



- **President's Column**
- **Director's Column**
- **New Grants & Loans**
- **City Spotlight**
Midwest City
- **Affiliate Spotlight**
Blackshare Environmental

- **Classifieds Online**
- **Service Providers Online**
- **Subscription Information**
- **Previous Issues**
- **OML Home Page**
- **Employment Opportunities**
- **Calendar of Events**



Contact Information:
Jimi Layman, Managing Editor
Oklahoma Cities & Towns
jlayman@oml.org
(800) 324-6651
(405) 528-7515

JANUARY 2010

CITY OF STILLWATER HOSTS MUNICIPAL GROUPS

The City of Stillwater hosted the January meetings of the OML Board of Directors, Legislative Committee, Oklahoma Municipal Services Corp. and Mayors Council of Oklahoma. A full day's business agenda included a report from OML Legislative Committee Chair Nancy Nichols, Edmond City Clerk, on the upcoming 2010 legislative session, appointment of Woodward City Manager Alan Riffel as Chair of the OMUP Steering Committee, election of Sand Springs Vice Mayor Mike Burdge as Chair of the Mayor's Council and initial planning of the June 24 – 26, 2010 MCO Mayor's Retreat in the City of Clinton. For more information click on the following: OML Board of Directors Meeting; OML Legislative Committee Meeting; Mayors Council of Oklahoma Meeting.

JOIN IN ON THE LEGISLATIVE PROCESS — SHARE WITH US YOUR SPECIALTY

One of the most important functions of the Oklahoma Municipal League is the lobbying initiatives that promote pro-municipal legislation and prevent potentially harmful bills from becoming law.

LOBBYING TIPS FOR CITY OFFICIALS

The 2010 Oklahoma Legislative Session will officially convene on Monday, Feb. 1, for the second session of the 52nd Legislature. With the 1,953 carry over bills from last year and the expected 2,000 of newly filed bills, we will begin the session with close to 4,000 active bills. Hundreds of registered lobbyists will be at the Capitol pushing their individual legislative agendas. It is important to understand your role as an advocate for cities and towns.

MUNICIPAL LEADERS DAY AT THE CAPITOL SET FOR MARCH 22

Mark your calendars now for March 22 to bring a carload of your officials, staff, and citizens under the capitol dome to let your legislative representatives know that "Cities Mean Business."

RETAIL SUMMIT. THE HOW OF RETAIL DEVELOPMENT

Looking to spur economic development and attract retailers to your municipality? Then you won't want to miss the OML Retail Summit on Thursday, Feb. 18, at the Moore Public Library, 225 South Howard.

THE IMPORTANCE OF INTERNAL CONTROLS OVER MISAPPROPRIATION OF GOVERNMENT ASSETS

It seems as though every other day, we hear of another instance of wrongdoing or lapse in moral judgment by government officials or employees. What can we do to put ourselves in a better position to prevent or detect such actions before they become a detriment to public trust? The key to preventing and detecting misappropriation of assets lies in the proper design and implementation of an effective system of internal control. A system of internal control is put in place to keep the government on course toward its goals and achievement of its mission, while at the same time minimizing surprises along the way.

This e-mail was sent by: Oklahoma Municipal League, 201 N.E. 23rd Street, Oklahoma City, OK 73105

Your subscription to Oklahoma Cities and Towns newsletter is one of your member benefits. If you do not wish to receive your copy of the newsletter with information pertinent to Oklahoma municipal governments, please e-mail cathy@oml.org to have your e-mail address removed. If you wish to continue to receive the newsletter, please add us to your safe senders list.

The Importance of Internal Controls over Misappropriation of Government Assets

By Michael A. Crawford CPA

It seems as though every other day, we hear of another instance of wrongdoing or lapse in moral judgment by government officials or employees. What can we do to put ourselves in a better position to prevent or detect such actions before they become a detriment to public trust? The key to preventing and detecting misappropriation of assets lies in the proper design and implementation of an effective system of internal control. A system of internal control is put in place to keep the government on course toward its goals and achievement of its mission, while at the same time minimizing surprises along the way.

