Fraud Indicators - "Red Flags"

Consider the following scenarios:

Like so many other prudent, responsible government officials in Ohio, you've read the last issue of *Best Practices* and have worked with your colleagues to implement its many recommendations designed to identify, assess, and mitigate fraud risks. If you haven't yet read the Winter 2006 issue of *Best Practices*, you may access it by clicking www.auditor.state.us/publications/. Specifically, your organization has established a formal fraud risk prevention program, incorporating such measures as standard operating procedures, an internal audit function, and an ethics policy. Further, your organization has implemented a risk assessment program and bolstered its internal controls in a number of areas that appear vulnerable to fraudulent activity. All in all, your organization's antifraud efforts seem to be working as planned, when suddenly your assessment activities reveal what appears to be an indication of fraud. In fact, you discover an unusual increase in adjustments and write-offs to customer utility accounts, which is a potential fraud indicator. At this point, without further investigation, management does not know whether fraud has actually occurred.

Compared to fraud risk indicators (which you may recall from the last issue of *Best Practices*), actual fraud indictors represent instances where fraud may have occurred, as opposed to situations or conditions in an organization's operations that lend themselves to an increased risk for fraud. To draw a further distinction between the two, fraud risk indicators help organizations develop preventative measures in areas that are at risk for fraud, while fraud indicators help organizations detect fraud after it has occurred. Other examples of fraud indicators or "red flags" and their corresponding area of operation include:

General Red Flags

- ✓ Significant lifestyle changes among employee(s): expensive cars, jewelry, homes, clothes, etc.
- ✓ Employee(s) with significant personal debt and credit problems
- ✓ Significant behavioral changes among employee(s) - possibly indicative of drug, alcohol or gambling problems, or fear of job loss
- ✓ Instances where employee(s) refuse to take vacation or sick leave or refuse to accept promotions
- ✓ Reluctance among employee(s) to provide information to auditors or investigators
- ✓ Excessive number of checking accounts maintained by entity
- ✓ Frequent changes in banking accounts
- ✓ Frequent requests for new external auditors
- ✓ Excessive number of year-end transactions or journal entry adjustments
- ✓ Unsupported transactions or journal entry adjustments
- ✓ Refusal by employee(s) to use serial numbered documents (e.g., receipts)
- ✓ Unexpected overdrafts or declines in cash balances
- ✓ Financial transactions that don't make sense - either common or business
- ✓ Service contracts for which there is no product
- ✓ Missing or altered documents (e.g., accounting records)
- ✓ Photocopied documents in place of originals
- ✓ Significant sums of money lent/borrowed among co-workers

- ✓ Visits by creditors or collectors at the workplace
- ✓ Evasive or unreasonable responses to questions
- ✓ Employee(s) with unusually large sums of money

Red Flags in Purchasing and Disbursement

- ✓ Increased number of complaints received by the entity about products or service
- ✓ Acceptance of gratuities or significant “promotional” items by employee(s)
- ✓ Frequent use of handwritten endorsements vs. stamped endorsements
- ✓ Prepayment of goods or services
- ✓ Frequent use of sole source procurement contracts
- ✓ Pressure to expedite payments
- ✓ Inordinate volume of “manual” checks
- ✓ Lack of physical security over assets/inventory
- ✓ Payments to vendors that aren’t on an approved vendor list
- ✓ High volume of purchases from new vendors
- ✓ Purchases that bypass the normal procurement procedures
- ✓ Vendors without physical addresses
- ✓ Vendor addresses matching employee addresses
- ✓ Purchasing agents that pick up vendor payments rather than have them mailed
- ✓ “Consulting” contracts for which there is no determinable end product
- ✓ Abnormal number of expense items, supplies, or reimbursement to employee(s)
- ✓ Significant deviations from specifications on delivered goods or services
- ✓ Handwritten/typed vs. computer generated invoices
- ✓ Cash payments when checks expected

