriding policies can defeat any system of internal control and allow irregularities to go undetected. No system of internal control can provide complete assurance that errors or irregularities will be prevented or detected.

What good, then, is internal control if it does not prevent or detect all errors and irregularities? And how much internal control is enough? The answers may be found in the law of diminishing returns. Inevitably, a point is reached in instituting controls beyond which the cost of providing more controls exceeds the potential losses they prevent. Identifying that point is no simple matter. It requires management judgment in weighing the estimate of potential losses against the cost of additional controls.

Developing and implementing a fraud policy

A well-designed policy should protect the financial institution against losses from embezzlement and costly litigation, while promoting a zero-tolerance atmosphere toward fraud through frequent compliance testing by supervisory personnel. The fraud policy will differ from an ethics policy or conflict of interest statement in that, rather than merely defining general standards of behavior, it addresses specific actions that are prohibited and procedures to be followed by management should embezzlement be discovered. The fraud policy should be discussed and signed by each new employee, then updated as part of an annual employment review or employee training workshop.

A fraud policy should be developed by the Board of Directors, the management and legal counsel to set a tone from the top that employee dishonesty will not be tolerated. Integral in the policy is the development of a corporate creed that will help employees recognize their ethical, moral and legal responsibilities toward fiscal assets, computer systems and fellow employees. The policy should establish responsibility for the deterrence, detection and investigation of suspected wrongdoing. The policy will also set guidelines and procedures for handling embezzlement events to reduce exposure to harmful publicity and costly litigation.

Fraud detection and deterrence should follow clear chains of command that cannot be delegated. It is the responsibility of the board of directors to require the implementation of the necessary procedures and internal controls that will provide obstacles for embezzlement. Management is responsible for ensuring the internal controls are established, and that all employees are instructed in the policy guidelines and the proper procedures related to their jobs. It is, then, the duty of a supervisory committee or internal auditor to examine the adequacy and effectiveness of the controls established by management. This duty will necessitate periodic, unscheduled compliance testing to monitor policy adherence. The internal auditor has the highest responsibility for fraud and is expected to develop and incorporate detection procedures into the auditing programs. The internal auditor may also lead any fraud investigation, or he/she may delegate to persons with specific fraud detection experience such as a CPA firm, an outside auditing firm, or state/federal regulatory agency.

The fraud policy must recommend that investigation be undertaken in conjunction with legal counsel to avoid damaging public statements and litigation relating to defamation, false imprisonment, assault and malicious prosecution. The procedures should be delineated for both the release of information and the notification of appropriate regulatory and law enforcement agencies. The financial institution should also be concerned with the effect that knowledge of an employee's dishonest act has upon its fidelity bond, as most contain a clause stating that coverage for an employee ceases when the employer learns of the dishonest act. Note that it is not necessary that this fraudulent act occur while the employee is working at the financial institution. However, it is necessary to give the insurer timely notice of the suspected theft, or payment of the resulting claim could be impacted.

When embezzlement occurs

Financial institutions should have procedures in place for handling a situation involving an embezzlement and note that insurance coverage terminates automatically upon discovery of dishonesty. If a financial institution suspects embezzlement, findings and suspicions may be documented. Any meetings with employees may also be noted. The documentation should be clear, accurate and unemotional. All findings may be verified by conducting an independent review to determine the validity of suspicions. If it is then determined that embezzlement has actually occurred, a consultation may occur with legal counsel and accountants, and a supervisory committee or board (for employee or manager, respectively) should be notified. The initial goal of your effort should be to protect assets and minimize losses.

Only after verification, consultation and notification have occurred should contact be made with the suspected employee. It is important not to make threats, accusations or promises, and to accept any offers of indemnification. It is common for the financial institution to suspend the employee with pay, document any contact with the employee, and be aware of union contracts. Take swift, decisive, consistent action when embezzlement or fraud has been discovered. Measures must be taken to restrict further employee access to accounts and transactions by changing passwords and restricting authorizations. If the embezzlement has been made public, the financial institution should ensure consistency by appointing one spokesperson as public relations liaison. Confidently emphasize the safety and soundness of the institution, and coordinate efforts with other agencies or institutions that may be involved or require information.

After an embezzlement has occurred, it is imperative that an assessment be completed to establish the scope of the breach of ethics involved. A postmortem analysis should be done to determine if the security of any computer systems were compromised. All internal controls and cross-checks should be re-evaluated to help prevent reoccurrence and to encourage a return to normal operation.

Internal controls checklist

This questionnaire is designed to provide information to make you aware of some of the opportunities for fraud, embezzlement and human error that exist within financial institutions. It provides a guideline and is not intended to be all inclusive.

Can you answer "Yes" to these questions?

