



FINANCIAL OVERSIGHT, INTERNAL CONTROLS, FRAUD, AND ENSURING ADEQUATE RESOURCES

Why this topic...

Sharon Rice, formerly the executive director of the Medical Association of Atlanta, pleaded guilty to one count of wire fraud in federal district court Thursday after stealing nearly \$300,000 from the non-profit organization. During that time, Rice wrote almost **\$300,000 in checks to herself** -- in addition to her allotted payroll amounts. She also wrote several checks to her medical association Visa card to pay for personal expenses. She was able to hide these payments from the board of directors and accountants by making fictitious entries in the company's bookkeeping and forging several co-signatures on checks.*

* *Atlanta Journal Constitution: www.ajc.com/news/nonprofit-executive-pleads-guilty-551760.html*

Why this topic...

- A Menifee woman who handled fundraising for the Boys & Girls Clubs of Southwest County has been charged with embezzling a laptop and two vacations to New York from the nonprofit, prizes meant to be doled out as part of the group's annual fundraiser last year.*
- Samuel Bunner, former director of emergency services for the Eastern Panhandle Chapter of the American Red Cross, admitted that he stole more than \$30,000 from the organization. Berkeley County Assistant Prosecutor Tim Helman says Bunner was authorized to put cash on Red Cross debit cards, but instead of giving the cards to disaster victims he would cash out the money himself.**

*North County Times: www.nctimes.com/news/local/temecula/article_18b664a1-fa04-599d-979e-4004d98a38d5.html

** MetroNews: www.wvmetronews.com/news.cfm?func=displayfullstory&storyid=46519

Why this topic...

- A federal grand jury indicted a former United Way of Central Maryland employee on charges that she bilked the nonprofit out of **more than \$400,000** by steering deposits to a bank account she had allegedly commandeered. Dorothy Shields Talbot, 48, who worked in United Way's finance department from 2001 through 2010, was charged with wire fraud. A statement from the Maryland U.S. attorney's office says she had been responsible for depositing donations into a corporate bank account.*

**The Baltimore Sun: http://articles.baltimoresun.com/2011-04-28/news/bs-md-united-way-steal-20110428_1_bank-account-indictment-fraud-charges*

Why this topic...

- A Neenah woman has pleaded no contest to three counts for **stealing nearly \$500,000** from a nonprofit center that supplies donated blood to hospitals. Tina Jacobsen, 50, was convicted of three counts of theft. Jacobsen was an account specialist at Community Blood Center in Grand Chute. The criminal complaint said she used fraudulent expense reimbursements and also drafted checks to herself that were intended for vendors.*

**Channel2000.com: www.channel3000.com/news/29720963/detail.html*

Fraud and Controls

- These frauds could not happen to us... they only happen at larger organizations or smaller organizations.
- We review budget to actual costs closely.
- What are board members to do? We are volunteers who have full time jobs and rely on the audit to identify issues.
- Our Accounting person has been with us for years and has proven to be trustworthy.
- We are too small to have best practices.
- We have an experienced CEO who closely monitors operations and activities.

Control/Fraud Responsibilities

- Assess fraud risks
- Assess controls
- Have management communicate controls and changes in control when they occur
- Ask the external auditor questions during their planning and exit presentations
- Set expectations on roles (Board vs. management)

One Resource:

Managing the Business Risk of Fraud: A Practical Guide

- Sponsored by The Institute of Internal Auditors, the American Institute of Certified Public Accountants and the Association of Certified Fraud Examiners
- It can be found at:
http://www.aicpa.org/interestareas/forensicandvaluation/resources/fraudpreventionanddetectionresponse/downloadabledocuments/managing_business_risk_of_fraud.pdf

Key Items In the Publication

- Fraud Risk Governance
 - Fraud risk management program should be in place
 - Written policy to convey expectations of those in charge in managing fraud risk
 - Establish tone a top
 - Establish a hotline/means of communication
 - Consider training and communication of fraud risks
 - Fraud risk assessment (Appendix A)
 - Conflict of interest policy

Fraud Risk Assessment

- Approach
 - Identify the risk (e.g., cash receipts can be taken/not properly deposited)
 - For each risk assess:
 - Likelihood
 - Significant/impact
 - Affected areas
 - Risks assessment before controls
 - Identification of controls
 - Identifying who tests/monitors the controls
 - Assess the residual risk

Areas of Concern

- Management override
- Fraudulent financial risk
- Misappropriation of assets
- IT risks
- Compliance/regulatory
- Reputation
- Other
 - Appendix A

Controls

- COSO (Appendix B) defines internal control as a process, effected by an entity's board of directors, management and other personnel. This process is designed to provide reasonable assurance regarding the achievement of objectives in effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations.