What Internal Control Is

Internal control is broadly defined as an entity's process, affected by the entity's board, management, and personnel, designed to provide reasonable assurance regarding the achievement of certain objectives. In the context of financial management, these control processes should provide reasonable assurance that reliable and fairly presented financial statements will be prepared, financial-related laws and regulations will be complied with, and the government's assets will be adequately safeguarded.

What Internal Control Is Not

Internal control is not a panacea. The internal control process can help an entity achieve its objectives. However, no matter how well designed and implemented it can only provide reasonable, not absolute, assurance of achieving those objectives. For example, although controls may be adequately designed and in place, control objectives may still be unachieved resulting from: (1) simple errors and mistakes, (2) faulty judgments in decision making, (3) circumvention by collusion, and (4) management override of controls. Finally, the design of internal controls must be considered within the context of resource constraints and cost effectiveness.

Designing an Effective System of Internal Control

Internal control processes can generally be classified into one of the following five components of an integrated internal control framework:

1. Control environment — the tone of the organization influencing the control consciousness of its people, such as a well-communicated and understood code of conduct, an effective management style, and interest in controls by the governing body
2. Risk assessment — the identification and analysis of relevant risks to achieving the control objectives, such as risks of noncompliance with legal spending requirements, and risks of misappropriation of assets for personal use
3. Control activities — policies and procedures that help ensure actions are taken to address the identified risks, such as effective policies and procedures related to the segregation of incompatible duties, authorization and processing of purchase documents, and controls over access to cash and certain other assets
4. Information and communication — the information and communication systems, both manual and automated, that make it possible to operate, control, and report the entity's activities, such as an effective information technology systems, sufficient internal and external reporting systems, and proper channels of internal and external communications
5. Monitoring — the on-going monitoring and evaluation of the effectiveness of the other four components of the internal control framework through internal and external audit activities and governing body and management oversight; a well recognized system of monitoring can also be an effective deterrent to misappropriation of assets

For internal controls to be properly designed and operating effectively, each of these five integrated elements must be working together. The evaluation of the effectiveness of the design and operation of internal controls should be focused on the identification of control objectives, the specific risks associated with achieving those objectives, and the internal controls designed to minimize those risks. In other words, you should define (1) "what we want to accomplish", (2) "what could go wrong", and (3) "what we should do about it."

PRACTICAL EXAMPLE: One of the objectives of internal controls over misappropriation of assets (what we want to accomplish) is to ensure that all revenue collected is properly deposited and not misappropriated. When evaluating the effectiveness of internals in regards to this control objective, you could consider what specific risks exist that could result in not achieving the control objective (what could go wrong) and then identify the specific internal controls needed to minimize those risks (what we should do about it). This process is illustrated in the table below.

Control Objective (what we want to accomplish): Ensure that all revenue collected is properly recorded, deposited and not misappropriated.	
Specific Risks (what could go wrong)	Controls to Minimize the Risks (what we should do about it)
Cash receipts could be intentionally misappropriated and not recorded or deposited.	<p>Establish proper segregation of duties by assigning cash collections duties to individuals not involved in the billing, adjustment, and posting processes.</p> <p>Implement a daily cash drawer balancing process performed or witnessed by an individual not involved in the cash collection process.</p> <p>Compare daily cash postings in the revenue or receipt subsidiary ledgers with supporting cash receipts and the actual amount of cash collected and deposited.</p>
Cash receipts from one customer could be inappropriately applied to another customer's accounts.	Review aged accounts receivable reports on a timely basis and follow up on old or unusual outstanding balances.
Cash receipts may not be protected from unauthorized access.	<p>Use locking cash drawers and safes and ensure cash drawers and safes are locked when not in use.</p> <p>Make deposits on a daily basis and only keep minimal amounts in a safe or vault overnight.</p>

It is important to note that in the above example, the risks of not achieving the control objective of ensuring that all revenue collected is properly deposited and not misappropriated are addressed with internal control processes that specifically respond to each risk. This type of approach to identifying and addressing specific risks is the most effective way to prevent and detect misappropriation of assets in government from the perspective of the design of internal controls.

