Department of Finance and Management
Financial Operations Division
http://finance.state.vt.us/

DECEMBER 2006 Volume IV

INTERNAL CONTROL NEWS

The purpose of this quarterly newsletter is to provide departments with articles on good business practices, internal controls, and responsibilities. Through articles intended to promote educational and professional development opportunities for employees, this newsletter seeks to raise awareness across state government on the importance of internal controls. We hope that by providing this array of information, we can keep you informed of internal control related activities, and help you implement and maintain effective controls in your areas of operation.

Occupational Fraud

In their **2006 Report to the Nation on Occupational Fraud & Abuse** the **Association of Certified Fraud Examiners, Inc. (ACFE)** studied 1,134 cases of occupational fraud reported between January 2004 and January 2006 by a certified fraud examiner. Below are some interesting facts and analysis from the ACFE report:

- Occupational Fraud is defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets.
- Occupational fraud schemes can be difficult to detect; the median length of time of the schemes in this study was 18 months from the time the fraud began until it was detected.
- Most of the occupational fraud schemes in this study were committed by employees in the accounting department (30%) or by upper management/executive-level employees (20%).
  - **This is more likely reflective of increased access and opportunity to commit fraud by these employees rather than an overall difference in the level of honesty from other employees.**
- Less than 8% of the perpetrators had convictions prior to committing their frauds; although background checks on new employees can be a valuable anti-fraud tool, the report suggests that other measures such as anonymous reporting systems, fraud training, and surprise audits can have more significant impact in detecting fraud.
  - **The VT State Auditor's Office maintains a confidential line at 1-877-290-1400 to report suspected financial fraud, abuse, or corruption in State Government.**
- The median loss caused by all fraud schemes studied was $159,000, with nine cases in excess of a billion dollars.
- All occupational frauds fall into one (or more) of three major categories:
  - Asset misappropriation – any scheme that involves the theft or misuse of an organization's assets (e.g. fraudulent invoicing, payroll fraud, skimming revenues, theft of equipment/supplies). % Cases: 92% Median Loss: $150K
  - Corruption – any scheme in which a person uses his or her influence in a business transaction to obtain an unauthorized benefit contrary to that person's duty to his or her employer (e.g. bribes/kickbacks, illegal gratuities, undisclosed conflict of interest, extortion). % Cases: 31% Median Loss: $538K

- **Fraudulent statements** – falsification of an organization's financial statements to make it appear more or less profitable (e.g. booking fictitious sales, recording expenses in wrong period). % Cases: 11% Median Loss: $2M

Percentages exceed 100% as several cases involved schemes that fell into more than one category.

- Misappropriation of cash (including currency, checks, and money orders) was by far the most common type of asset misappropriation. The eight common methods, with examples, by which employees misappropriate cash from their employers are:
  - **Skimming** – stealing money before it is entered into the books
  - **Larceny** – stealing cash-on-hand
  - **Billing** - billing for fictitious goods/services through a shell company, submitting invoices for payment of personal items
  - **Expense Reimbursements** - claims for personal travel or non-existent meals
  - **Check Tampering** - making out blank checks to themselves or an accomplice, stealing outgoing vendor check and depositing into own account
  - **Payroll** - claiming overtime for un-worked hours, adding ghost employees
  - **Wire Transfers** - wiring of funds from employer's bank account to employee or accomplice controlled account
  - **Register Disbursements** - fraudulently voiding register sales and stealing the cash
- Occupational fraud was initially detected by the following methods (with % of cases): •**Tip** (34%) •**By Accident** (25%) •**Internal Audit** (20%) •**Internal Controls** (19%) •**External Audit** (12%) •**Notified by Police** (4%)
  - Employees were the most common source of **tips** but more than 1/3 of the tips came from outside sources such as customers and vendors.

Percentages exceed 100% as in some cases respondents identified more than one detection method.

