Volume 1
Issue 2

IN CONTROL

DECEMBER 2007

DEPARTMENT OF ADMINISTRATIVE SERVICES
STATE CONTROLLER'S DIVISION

Antifraud Programs and Controls

The April 2007 issue of ***In Control*** introduced ***Statement of Auditing Standards (SAS) No. 112–Communicating Internal Control Related Matters Identified in an Audit.*** The purpose of this standard is to provide guidance to auditors on communicating internal control deficiencies identified in an audit of financial statements. Specifically, the standard requires auditors to communicate, in writing, to management, *significant deficiencies* and *material weaknesses* identified during the audit.

Under SAS No. 112, there are certain areas of deficiencies that generally are considered *at least* significant deficiencies in internal control and, therefore, must be communicated to management in writing. One of these areas is deficiencies in **antifraud programs and controls**. In fact, SAS No. 112 requires auditors to treat fraud of any magnitude on the part of senior management as *at least* a significant deficiency and a *strong indicator* of a material weakness in internal control.

What can state agencies do to strengthen antifraud controls and build an effective antifraud program? Where can agencies find resource materials and get training? The answers to these questions will be the subject of a series of articles, starting with this issue of ***In Control.***

We will begin by defining the term "fraud" and looking at the various types of fraud, paying special attention to occupational fraud. Later, we will examine the "fraud triangle" to gain a better understanding of the motivators behind fraud. Along the way, we will identify some of the actions agencies can take and the resources available to help reduce the risk of fraud, including training opportunities and online resources.

Fraud Defined

Although many authoritative fraud definitions exist, they all have one thing in common, *scienter*, the intent to deceive. Common thievery is not considered fraud, unless the person engaged in stealing also takes steps to alter receipts and/or other records in order to hide the theft. Fraud may be defined, therefore, as an intentional deception. Broadly speaking, it encompasses a wide range of irregularities and illegal acts, perpetrated by a person or persons inside and/or outside an organization, knowing that the act could result in some unauthorized benefit to the perpetrator, to the organization, or to another person or persons.

Occupational Fraud

There are many types of fraud — however, the focus of this series of articles is *occupational fraud*. Occupational fraud is fraud committed by an employee against his/her employer. In its *2006 Report to the Nation*, the Association of Certified Fraud Examiners (ACFE) defined occupational fraud as, "The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

TRAINING OPPORTUNITY

Oregon State Fiscal Association presents

Real World Business Ethics: How will you react?

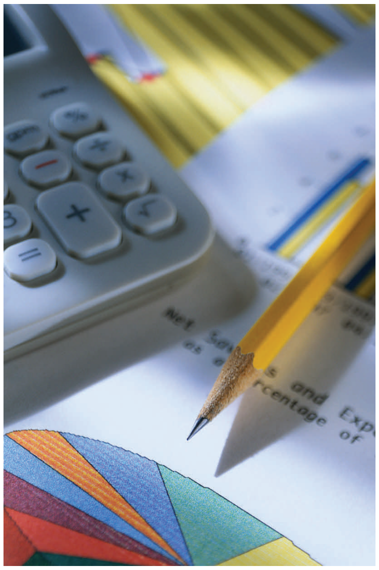
- **January 29, 2008**
- **Registration: 8:00 to 8:30 am**
- **Training: 8:30 am to 4:30 pm (8 CPE credits)**
- **Location: Salem Conference Center, 200 Commercial Street SE, Salem, OR**
- **Cost: $265 members; $280 non-members**

Registration link: http://www.oregonstatefiscalassn.org/Professional%20Development.htm

Who should attend:

- **CFOs, fiscal administrators, fiscal managers, accounting/finance professionals & auditors**

Inside this issue:



Antifraud Programs and Controls (cont'd)

Occupational fraud occurs at all levels of employment from clerical positions to mid-level managers to executive officers. Two of the chief ways occupational fraud is carried out is through the *misappropriation of assets* or *corruption*. Misappropriation of assets involves the theft of an organization's revenue receipts, theft of inventory or other assets, or the diversion of payments to unauthorized or personal use. Corruption includes fraud attributable to bribery, conflicts of interest and extortion — bribery being most prevalent.

Misappropriation of Assets

1. Schemes Involving Cash Receipts and Cash on Hand

Skimming: Skimming is the diversion of cash to personal or unauthorized use *before* it is reflected in the accounting records of the victim organization. Essentially, skimming is pocketing cash receipts without recording the sale. It is hard to detect because there is no trail or record of the transaction. It can happen any time a cashier does not ring up a transaction or does not write out a customer receipt and then pockets the cash when no one is looking. Other more complicated examples include:

- **Diversion of customer payments to personal use** and then writing off the customer's receivable balance as uncollectible.
- **Recording bogus sales discounts or lower than actual sales amounts** and pocketing the difference between the cash receipts recorded on the books and the amount actually received.

Larceny: Larceny is more difficult to conceal than skimming because it involves the theft of cash receipts *after* the receipts have been recorded on the accounting system, but *before* they have been deposited in the bank. Because of this, larceny is much less common than skimming. It is generally successful only when small or insignificant amounts of cash are diverted over time.