When embezzlement occurs

1. Does a formal organizational structure exist that clearly defines and imparts authority limits?

2. Is officer approval required for:

   a) withdrawal of funds uncollected, attached or pledged?

   b) submission of substitute documents (e.g., replacement for rejected proof-transit items)?

   c) adjustment to general ledger and cash reserve balances?

   d) disbursement of administrative expenditures? (note: dual signatures should be required for all disbursements)

3. Are external audit reports, internal audit evaluations and examination reviews presented directly to the board of directors?

4. Is the institution's balance of outstanding commitments regularly monitored by management?

5. Are administrative expenditures disbursed from centralized account(s)?

6. Is access to unissued checks, check-signing machines, signature plates and wire transfer equipment restricted from unauthorized employees?

7. Are external audit management letters, internal audit reports and regulatory examination reports reviewed by management and the board of directors?

8. Does the institution have policies and procedures concerning questionable transactions and illegal payments?

9. If the institution uses a service bureau, has a recent review of the bureau's computer-related controls been performed?

Teller operations

1. Are each teller's cash reserves accounted for separately and balanced to an independent control on a daily basis?
2. Are all transactions processed by tellers cleared to proof-transit on a daily basis?
3. Is dual control exercised at all times over the following negotiable instruments: cash reserves, blank CDs and cosigned traveler's checks, money orders and U.S. Savings Bonds?
4. Are dual controls exercised over dormant accounts, new account starter kits and notes that have been charged-off?
5. Do check cashing and withdrawal policies preclude the cashing of checks payable to third parties, corporations, partnerships and other organizations and restrict the withdrawal of uncollected, attached or pledged funds?
6. Are there limits to the amount of funds employees and officers can disburse?
7. Are dual signatures required for all disbursements?
8. Are officers' and employees' checking accounts segregated from customer accounts and identified by a separate series of account numbers?
9. Are officers' and employees' checking accounts reviewed periodically for unusual or excessive activity?
10. Are tellers prohibited from performing functions in other departments?
11. Are the responsibilities segregated for initiating administrative expenditures, preparing negotiable instruments and reconciling transactions?
12. Are transactions to dormant accounts tracked separately and reviewed periodically to unusual or excessive activity?
13. Are account statements mailed to customers on a regular basis?
14. Are all customer inquiries handled independently of the teller and accounting functions?

Wire transfers

1. Do the wire transfer procedures include:

   a) confirmation of all incoming and outgoing requests, including callback verification to an authorized phone number for requests submitted verbally?

   b) tape recording of all verbal requests and retention of all wire transfer records?

   c) the use of prenumbered transfer request forms and transfer control registers?

   d) reconciliation of the transfers processed with those requested?

2. Are the responsibilities segregated for originating, processing and reconciling wire transfers?

Proof-transit

1. Are proof-transit control totals prepared by branch operations and reconciled by an individual(s) who is independent of the encoding process?

2. Are batch control registers used to control all production through the department?

3. Are batch control registers reconciled to production on a daily basis?

4. Are the signatures for all in-clearing checks over a specified limit verified to an approved authorization card?

5. Are proof-transit employees prohibited from performing functions in other departments?

6. Are the responsibilities segregated for proof-transit encoding, batch control processing and reconciliation of control totals?

Lending

1. Do lending policies comply with industry/secondary market standards?

2. Do lending policies address lending authority, loan-to-value ratios, appraisal criteria, inventory and inspection of collateral and repossession of assets?

3. Do loan documentation procedures address:

   a) the preparation of loan document checklists?

   b) application review procedures?

   c) credit review procedures?

   d) procedures for adjustments, renewals and extensions?

   e) physical control of loan documents?

4. Are the following monitored at least on a quarterly basis?

   a) concentrations of loans within particular industries or geographical areas?

   b) delinquent loans?

   c) graded loans?

   d) the allowance for loan losses?

   e) investments in foreclosed property?

5. Are loan balances verified annually at least on a sample basis, by an external audit firm or an internal audit staff?

6. Are detailed statements of the loan balances, including charge-offs and pledged collateral mailed to borrowers at least annually?

7. Are the following functions performed by individuals independent of the lending function:

   a) credit reviews?

   b) property appraisals?

   c) loan disbursements?

   d) payment processing?

   e) compilation of delinquent loan information?

   f) management and disposal of repossessed collateral?

   g) adjustments to employee loans?

   h) adjustments, renewals and extensions to the loan applications?

8. Are the loan files reviewed for completeness by a senior lending officer prior to disbursement of the loan proceeds?

9. Are loan officers restricted from posting account entries and reconciling account balances?

10. Are charged-off loans segregated and maintained under separate accounting control?

Investments and trust

1. Does the institution's investment strategy address:

    a) investment objectives?

    b) authorization limitations?

    c) industry and geographical concentration?

    d) holding positions?

    e) correspondent relationships?

    f) distinctions in portfolio vs. trading accounts?

    g) reporting of investment gains and losses?

2. Does an investment committee regularly review investment transactions, transfers between portfolio and trading accounts, gains and losses, and the composition of the investment portfolio?

