Fraud in Government: Prevention and detection

BAKER TILLY

Have you ever heard the saying, “Don’t be that guy?” Well in this case, “Don’t be that government.” In a recent study,[1] government and public administration was the second most likely industry to be impacted by fraud. A finding from that study showed the presence of anti-fraud controls is associated with reduced fraud losses and shorter fraud duration. Management and those charged with governance are responsible for ensuring these controls are in place. This article will explore common fraud schemes and provide prevention and detection controls that can be put in place to help mitigate fraud risk.

What is fraud?

Fraud is often defined as wrongful or criminal deception intended to result in financial or personal gain. The impact of fraud ranges from financial loss to declines in organizational performance, credibility, and public confidence. As a result, risk management strategies and internal control systems should be implemented, monitored, and modified as necessary by management and governing bodies.

Who is responsible for fraud prevention?

According to American Institute of Certified Public Accountants (AICPA) auditing standards,[2] the primary responsibility for prevention and detection of fraud rests with those charged with governance and management. There are a number of strategies[3] to help management and public officials navigate the challenges associated with prevention and detection of fraud.

1. **Understand your organization and industry:** Explore key drivers of revenue and related benchmarks, be active in the budget process and evaluate historical trends.
2. **Brainstorm with department heads, key members of management, external and internal auditors to identify fraud risks:** Review material weaknesses, compliance findings, and control deficiencies related to the financial and single audits. Also consider decentralized operations. Examples of control weaknesses that contribute to fraud include: lack of internal controls, lack of management review, override of existing controls, poor tone at the top, and lack of competent personnel.
3. **Assess the tone at the top and the entity’s culture:** It is imperative that organizations set an appropriate tone at the top, one that demonstrates a commitment to honesty and ethical behavior.
4. **Create a whistleblower policy**: Establishing a whistleblower hotline and/or policy is critical. History has shown that the initial detection of fraud most often occurs through a tip followed by management review, internal audit, or by accident.
5. **Understand the objective of a financial audit and a forensic audit:** The Association of Certified Fraud Examiners reports that less than 10% of frauds are discovered as a result of a financial audit conducted by an independent accounting firm. That is because a financial auditor is required to obtain reasonable assurance that the financial statements as a whole are free from material misstatement, whether caused by fraud or error. There is a risk that, even though an audit is properly planned, material misstatements may not be detected. Whereas, the objective of a forensic audit is to determine whether fraud has/is occurring and to determine who is responsible.

[1] Association of Certified Fraud Examiners. Report to the Nations on Occupational Fraud and Abuse. Report. 2014. http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

[2] "AU-C Section 240.04; Independent auditors are required to follow existing standards put out by the AICPA." American Institute of Certified Public Accountants (AICPA). 2015. http://www.aicpa.org/.

[3] "Management Override of Internal Controls: The Achilles’ Heel of Fraud Prevention." American Institute of Certified Public Accountants (AICPA). 2005. http://www.aicpa.org/.

While management and governing bodies are typically trusting, simple “blind faith” in a trusted employee alone is not sufficient. Management and governing bodies need to also verify what they are being told or shown. This begins by promoting an organizational culture of honesty and ethical behavior and includes spending time following through, holding others accountable, and asking probing questions. The simple tactic of verifying information can act as a deterrent, which could reduce the likelihood of fraud.

What common fraud schemes look like and how to prevent/detect fraud

Skimming. Money intended for the government that an individual takes for personal use. For example, cash receipts may never get entered into the system or they may be entered, but then voided/manipulated. This type of fraud is more likely to occur in unsupervised areas that lack controls over accepting cash.

Limit unsupervised cash collection locations. For remaining unsupervised cash collection locations, implement procedures for reconciling receipts and ensure deposits are properly reviewed and supported. For all cash collections, track, reconcile, and review adjustments made to fees charged and collected, and analyze deposits over time to identify anomalies.

Forgery or alterations. Includes checks, p-cards, vendor invoices, or employee payroll that are forged or altered. Be aware of a lack of security surrounding unwritten checks and signature stamps, little to no oversight or segregation of responsibilities, and the failure to account for all checks, wires, and electronic payments.

Develop appropriate check processing and reconciliation procedures, and ensure the approval of disbursements includes accounting for the entire sequence of payments (checks, wires, electronic payments, etc.). Do not pre-sign checks. Require dual signatures. Finally, limit the number of bank accounts used by decentralized locations. Someone independent of check processing and distribution should reconcile all bank accounts.

Unauthorized vendor distributions. Payments may be made to a fictitious vendor for goods never received or a legitimate vendor for personal goods. Vulnerable situations that allow for unauthorized vendor distributions occur in departments without effective oversight. Vulnerability may also stem from the lack of segregation between ordering, receiving, and approval functions.

Create/update purchasing, procurement card, wire transfer, and vendor management policies. Purchasing policies should address limits and purchasing authority; as well as authorization for users, daily and transaction limits, and documentation requirements. When new vendors are created, limit access to select personnel who are not involved in the disbursement or approval process. Ensure all new vendors are appropriately reviewed and approved by a supervisor.

Unauthorized payroll disbursements. This can include fictitious employees, unauthorized pay increases, or overtime. An inadequate review of employee timesheets or lack of reconciliation of payroll records to disbursements is another gateway to unauthorized disbursements.

Enforce appropriate payroll process policies and controls. Similar to the creation of new vendors, creation of new employees or financial disbursements in the payroll system should be limited to select personnel who are not involved with the approval process. A supervisor should review new employees added to the system on a regular basis, and review of payroll or financial disbursements should be assigned to someone independent of the process.

Prevention/Detection

Conduct a fraud risk assessment: One of the most effective ways to prevent fraud is to conduct a fraud risk assessment. This type of assessment will identify where and how fraud could occur, as well as who might be in a position to commit fraud. Fraud risk assessments will also determine an overall rating for the risk (high, medium, or low) and evaluate controls in place to detect those risks. Below are suggested components of a fraud risk assessment, adapted from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) guidance on enterprise risk management, internal control and fraud deterrence[4].

1. Identify the fraud risk
2. Determine the likelihood of a misstatement occurring if a control were to fail or a control was not present
3. Determine the significance/magnitude of a misstatement occurring if control were to fail or control was not present
4. Assign an overall rating (high medium or low)
5. Identify compensating controls
6. Determine if existing controls are operating effectively
7. If not, determine what additional, more effective controls should be put in place

We recommend updating the risk assessment on a regular basis.

Making time to ensure proper controls are in place is critical. No matter the size of your government, internal controls must be present. It is the responsibility of management, with oversight from those charged with governance, to ensure a system is in place to prevent and detect fraud. The time to act is now.

[4] "Guidance on enterprise risk management, internal control and fraud deterrence." Committee of Sponsoring Organizations of the Treadway Commission (COSO). May 14, 2013. http://www.coso.org/guidance.htm.