Red Flags in Sales/Receipts/Accounts Receivable

- ✓ Excessive number of voided receipts, customer discounts, and/or returns
- ✓ Unauthorized voided receipts, customer discounts, and/or returns
- ✓ Unauthorized customer/taxpayer account adjustments or write-offs
- ✓ Untimely deposits
- ✓ Unauthorized bank accounts
- ✓ Frequent use of handwritten vs. stamped endorsements
- ✓ Sudden activity in a dormant banking account
- ✓ Taxpayer/Customer complaints that they are receiving non-payment notices
- ✓ Discrepancies between bank deposits and postings
- ✓ Excessive or unjustified cash transactions
- ✓ Large number of write-offs of taxpayer/customer accounts
- ✓ Significant and/or frequent cash register shortages and overages
- ✓ Increase in past due accounts
- ✓ No collection efforts on past-due or written-off accounts
- ✓ Cash payments when checks expected

Red Flags in Payroll

- ✓ Inconsistent overtime hours for a cost center
- ✓ Overtime charged during a slack period
- ✓ Overtime charged for employee(s) who would not normally receive overtime pay
- ✓ Budget variations for payroll by cost center
- ✓ Employee(s) with duplicate Social Security numbers, names, and addresses
- ✓ Employee(s) with few or no payroll deductions

Reactions to Fraud Indicators

Once the organization is confronted with a fraud indicator, the next step is to develop a strategy for determining whether fraud has, in fact, occurred. As a general consideration, the steps taken to investigate potential fraud should occur from the "outside-in." In other words, management should begin by gathering information from other sources before confronting the alleged fraudster. This approach is recommended so as not to alert the alleged fraudster to the investigation and to protect the parties involved against unproven allegations.

To begin the investigation, management should gain a thorough understanding of the process surrounding the fraud indicator. Not only should management evaluate any relevant policies and procedures, management should also interview personnel to assess adherence to the policies and procedures. Further, management should gather any corroborating documentation related to the suspicious activity. Sources of corroborating documentation may include other departments, external third-parties (e.g., vendors or other governmental entities), and various information systems. At this point, management should be able to make a preliminary assessment as to whether fraud has taken place. Additionally, early on in the investigation, management should consult with the organization's legal counsel and human resources department to address any legal or other liability issues. Once the allegation is substantiated, management should then determine whether to contact the appropriate law enforcement agency and/or the Auditor of State.

Using our previous example where management discovered an unusual increase in adjustments and write-offs to customer utility accounts, management should consider the following steps to further investigate the fraud indicator:

- Evaluate any available documentation supporting account adjustments or write-offs.
- Compare the current billing period to prior billing periods to determine if write-offs and adjustments are abnormally high or in line with prior periods.
- Select a sample of written-off and adjusted accounts and recalculate the billings based on actual usage levels.
- Confirm amounts paid with utility customers.
- Reconcile amounts paid by customers with amounts posted to their utility accounts.
- Compare money collected and deposited to customer receipts.

If the results of performing the above steps indicate alleged fraud, management should consult the organization's legal counsel to determine the best course of action, which may include contacting the appropriate law enforcement agency and confronting the alleged fraudster.

Fraud and Small Governments

As the Association of Certified Fraud Examiners (ACFE) survey revealed in the last issue of *Best Practices*, small organizations (those with fewer than 100 employees) are particularly vulnerable to fraud, primarily because they lack the resources that are necessary to sufficiently control their risk for fraud. For instance, they may not employ enough fiscal personnel to ensure segregation of duties among the government's receipt and deposit processes. With the same person responsible for both receipting and depositing monies, the government's risk for fraud increases as that individual is better situated to take the funds before they are properly recorded and deposited into the government's account.

Because small governments lack the necessary resources to implement sufficient controls, it is critical for their governing boards and fiscal officers to actively monitor areas that are particularly vulnerable to fraud. Further, they should be cognizant of fraud indicators so frauds are detected before they cause significant loss to the organization.

Although smaller governments generally do not have staff dedicated specifically to do internal audits, there are a number of risk assessment activities and other fraud prevention techniques that can be completed by the government's governing board, fiscal officer, and other fiscal personnel. Below are some of the more common fraud prevention techniques used by small governments and their associated risk areas:

Receipts

- Issue all receipts sequentially so missing receipts can be more easily identified.
- Use a duplicate or triplicate receipt book to ensure corroborative documentation exists for monies received by the government.
- Periodically total receipts for a selected period and compare the amount collected to the amount deposited to identify discrepancies.
- Review any voided receipts to ensure there is sufficient reasoning and support for the void. Typically, if a receipt is voided, there should be a reason documented on the receipt, and a subsequent receipt should be issued for that payment.

