BEST PRACTICES

Dave Yost
Ohio Auditor of State

November 2017

To deter payroll fraud, internal controls are vital

When an employee games a local government's payroll system to steal from taxpayers, he or she is the one who pays the price when caught. But negligent elected officials and oblivious administrators sometimes share the blame. They are the ones responsible for creating the internal financial controls that are needed to deter payroll fraud. By failing to set these controls in place – or worse, putting them in place then failing to enforce them – they leave the door open to fraud.

These kinds of errors took their toll in Grove City between 2004 and 2011, when payroll specialist Jacqueline Kincaid stole $67,799 by manipulating the city's payroll system.

Kincaid, who ultimately was sentenced to two years in prison for the theft, was able to write unauthorized checks to herself because city officials had left her in charge of the payroll system from beginning to end. If someone had been looking over her shoulder, her manipulations would have been apparent.

Integrity of information

At the most basic level, fraud prevention is about the integrity of information, how accurate it is, who has access to it and what they can do with it. It starts with basics such as knowing who is on the payroll, when they were hired, their pay rate, the hours that they work, vacation and sick leave entitlements, and

Continued on back »

Warning signs

Anomalies that might be clues to payroll fraud:

- Employees who have the same Social Security number, address or bank account.
- Pay deposited to a bank account whose owner has a different name than the employee.
- Employees with no Social Security number in their records.
- Duplicate paychecks.
- Paychecks with no deductions for benefits and taxes.
- An employee still on the payroll roster after leaving the company.
- An employee who is on the payroll roster, but not in personnel records
- Unusual amounts of overtime or leave pay
- An employee paid for working more than 24 hours in one day.
- An employee with the same address or bank account number as a vendor doing business with the government entity.

images from 123rf.com

Basic internal controls

- Maintain accurate personnel records, listing hire/departure dates, pay rates, authorized deductions, vacation and sick leave entitlements.
- Periodically reconcile personnel roster with payroll roster, to ensure that pay disbursements, sick-leave and vacation payouts match personnel records.
- In smaller governments with one person handling payroll duties, elected officials or designated monitor should conduct frequent, rigorous review of personnel, payroll and related bank-account activity.
- Restrict access to payroll data to prevent unauthorized changes.
- Require independent review and sign-off on authorized changes to payroll data.
- Segregate payroll duties so one person doesn't control the process from beginning to end.
- Adhere stringently to all internal controls. Laziness or inattention open the door to fraud.

Questions?

Contact the Auditor of State regional office serving your area. Regional offices and contact information can be found at: https://ohioauditor.gov/contact.html

their separation date.

The ability to access this information – and alter it – is often a starting point for fraud, for example, by creating a fictitious employee and then collecting the pay for the nonexistent worker. Another scheme is to alter the record of an employee's hours or pay rate in order to overpay the employee.

A sound payroll system must restrict access to such information and include regular verification of the actions of those authorized to makes changes.

For example, the payroll roster created by those authorized to add new employees should be checked periodically against personnel records to ensure that those on the roster actually are employed by the government entity. This is a way to detect ghost employees and to ensure that employees who have resigned or retired have been removed from the payroll system.

Authorization

A key to controlling access to information is a system that authorizes those who are empowered to access and alter information. The number of people with this power should be restricted and they should not be able to take any action unilaterally, but each action should be subject to review and sign-off by someone else.

Segregation of duties

One of the fundamental ways to deter fraud is through segregation of duties.

Dividing a payroll process into several steps and assigning a different person to each of those steps makes it more difficult for any one person to steal and then cover it up. For example, the person responsible for adding new employees to the payroll and changing pay rates should be different from the person who processes payroll. For the same reason, someone else should be responsible for reconciling payroll accounts.

Segregating duties ensures that it would require the collusion of two or more persons to commit fraud, making such schemes harder to initiate and thereby reducing their likelihood.

Review and responsibility

Even the best system of checks and balances will fail if elected leaders and administrators don't require adherence to the policy. Failing to insist on authorization procedures, periodic reviews and cross-checking renders internal controls useless.

This responsibility is particularly important in smaller governments, such as townships and villages, where one person – a clerk or fiscal officer – has primary responsibility for the payroll and other financial affairs.

In such circumstances, township trustees and village council members must regularly check the fiscal officer's work or appoint someone to do so. This would include comparing personnel records with the employees on the payroll roster, double-checking pay rates and vacation entitlements, and making sure that internally generated payroll reports match statements from the government entity's bank account.

There are no shortcuts in payroll security, because taking a shortcut with internal controls also creates a shortcut to fraud.

Share this

Up next

Credit card abuse

More than $1.2 million has been stolen or misspent from government credit cards since 2011. Learn the keys to limiting credit card abuse.

Follow us

Ohio Auditor of State

@OhioAuditor

Dave Yost
Ohio Auditor of State

88 E. Broad St.
Columbus, Ohio 43215

Phone: 800-282-0370
Fax: 614-466-4490

www.ohioauditor.gov