2. Schemes Involving Fraudulent Cash Disbursements

Billing Fraud: This is the most popular disbursement scheme because the perpetrators can avoid the risk of physically taking cash or other assets. Common types of billing fraud include:

- **Fictitious companies –** A person establishes a shell company and sends phony invoices for nonexistent services to an organization for payment.
- **Purchases diverted to personal use –** An employee acquires items with a personal-use element, such as a laptop; diverts it to personal use, such as to a son or daughter away at college; and submits the invoice to his/her employer for payment.
- **Paying vendor invoices twice –** The employee pays a vendor's invoice twice; requests the vendor to refund the overpayment; and, then, cashes the returned check without making any entry to the employer's accounting records.

Expense Reimbursements: Fraud of this type involves any scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses. Although not as prevalent as billing fraud, false expense claims can result in significant losses.

Check Tampering: Examples of this type of fraud include any scheme in which a person steals an employer's blank check stock to commit forgery or alters a legitimate outgoing check and deposits it into his/her own bank account. Because it is often difficult to physically access blank check stock or to confiscate outgoing checks, many fraud-

Antifraud Programs and Controls (cont'd)

sters prefer to dupe an organization into issuing legitimate checks based on false documentation and invoices through one of the billing schemes noted earlier.

Payroll Fraud: Although not popular with fraud perpetrators, the resulting loss from payroll schemes can also be significant. The following are examples of payroll fraud:

- **Fictitious employees –** A fictitious employee is added to the payroll or an ex-employee is not removed from the payroll, and the paychecks created for the "ghost" employee are diverted and cashed by the perpetrator.
- **Falsifying time and rate data –** Employees overstate the number of hours worked, or are able to increase their rate of pay.

3. Schemes Involving Non-Cash Assets

The majority of these schemes involve the theft of inventory or other physical assets, such as equipment and supplies. Sometimes, an employee "borrows" a laptop or other equipment to work on a project at home; the laptop is never returned to the office, or the equipment is used to start a personal business. These are fairly common scenarios that generally do not result in large losses. However, if warehouse personnel, inventory clerks or shipping clerks have direct access to the inventory, large losses may result.

Steps You Can Take Now

All organizations are exposed to the risk of fraud. The degree of exposure depends on the fraud risks inherent in the business, the extent to which effective internal controls are present to prevent or detect fraud, and the honesty and integrity of employees. The reason for the focus on occupational fraud is because it is the type of fraud that auditors and accountants most frequently encounter. In this issue of ***In Control,*** we have identified some of the common fraud schemes associated with the misappropriation of assets. In the next issue, we will take a closer look at *corruption*, the other type of occupational fraud.

In the meantime, there are many things that agencies can do to establish and maintain an effective fraud prevention program. One of the first steps is to ensure that the control environment includes:

- A code of conduct, ethics policy, or fraud policy to set the appropriate tone at the top.
- A safe haven program or other mechanism through which employees can report their concerns anonymously.
- A structured process for incident investigation and remediation.

Training

Fraud prevention training is also important, particularly training that provides opportunities for employees to discuss ethical dilemmas. On January 29, 2008, the **Oregon State Fiscal Association** will host an 8-hour training program on ethical standards and considerations. The goal is to help accounting and auditing professionals to apply ethical standards to "real life" situations. For more details and to register, please turn to page 4. Class size is limited; the training is offered on a first- come, first-served basis. ■

Real World Business Ethics: How will you react?
January 29, 2008

This class examines case studies of "real-life" litigation and administrative proceedings.

- Key issues in civil and regulatory actions
- Analysis of ethical requirements and considerations
- Fact patterns from actual proceedings
- Special ethical issues in select reporting and disclosure areas
- Effect of changes in disciplinary procedures and oversight

Instructor: ***James F. Buckley***, CPA, PricewaterhouseCoopers, Detroit, Michigan, previously served as the Controller for the City of Port Huron, Michigan. Mr. Buckley has helped to develop guidance and training for implementation of GASB 34 and 35 and has received the Government Finance Officers Association "Certificate of Achievement" reviewer. He is a committee member of the Michigan Committee on Governmental Accounting & Auditing, a member of the Government Finance Officers Association, and a member of the Accounting Standards Committee for the Michigan Municipal Finance Officers Association.

Cost: $265 for OSFA members; $280 for non-members

Location: ***Salem Conference Center***, 200 Commercial St. SE, Salem, OR

Time: Registration from 8:00 - 8:30 am; training from 8:30 am - 4:30 pm

CPE*: 8.0 credits, based on a 50-minute hour

Meals: Continental breakfast and lunch buffet will be provided.

To register: http://oregonstatefiscalassn.org/Ethics%20Registration%20Form.pdf

* This is a general ethics course. It is not intended to satisfy the 4 hours of specialized ethics training required every four years by active Oregon CPA licensees.

***In Control* is published by the State Controller's Division**

Statewide Financial Services
155 Cottage Street NE
Salem, OR 97301
Phone: 503-378-3156
Fax: 503-378-3514
http://www.oregon.gov/DAS/SCD/index.shtml

Who Can You Call for Help?

The State Controller's Division reminds state agencies that it is always available to answer internal control questions. If you have an internal control problem or an audit finding and need help in resolving it, please contact:

Kathryn Ross

Statewide Financial Internal Control Officer

Kathryn.Ross@state.or.us

503-378-3156 x277

Internal control tools are on the Web!

http://www.oregon.gov/DAS/SCD/internal_controls.shtml