- As **tips** and **accidental discovery** were the two highest detection methods this suggests that organizations need to do a better job of proactively designing controls and audits to identify fraud.
  - Organizations should conduct anti-fraud training to educate their employees on how to recognize and report illegal conduct.
  - Organizations should generally seek to foster open channels of communication among employees and all levels of management so that questionable conduct can be brought to light before it develops into outright illegal activity.

In the News: Expense Abuse

Over the past year there have been reports about the misuse of public funds by executives within two Vermont government organizations. These acts not only resulted in serious disciplinary consequences for the offenders but also lead to negative public perception of these organizations and government in general. Each employee with the authority and ability to spend public funds, whether through credit cards, procurement cards, employee expense accounts, petty cash, travel advances, or purchase requisitions, has been entrusted to use the State's funds wisely, prudently, and in accordance with governing laws and regulations. To minimize and avoid expense transactions from being classified as excessive or abusive, here are some general principles to follow:

- Management sets the ethical tone for the organization by establishing, and adhering to, the principle that expenditures should be neither excessive nor inappropriate. Some examples of expenditures that *may* set the wrong ethical tone and/or harm public perception are: • meetings at higher-priced establishments when there are viable, lower-cost options available; • use of petty cash funds for office entertainment

expenses; •incurring excessive or additional travel-related expenses for the convenience of the employee.

- Authorized approvers are responsible for having sufficient knowledge of the business purpose and accuracy of the expenses being claimed. Employees should ask questions or seek additional documentation if they do not have sufficient information to validate the propriety of the transaction. Report questionable transactions or activity to appropriate supervisors or use the Vermont State Auditor's confidential line at 1-877-290-1400 to report suspected waste, fraud, or abuse.
- Employees responsible for incurring expenses must ensure the expense is for authorized purposes and is an appropriate use of public funds. Moderation and discretion should be used when expending public funds. Expenses should serve a public purpose and be consistent with the organization's mission and objectives; expenses should not be for the purpose of providing a personal benefit to any employee, or give the appearance of doing so, unless there is a valid and documented business benefit to the organization.

Protecting Confidential Data

In the often frenetic pace of our jobs it's easy to overlook some of the basic precautions to protecting confidential data in and around our workplaces. The following items are not revolutionary ideas but rather common-sense reminders of the steps we can take to minimize risk and provide a more secure work environment.

from VISA.com…

- ✓ **Empty the mailbox.** Never leave outgoing or incoming mail in pick-up boxes overnight. This is your best defense against possible off-hour mail snoops.
- ✓ **Watch the fax**. A document sitting on the fax waiting for pick-up is an open invitation for prying eyes. Try to stand by the fax machine to receive sensitive information as soon as it comes in.
- ✓ **Make copies carefully.** Private matters can go public fast when juicy stuff gets left behind. When making copies of sensitive documents, remember to grab your originals off the copy machine.
- ✓ **Use the shredder.** Always shred sensitive information before dumping it in the trash bin. If you can't shred, use receptacles designed for sensitive paper disposal.
- ✓ **Leave discrete voicemail messages.** You never know who's standing within earshot of someone's work area, so avoid leaving a detailed voice-mail message if it involves sensitive information.
- ✓ **Protect your onsite ID**. Play it safe with your ID badges, office keys, and building-entry codes. Protect them as you would your own credit cards and cash.
- ✓ **Keep things private in public.** When you're in a public place, think twice before discussing proprietary information or any details about sensitive projects. You never know who's listening.
- ✓ **Identify strangers.** Don't make it easy for an outsider to pull an inside job. If you see an unfamiliar face roaming around your office, step up and ask if you can assist. Make your presence known.
- ✓ **Be careful with your documents.** Remove all sensitive materials from your work area when you're not using them or at the end of the day. Be sure to lock them in the appropriate file cabinets, desk drawers, etc.