Establishing Key Controls

While the design and implementation of an effective system of internal control requires a thorough evaluation of control objectives and risks, there are certain broad “key” types of controls that should be considered in the design of controls over misappropriation of assets. These controls include:

- **Authorization and Approval** – controls over billing, receipting, and spending that involve delegation of authority with specified limitations and approval requirements (e.g. identifying who is authorized to make certain purchases or authorize billing adjustments, setting limits where advance approval is needed, indicating who must review and sign documents for evidence of approval, etc.)
- **Security over Access** – controls over access to cash, other assets susceptible to theft, purchase authorization documents, signature stamps, checks, and computer system processes that safeguard assets from loss or misappropriation (e.g. maintaining locked safes, cash drawers, and frequently changed computer access codes)
- **Segregation of Duties** – controls that do not put a single individual in a position to be able to commit a fraud or misappropriate resources and then be able to conceal it (e.g. preventing the same individual from billing, collecting and posting utility revenue; or placing and order for goods or services, acknowledging the receipt of those goods, and authorizing payment)
- **Review and Oversight** – controls that provide sufficient monitoring over revenue and expenditure activities, the reconciliation and investigation of unresolved questions and differences, and the ultimate resolution of those questions or differences (e.g. a comparison of budget and actual amounts to look for unexplained variances, periodic internal audits, etc.)

Identifying and Addressing Fraud Risks

Identifying fraud is difficult because unlike identifying errors in judgment or application, fraud involves an attempt to conceal. Therefore, it is important to be alert to certain conditions that may be present in your organization that could heighten the risk of fraudulent activity. Popular guidance in the area of fraud awareness indicates that most frauds contain all of the following three elements:

1. **Motive or Pressure** – the reason an individual decides to engage in fraudulent behavior
Examples:
 - Unmanageable personal financial obligations
 - Excessive gambling or other addictive vices
 - Adverse employment relationships
 - Living beyond one’s means
2. **Opportunity** – the condition that provides an individual the ability to perpetrate the fraud
Examples:
 - Unrestricted access to cash or other assets
 - Inadequate segregation of incompatible duties
 - Inadequate monitoring or oversight
 - Records are in disarray and difficult to follow or trace
3. **Rationalization** – the mindset of the individual that allows him or her to justify fraudulent actions
Examples:
 - Employee displeasure or dissatisfaction with job or compensation, or revenge for unfair treatment
 - Just a temporary borrowing that will be paid back
 - Everyone does it, it is no big deal
 - No harm, no foul

To enhance your ability to identify fraud in an organization, you must understand these three elements and constantly be alert for evidence of their existence and watch for warning signs (red flags) of potential fraud.

Identifying Potential Fraud Red Flags

Indicators of a heightened risk of fraud resulting in misappropriation of government assets could include the following red flags that should not be discounted or overlooked:

- Employees are scared of superiors and there is evidence of management override, in other words management by passing controls or overriding lower-level decisions for personal gain
- Employees do not take or refuse to take vacations or extended periods of time off or carry unusually high unused leave balances
- Employees with fraud opportunities exhibit evidence of fraud motives or pressures, such as unusual behavior, personal financial problems, excessive gambling, living beyond their means
- Daily balancing of cash drawer shows consistent differences, especially in even dollar amounts
- Bank deposits are not being made on a timely and consistent basis
- Bank statements are difficult to reconcile to the accounting records or consistently have unreconciled differences
- IRS notices arrive for untimely tax deposits or failure to make required deposits
- Unexplained budget and actual variances for revenues or expenditures exist
- Certain transactions are subjected to “special” handling outside the normal policies and procedures
- Key purchasing or payment documentation is lacking or does not exist, such as no evidence of receiving advices
- Invoices are faxed, only in photocopy form, or appear altered
- Vendors have only post office box addresses
- Contracts or invoices are in amounts just under the dollar threshold that would require bidding or pre-approval
- There is evidence of excessive use of sole source purchases or certain vendors appear to consistently obtain all or an extraordinary share of the business
- Payments are made to unfamiliar employees or terminated employees
- Family relationships exist within the same entity or department where unusual or questionable spending has occurred
- Tips or complaints regarding misappropriation of assets or fraud are ignored or not followed up on

When any of these fraud red flags are present, they must not be ignored or overlooked. Appropriate follow up is needed to ensure they are not indicators of an actual fraud.