3. Is the market value of investments verified independently and recorded on a regular basis?

4. Is dual control exercised over all investment securities?

5. Are investment securities adequately segregated from securities held in trust?

6. Are trust transactions periodically reviewed to ensure that the transactions are in accordance with the trust agreement?

7. Are the trust accounts reconciled to a control total by an employee who has no involvement with investment transactions?

8. Are trust statements periodically mailed to the parties of interest?

Computer manipulation and data processing

1. Has a strategic information systems plan been developed?
2. Has an overall priority plan been developed for systems development and maintenance?
3. Do systems development policies and documentation procedures exist?
4. Do data access and security standards exist?
5. Is dual control exercised over the monitoring of ports and usage logs for irregularities or unauthorized access attempts?
6. Are procedures documented for the backup of all data, either automatically (nightly batch) or on a schedule? Who manages the security of the backup data?
7. Has a data security policy been drafted and has each employee agreed to comply with the policy? Do you require the employee to sign this policy annually?
8. Are data processing records physically secured?
9. Are security codes and passwords periodically revised?
10. Are security codes for terminated employees immediately deleted from the system?
11. Is access to remote terminals and communication lines restricted, especially those connected to a communications network?
12. Are there adequate controls in place over the information processed on microcomputers including access to sensitive information on these systems, and the existence of contingency plans for these operations?
13. Does the data processing system provide automatic audit trails for transaction verification?
14. Does the institution have a business contingency plan to address disasters and interruptions in service? How and where is backup data stored?

15. Are rejected transactions corrected promptly and re-entered into the system?
16. Are critical master file transactions supported by written documentation and reviewed by an individual who is independent of the data processing function?
17. Are run-to-run batch control totals prepared to control master file changes?
18. Are ATM account identification codes strictly controlled by an individual with no data processing responsibilities?
19. Are data processing and the reconciliation of batch control totals segregated from systems applications?
20. Are systems development and programming personnel restricted from customer file access?
21. Are customer discrepancies resolved by individuals outside the data processing function?
22. Are computer applications personnel restricted from implementation of program changes?
23. Is a library of computer programs maintained and controlled?
24. Does a person or group without data processing responsibilities control the input and output of production through the department?
25. Who monitors and audits the activities of the information technology department, including the network administrator?
26. Are electronic barriers or firewalls present on all computer networks that interface with the internet to prevent uninvited access by hackers proficient at breaching password protection?
27. Are internet banking users provided with unique PINs or passwords to prevent unauthorized entry into the system?
28. Is all sensitive financial and proprietary information encrypted, with access restricted to those in possession of frequently changed passwords?
29. Is a virus scan run against all programs/systems on a regular basis?

Plastic cards

1. To monitor for fraudulent plastic card facilities, do you regularly review a sample from new accounts, requested limit increases, overlimits, change of address or name, and reissues (for lost/stolen cards)? Do you verify such items by telephone?
2. Are you cautious about issuing multiple cards to the same individual, in case they may be sharing or selling the extra card to an unauthorized party?
3. Do you red flag any approval ending in $.00 that may represent a fraudulent cash advance?
4. Is there a neural network in place to help detect plastic card fraud by examining accounts for possible patterns of fraud or fraudulent transactions? If so, are you alert for situations where employees are making manual approvals outside the network?

Automatic teller machines

1. Is access to customer PIN codes restricted from unauthorized employees?
2. Is dual control exercised over all ATM cash reserves?
3. Are all ATM transactions settled on a daily basis?
4. Do the ATM machines have withdrawal limitations?
5. Are ATM cards and PIN numbers mailed separately to the customer?
6. Do the customer statements provide a clear indication of ATM transactions and the procedures a customer should follow to resolve any discrepancies?
7. Are all customer-initiated discrepancies resolved promptly?
8. Does the ATM system have controls to prevent the withdrawal of uncollected, attached or restricted funds?

Summary

As an officer or director, one of your primary responsibilities is to protect and preserve your institution's assets. Maintaining a sound system of internal controls is essential.

Embezzlement is a constant risk that can never be completely prevented, but can be mitigated through a strict internal control policy, effective audit techniques and a zero-tolerance atmosphere toward fraud. All financial institutions can devise fraud prevention strategies and verification tools to help prevent and combat future losses. However, as we have pointed out several times in this treatise, no system of internal controls yet devised can provide absolute protection from all acts of fraud or theft.

Thus, it is imperative that your institution's officers and employees be bonded in an adequate amount. Furthermore, provision should be made for periodic reviews of this vital protection to be sure that the amount of coverage is adequate in relation to your institution's current resources.

Ask your insurance agent or broker for full details about Zurich's program. We have been a leader in providing financial institution bonding and insurance protection for over 110 years. Zurich can help protect your institution from financial loss.

Zurich Services Corporation

1400 American Lane, Schaumburg, Illinois 60196-1056
800 982 5964 www.zurichservices.com

ISO 9001:2000
Quality-Assured Solutions Provider

A1-13678-C (11/06) 06-3783

ZURICH®