- ✓ **Note what's on your screen.** Those account numbers and financial details on your computer screen are intended for your eyes only! To keep it that way, use a glare screen to minimize easy information access.
- ✓ **Limit cell phone conversations**. Anyone can listen in on your cellular conversations. All it takes is a good ear and a decent scanner. Avoid sharing any sensitive information over a phone.

  - ➢ Refer to the Vermont Chief Information Officer's website for **data protection** policy & standards (*currently in draft form*) of electronically stored data.

Test Your Knowledge of Internal Controls

(Answers are at the end of the newsletter.)

1. The definition of internal control developed by the Committee of Sponsoring Organizations (COSO) addresses the achievement of objectives in the following categories: (1) the reliability of financial reporting, (2) the effectiveness and efficiency of operations, and
   a. Safeguarding of entity assets.
   b. Compliance with applicable laws and regulations.
   c. Effectiveness of prevention of fraudulent occurrences.
   d. Incorporation of ethical business standards.

2. "Control procedures whose effectiveness depends on separation of duties can be circumvented by collusion." This statement is an example of…
   a. Incompatible duties.
   b. A department's risk appetite.
   c. A processing inefficiency.
   d. An inherent limitation of internal control.

3. Auditors bear the primary responsibility for establishing effective internal controls.
   a. True
   b. False

4. Management fails to provide leadership in maintaining the department's ethical tone when it…
   a. Engages in related-party transactions.
   b. Circumvents or overrides established internal controls.
   c. Fails to enforce appropriate disciplinary practices.
   d. All of the above.

5. "Employees responsible for data entry of accounts payable vouchers in VISION should not be responsible for approving payment of these vouchers" is an example of what internal control activity:
   a. Separation of duties.
   b. Safeguarding of assets.
   c. Documentation.
   d. Reconciliation.

6. Which of the following expenditures is an unallowable use of petty cash according to VISION Procedure #5: Petty Cash?
   a. Postage to meet a filing deadline.
   b. Cash bonus to an employee for outstanding performance.
   c. Incidental supplies from a local store.
   d. All of the above.

7. Per Best Practices #1: Cash Receipts and Deposits, all cash receipts (i.e. currency, coins, checks, etc) received by a department should be deposited:
    a. Daily regardless of amount.
    b. At least monthly.
    c. Daily when in excess of $500, but no less frequently than weekly.
    d. When most convenient to the department.

8. When executive management establishes strong, clearly stated support for internal control it is most commonly referred to as:
    a. Creating reasonable expectations.
    b. Raising the bar.
    c. Demanding excellence.
    d. Setting the tone at the top.

9. As defined in VISION Procedure #1: Asset Management, a capital asset is:
    a. A physical resource that costs at least $5,000 and provides future economic benefit for a minimum of two years.
    b. A long-term, physical resource of considerable value held for business use and not intended to be sold or consumed for at least one year's time.
    c. A physical resource that costs at least $5,000 and provides future economic benefit for a minimum of three years.
    d. None of the above.

10. Internal controls may be preventive or detective (and/or corrective). Which of the following is an example of a *preventive* control?
    a. The use of batch totals.
    b. Reconciling the accounts receivable subsidiary ledger with the general ledger control account.
    c. Requiring two persons to open mail that may contain cash receipts.
    d. Preparation of bank reconciliations.

Important Dates

December 31st	Issuance date for FY 2006 Comprehensive Annual Financial Report
January 3rd	Legislature Convenes
January 23rd	Deadline for Governor's budget address
January 31st	Deadline for issuing Forms 1099-Misc to recipients
***Week of* February 5th**	Scheduled availability of VISION Financials 8.8 Sandbox for end-users
***Week of* March 5th**	Scheduled "Go-Live" for VISION Financials 8.8

Answers to Test Your Knowledge of Internal Controls:

1. (b); 2. (d); 3. (b); 4. (d); 5. (a);

6. (b); 7. (c); 8. (d); 9. (a); 10. (c);