Tips for Preventing or Detecting Fraud

Even the best of internal controls may not be sufficient to prevent or detect fraudulent activities because the individual(s) perpetrating the fraud are also doing their best to conceal the fraud. Therefore, it is especially important to be alert to the indicators of potential fraudulent activities. The following guidance will help you be more alert to potential fraud and enhance your ability to prevent or detect it.

1. **Just Going through the Motions** – avoid the work mentality of just doing the steps in a process without thinking about what you are doing; supervisors should reinforce with employees the need to pay attention to their tasks and the consequences for failure to be responsible in carrying out those tasks
2. **See No Evil, Hear No Evil** – avoid putting blind trust in any individual, thereby failing to recognize or acknowledge fraud warning signs or red flags; realize that anyone can commit fraud and when faced with warning signs prove to yourself that it is not fraud
3. **It’s Good to be the King** – look out for positional immunity, or in other words, upper level management or the governing body rationalizing that rules or controls don’t apply to them because of their position; these conditions generally present themselves as management override of existing processes or controls; identify someone within or outside the organization to whom you can report such activities without jeopardizing your job
4. **New Kid on the Block** – don’t give into the thinking that new employees are not yet competent in their position and therefore not in a position to question why certain things are happening; new employees are generally not prejudiced by past policies, procedures, and practices; supervisors should take all employees questions seriously, and employees doing the questioning should question more than just a single individual

5. **Where's All the Time Gone** – beware of workload overload and do not use this excuse to rationalize why designed internal controls cannot be followed; for example, it may take more time to reconcile differences noted in bank reconciliations, but that reconciliation is essential to managing fraud risks; when faced with workload overload, reevaluate assignment of duties, and if necessary demand more resources by explaining the consequences of fraud
6. **Don't Invade my Space** – beware of employees who do not want any other individual performing their tasks or learning what they do; encourage cross-training, periodic rotation of duties, and mandatory vacations for all employees and positions
7. **Must Not Be for my Eyes** – be concerned when you are denied access to requested records that support the work to which you are assigned; report such activities and lack of openness to appropriate supervisors and do not give up on the unfulfilled request
8. **It's None of my Business** – don't look the other way when faced with signs of fraudulent or unethical behavior by rationalizing that the activities are none of my business; work to create an environment within the organization that fosters ethical and responsible behavior and the reporting of lapses in such behavior
9. **It's Over my Head** – avoid the failure to question activities, events, or transactions that appear unusual because you feel you do not fully understand the situation or circumstances; individuals involved in fraudulent activities often rely on the complexity of the circumstances to help them conceal such fraud; continue to educate yourself, and ask for simplification in reports and explanations
10. **Just a Bad Apple in the Bunch** – realize that even with the best of internal controls, some people are just “morally challenged” and are looking for ways to commit fraud or improperly benefit themselves or gain an advantage; do your due diligence in hiring employees and learning as much as possible about their background and ethics

Government officials are entrusted with public resources and are responsible for carrying out public functions efficiently, economically, effectively, and ethically, while achieving desired program objectives and providing public services. Therefore, it is essential that government officials and employees embrace the concepts of transparency and accountability for their use of public resources. An actual misappropriation of assets from embezzlement or wrongful spending or the mere perception of such acts through lack of transparency can be the downfall of public trust. An effective system of internal control must be put in place to keep the government on course toward its goals and objectives, to manage the risks associated with misappropriation of assets, and to maintain and protect the public trust.