Control Areas to Consider

- Information systems
- Financial close/general ledger
- Financial reporting
- Monitoring of subrecipients
- Recording/oversight of grants (federal and other)
- Paying of bills/disbursements
- Paying of employees/human resources
- Processing and recording of contributions/donations/cash receipts
- Inventory
- Fixed Assets
- Investments
- Cash management/debt
- Other

Controls

- Management should report/communicate controls to Board/Finance Committee
- Auditors can report on testing results
- Internal audit can verify on test basis
- Controls should be documented

Cost Effective Monitoring Controls

- Key policies should be reviewed by the Board/Finance committee
 - Authorization matrix
 - Credit cards/debit cards if used (consider if necessary)
 - Conflict of interest
 - Reserve policy (cash and equity)
 - Use of restricted funds
 - Endowment
 - Investment
 - Fraud
 - Other

Cost Effective Monitoring Controls

- Obtain understanding (updated at least annually) of Accounting personnel roles and responsibilities
 - Finance/Audit Committee should meet with Accounting team at least annually to ask about any issues/concerns and have them explain duties/roles
 - Consider having other personnel (e.g., IT, operational personnel, etc.) meet periodically to update Board on their roles, issues, concerns and processes

Cost Effective Monitoring Controls

- If Accounting resources are limited, have the Finance Chair and/or Board President receive the bank statements from the Bank to review prior to providing to Accounting to reconcile
 - Look for payments to cash
 - Identify unusual payments
 - Review for checks out of order
 - Review for unusual trend in deposits
 - Review for wires/ACH activity
- Review insurance coverage and who is listed/positions covered

Cost Effective Monitoring Controls

- In the area of payroll,
 - Consider having Finance Chair/Board receive payroll registers/summary directly if third party service is used; a copy/summary if internally processed
 - Review W2 for unusual amounts
 - Received quarterly list of employees and titles
 - Approve/review any non salary payments (e.g., bonus, vacation pay, etc.)
- Review insurance coverage annually
- Review activities with related parties

Cost Effective Monitoring Controls

- Obtain a computer generated list of disbursements
 - Review monthly
 - Review vendor summaries
- Require second signature on check
- Discourage use of stamped signatures
- If Board member is signer, should not sign check without support attached/appropriately approved documentation. Consider documenting the “support” reviewed. Ask questions as appropriate.
- Assess need for use of credit cards/debit cards; if used, have management provide list of users and describe how monitored.
- Understand who can and who does post journal entries
- Key estimates
 - Have management explain methodology
 - Have management review calculations (e.g., Aging)

Cost Effective Monitoring Controls

- Have IT describe operations
 - At least annually obtain an update
 - Key procedures
 - Number of personnel/use of third parties
 - Software aging/hardware needs
- IT should develop a long-term budget regarding needs
- Inquire as to controls and oversight (e.g., who is monitoring)
 - Appendix C

Cost Effective Monitoring Controls

- Key financial data
 - Review complete set of GAAP financial statements monthly/quarterly
 - Review budget to actual income statement comparison - By program and In total
 - Ask for a MD&A explanation to be provided
 - Have management explain purpose of restricted assets/net assets
 - Inquire as to frequency of balance sheet reconciliations/understand policy
 - Obtain aging of accounts receivable (grants, pledges, other) and accounts payable
 - Review rolling 12 month cash forecasts

Cost Effective Monitoring Controls

- Grants
 - Obtain explanation of key grants (ideally before approval) including risks, complexity, monitoring process, who is accountable, method of reimbursements, description of controls, key risks, list of subrecipients if practical, expiration date, monetary amount of program, how awarded, last monitoring/audit date, etc.
 - Obtain updated list at least quarterly by grant and status
 - Require all monitoring reports/audits to be presented to the Board
- Contributions
 - Obtain an updated list at least quarterly which agrees to financial statement
 - Determine level of detail (e.g., large amounts rather than all), list purpose, date, donor, amount, etc.