Expenditures

- Issue all checks sequentially so missing checks can be easily identified.
- Ensure that checks are signed by someone other than the preparer. If one person performs both functions, he or she could more easily divert public funds to his or her personal account.
- Require the individual who signs the checks to review invoices and other documentation to verify the amount of the purchases and to ensure that the purchases are for government business.[1]
- Periodically review checks and related endorsements for irregularities, including the

[1] For those villages with combined clerk/treasurer positions, the mayor or council president should sign the checks, while someone independent of the check preparer should review the supporting documentation.

use of varying font types on checks and forged endorsement signatures.
- Refrain from providing employees with blank, endorsed checks as this increases the risk that a portion of the purchase could be used for personal items.
- Avoid the use of erasable ink as the name of the payee may be altered for fraudulent reasons.

Payroll

- Regularly compare staff rosters with payroll registers to identify potential ghost employees through whom fraudsters may receive additional pay.
- Periodically compare employee hourly rates per the payroll register to the approved hourly rate to ensure rates have not been erroneously, or worse, fraudulently inflated.
- Review time cards for approval prior to payment to help protect the government from paying for work not performed.
- Ensure policies are in place governing overtime compensation and leave.

Petty Cash Funds

- Establish the amount of the petty cash fund and guidelines for its use. Generally, the fund should be used for small emergency purchases for which there is not enough time to use the government's normal purchasing process.
- Require those using the petty cash fund to attach the receipts to the reimbursement voucher to ensure purchases were for government business.
- Periodically review receipts to ensure the purchases are for a proper public purpose (see AOS Technical Bulletins 2003-005 and 2004-002 available at **www.auditor.state.oh.us** under Publications).
- Periodically compare the petty cash fund balance with the amount of receipts supporting the checks issued to replenish the fund. Identified shortages could be an indication of fraud.

Procurement/Credit Cards

- Establish a thorough policy governing card usage and the processes used to ensure proper use of the card.
- Implement limits and other restrictions through the credit card company on the amount and type of purchases that can be made using the card.
- Review purchases along with receipts and invoices to ensure they are related to official government business.
- Require employees to sign an agreement stating they will not use the card for personal purchases.
- For an extensive discussion on procurement/credit cards including recommended controls and usage policies, please see the Winter 2004 issue of this newsletter at www.auditor.state.oh.us/Publications/.

Other Preventive Techniques

- Ensure the governing board is involved in the organization's finances. The mere involvement of the board can help deter employees from committing fraud in the first place.
- Document job duties for each employee to define work processes and standards for performance. Once job duties are formally defined, management can more easily identify areas that are at risk for fraud.
- Review monthly bank account reconciliations. Any unusual adjustments should include supporting documentation; otherwise, such adjustments are "red flags" for potential fraud.
- Segregate critical fiscal duties among staff to ensure one person does not have sole responsibility where checks and balances are necessary. Such duties include receipting and depositing public funds, preparing and signing checks, submitting and approving payroll, etc. When segregating these duties is not possible, the governing board should conduct surprise reviews on the activities of those individuals to help detect irregularities.

Village of Mechanicsburg

The following case is being provided to show readers how fraud impacts even the smallest level of government in Ohio. The case also illustrates the need for small governments to implement the prevention techniques discussed above to help reduce their risk for fraud.

In February 2004, the Auditor of States' Office (AOS) received a tip from a concerned employee from the Village of Mechanicsburg (Champaign County) alleging that the Village Clerk/Income Tax Administrator was misusing public funds. The tip was received through the AOS Fraud Hotline at **1-866-FRAUD-OH**, a component of the AOS's *Taxpayer Protection Initiative* (Visit www.auditor.state.oh.us for more information on this initiative).

The AOS Special Investigations Unit met with Mechanicsburg Police Chief, Tim Bostic, who indicated that he was aware of monies missing from the Village's Summer Celebration Account. Upon further review of this account, Bostic believed income tax monies were being used to replenish missing Summer Celebration funds. He also noticed that cash income tax collections were missing.

Following meetings with other Village officials and the Champaign County Prosecutor, the AOS initiated a special audit of the Village of Mechanicsburg for the period November 1, 2001 through April 16, 2004.