Cost Effective Monitoring Controls

- Contributions
 - Require acknowledgement letter for all
 - Consider the cost effectiveness of having the receptionist/someone outside of Accounting log in checks received and have someone in Accounting sign for the checks. Once the deposit is made, the receptionist should mark date of the deposit.
 - Require reconciliation of fund raising data to accounting data
 - Obtain updated list of pledges, due dates, terms and amounts
 - Have management explain release in net restricted net assets at least annually

Cost Effective Monitoring Controls

- Cash Management
 - Request a rolling 12 month cash flow projection
 - Ask management to explain how investments are monitored, controlled and safeguarded as well as reliance on controls of any third parties
 - Receive periodic reports on the market value/changes in investments
 - Obtain an understanding of line of credit/debt terms and renewal
 - Collateral requirements
 - Covenant requirements
 - Debt service requirements

Cost Effective Monitoring Controls

- Other Areas
 - If inventory, have management describe results of any physical counts/perpetual to physical differences
 - Review investments for compliance with investment policy
 - Understand tax effect of new initiatives
 - Require special events to be reported by those involved in process to describe gross receipts and related costs (could be part of budget process), how receipts are controlled, how costs are approved paid, etc.
 - Require periodic verification of fixed assets
 - Have executive session with external auditors
 - Require planning and exit meetings with auditors
 - Ask questions about accounting policies, adjustments, controls tested, etc.

Exercise 1

- A non profit is proud of the fact that 95% of its fund raising efforts go directly to the organizations' purpose. Non operational costs are closely scrutinized. The CEO has been able to ensure that the Accounting Department only needs 2 fulltime personnel, changing procedures such as paying checks once a month, limiting the use of company credit cards, purchase orders, etc., to ensure work flow for the Controller and the related clerk enable them to only work 40 hours a week.
- The CEO just got off the phone with another CEO who is trying to streamline his overhead costs. He described his folks as very trust worthy and honorable. He described how he reduced cumbersome procedures to streamline the data flow to Accounting as well as tasks that each of the Accounting persons performed to minimize having to hire additional personnel.

Exercise 2

- NOP Executive Director (ED) will be on an overdue 2 week vacation. The Board is very supportive as the ED has just completed a \$2 million capital raise. Before he leaves, the ED decides to streamline the disbursement process while he is out since all have been working so hard.
- Since only he and a Board President are the ones to sign checks and the Board President is in the midst of tax season, the ED leaves just 3 blank signed blank checks to cover any emergency payments.

Areas to Consider

- Having no one outside of the Accounting Department review the bank statement
- Use of credit cards/debit cards
- Profitability of programs/initiatives
- No one outside the Accounting department reviews checks/disbursements
- No one outside of payroll reviews pay/pay rate changes

Appendix

- Appendix A – Example Fraud Risks
- Appendix B – What is COSO
- Appendix C – Example IT Controls
- Appendix D – Handouts

Appendix A – Example Fraud Risks

Fraudulent Financial Reporting

- **Incentives/Pressures**
- Is the organization financially stable?
- Have raises/bonuses been provided regularly to employees?
- Is the organization declining profit/significant cash need?
- Is there a threat of a major source of funding being terminated or significantly reduced?
- Does the organization receive significant contributions based on allocation formulas tied to the organization's budgeted or actual revenues that may create an incentive for management to alter financial reports to maximize the contribution allocation?
- Is the organization under significant pressure to obtain additional grants or contributions to fund major programs or expenditures?
- Is organization is unusually dependent on debt financing or has a marginal ability to meet debt repayment terms?
- Does the organization's financing agreements have debt covenants that are difficult to maintain?
- Is organization is under significant pressure to meet budget?
- **Opportunities**
- Does the organization have assets, liabilities, revenues, or expenses based on significant estimates that involve unusually subjective judgments or uncertainties that are difficult to corroborate, or that could significantly change in the near term in a manner that may be financially disruptive to the organization?
- Does the organization has diverse programs with multiple provisions of donor restrictions; statutes; or grant, trust, or contractual agreements)?e funding sources and complex compliance requirements (such as complex
- Is Management dominated by a single individual (such as the executive director, development director, or a program director) or a small group without compensating controls, such as effective oversight by a board of directors or audit committee?
- Is there ineffective oversight over financial reporting and internal control by the board of directors or audit committee?
- Has there been a high turnover in management-level employees, board members, or counsel?
- **Attitudes/Rationalizations**
- Does Management effectively define, communicate, implement, support, or enforce the organization's values or ethics?
- Does Management communicates or demonstrates appropriate values or ethics.
- Does Management continually attempt to justify marginal or inappropriate accounting on the basis of materiality?
- Does Management frequently and inappropriately override the organization's control policies and procedures.
- Does Management undervalue the importance of the accounting function and financial reporting.
- Is there failure by management to respond to specific inquiries or to volunteer information regarding significant or unusual transactions, only providing the information reluctantly when specifically asked.
- Other situations indicating a strained relationship between management or the board of directors and the current or predecessor auditor.

Misappropriation of Assets

- **Incentives/Pressures**
- Are there
- Known or anticipated future employee layoffs
- Unfavorable recent or anticipated changes in employee compensation or benefit plans
- Failure to receive promotions or other expected rewards
- Conditions that indicate adverse relationships between the organization and its volunteers with access to assets susceptible to misappropriation, such as failure to receive proper recognition or other expected rewards for volunteer efforts
- **Opportunities**
- Does the organization maintain or process large amounts of cash?
- Does the organization receive numerous small dollar-value contributions for which the donors receive no acknowledgment?
- Are cash and other contributed assets received by numerous departments, such as development, programs, administration, and accounting?
- Is the organization's inventory easily susceptible to misappropriation (for example, due to small size, high value, or high demand)?
- Does the organization have significant amounts of assets, such as cars, susceptible to personal, nonofficial use?
- Is the organization susceptible to fraudulent, unauthorized disbursements (such as vendor, payroll, or sub recipient disbursements) being made in amounts that are material to the financial statements?
- Is there a lack of appropriate segregation of duties that is not mitigated by other factors (such as effective management or board oversight)? Does the organization lack job applicant screening procedures when hiring employees with access to assets susceptible to misappropriation?
- Does the organization lack screening procedures for volunteers with access to assets susceptible to misappropriation?
- Does the organization have an appropriate system for authorizing and approving transactions (for example, in purchasing or payroll disbursements)?
- Does Management have an inadequate understanding of IT that enables IT employees to perpetrate misappropriation? Is there a lack of adequate access control over automated records, including controls over and review of computer systems event logs (for example, the audit trail functionality of standardized accounting software packages is not used or can be turned off by employees)?
- Is there a lack of an appropriate system for authorizing and approving the use of the organization's purchase cards or credit cards.
- **Attitudes/Rationalizations**
- Do employees or volunteers with access to assets susceptible to misappropriation disregard the need to adequately monitor and safeguard assets?
- Do employees or volunteers with access to assets susceptible to misappropriation disregard internal controls designed to prevent or detect misappropriation, for example, by overriding controls or failing to correct known deficiencies in controls?

Appendix B – What is COSO

- The Committee of Sponsoring Organizations' (COSO) mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations.
- COSO was organized in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
- The National Commission was sponsored jointly by five major professional associations headquartered in the United States: the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), Financial Executives International (FEI), The Institute of Internal Auditors (IIA), and the National Association of Accountants (now the Institute of Management Accountants [IMA]). Wholly independent of each of the sponsoring organizations, the Commission included representatives from industry, public accounting, investment firms, and the New York Stock Exchange.
- The first chairman of the National Commission was James C. Treadway, Jr., Executive Vice President and General Counsel, Paine Webber Incorporated and a former Commissioner of the U.S. Securities and Exchange Commission. Hence, the popular name "Treadway Commission." Currently, the COSO Chairman is David Landsittel.

Appendix C – Example IT Controls

- All outside service providers used by the entity are evaluated to determine those who provide material financial services that may impact controls.
- All outside service providers used by the entity are evaluated to determine those who provide material financial services that may impact controls.
- A backup and data retention policy/schedule exists, specifying how often backups are to be performed, how long they are to be retained, and where the backup media is to be stored.
- Application data and file server recovery procedures are tested at least annually to ensure data integrity and recovery.
- Appropriate environmental controls (such as fire/smoke detection, temperature controls, and alternate power supply) exist to ensure the security and reliability of equipment.
- A process exists to ensure that systems incidents, problems, and errors are reported, analyzed, and resolved timely.
- An information security policy exists that defines information security objectives. This policy is supported by documents standards and procedures where necessary.
- Procedures exist and are followed to ensure timely action relating to requesting, establishing, issuing, suspending, modifying, and closing user accounts, including proper authorization.
- User access rights are removed or suspended in a timely manner when employees are terminated. Standards exist to define timeliness requirements for various situations (i.e., voluntary or involuntary termination).
- User access rights (network, application, etc.) are granted on a need-to-know, need-to-do basis that considers appropriate segregation of duties. Review of access to system occurs at least annually by key users to verify segregation of duties.
- Procedures exist and are followed to maintain the effectiveness of authentication and access mechanisms (e.g., password length, password history, password expiration, and lockout for failed attempts).
- Access to IT facilities is secure/restricted to authorized users.
- Changes to key systems are approved and tested by users
- Adequate segregation of duties within IT exists