Local Government Fraud Risks – The Problem is Real, But So Are the Solutions

Introduction

#1 take away: Just because you have a regular audit, you have professional staff in place, you have internal control policies and procedures, and nothing has ever been discovered before, does not mean that you do not have vulnerabilities that will allow a fraud to occur, and potentially continue to happen while going undetected for years. Hundreds of recent local governments that fell victim to fraud met that description, and only after the discovery did they take a critical look at their existing controls to prevent and detect fraud.

Frauds committed against local governments happen frequently and they come from both outside and inside the organization. Check tampering, theft of cash, inventory theft, expense reimbursement fraud, ransomware attacks, DDoS and TDoS attacks, vendor payment fraud, procurement fraud, account lapping, etc. These are just a handful of fraudulent schemes common to local government operations, and there are many more. Updating and modernizing internal controls can significantly reduce your fraud risks; allowing implementation of recent internal control best practices across the country.

Assessing Fraud Risks

Annual audits serve a valuable purpose, but the reality is that fraud prevention is not the main focus. As a matter of fact, only 4% of fraud cases discovered last year were due to annual audit.[1]

Comprehensive fraud risk reduction and internal control modernization assessments go much deeper than an “audit” and can prove highly valuable. There are numerous local

[1] Association of Certified Fraud Examiners, 2020 Report to the Nations, https://www.acfe.com/report-to-the-nations/2020/

governments that conduct them, some of which do so after a known fraud or embezzlement incident and others proactively – to best protect the organization from the real risks that exist and are causing other local governments significant harm. Think about the last time your organization's fraud risks and internal controls were evaluated from the perspective of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control Integrated Framework.

Technologies change, fraudsters adapt and become more sophisticated, and controls should be regularly updated. Ensuring your controls are modernized and your fraud risks assessed could mean the difference in keeping the organization out of the negative news headlines from a fraud event having occurred or at least helping to reduce the severity of an ongoing incident should it be occurring.

Avoiding Negative News Headlines

Local government management professionals understand the importance of internal control. Unfortunately, the mindset of "everything must be okay since nothing has happened" has led to some devastating results for many local government organizations. Here are just three quotes taken from online articles from a couple of years ago (there are hundreds of more recent ones as well), showing interviews with government officials after the discovery of an embezzlement in their organizations:

> **Headline:** Former Surprise employee stole $836,000
> **Quote:** "It's pretty embarrassing for the City to have that happen right under our noses" – City council member
> **Length of embezzlement:** Approximately eight years
> **Source:** AZcentral.com, April 27, 2016
>
> **Headline:** Why was she hired? Was there oversight? Harrisburg officials tightening controls after $180k theft

Quote: “We were all shocked. Disbelief, disappointment. It was an overwhelming amount of emotion” – District spokesperson
Length of embezzlement: Approximately two years
Source: Pennlive.com, March 1, 2018

Headline: Columbia County Sheriff’s Office Employee Arrested after Embezzlement
Quote: “When Columbia County Commissioners realized that a long-term employee was embezzling funds, we were shocked. Our first thoughts were ‘how could this person, this trusted employee of 30 years, do this?’” – County Commissioner
Length of embezzlement: Approximately 16 years
Source: iape.org, May 3, 2018

No finance professional, local government manager, or elected official wants to be on the receiving end of any negative news headline, especially one so emotion-stirring as that of a local government fraud incident.

A Real Issue for Local Governments

According to the Association of Certified Fraud Examiners 2018 Report to the Nations, organizations that regularly assessed fraud risks and completed a formal fraud risk assessment saw a 50 percent reduction in the duration of a fraud event. Organizations that did not regularly assess their risks and complete formal fraud risk assessments saw a 62 percent greater financial loss from fraud[2].

[2] [1] Association of Certified Fraud Examiners (2018) Report to the Nations 2018 Global Study on Occupational Fraud and Abuse. Retrieved from: https://www.acfe.com/report-to-the-nations/2018/default.aspx.

A data review from an internet search of known fraud cases where government employees embezzled from their employer revealed the employee stealing worked in a variety of classifications throughout the organization, their ages generally were between 40 and 65, and the dollar amount embezzled was certainly enough to get the attention of the local citizenry (numerous cases over $100,000 and many in the millions of dollars). The most infamous known case is that of Rita Crundwell and the City of Dixon, Illinois, in which she embezzled $53.7 million over 20 years. These incidents occurred in local government organizations with professional finance staff and regular annual audits; many of which happened undetected year-after-year.

Steps you Can Take

A comprehensive review of your organization's fraud risks and internal control effectiveness should include analyses for over 225 areas across these main categories:

- Purchases and vendor management
- Cash and cash handling
- Checks and check handling
- Governance
- Inventory and asset management
- Financial controls
- Information technology
- Internal audit and analytics
- Human resources and payroll

It all comes down to protecting your organization's finances, preserving public trust, and the importance of professionalism. Trusting employees is important; however, trust-but-verify is essential. According to a case study on the Dixon, Illinois embezzlement, the trust in the city's embezzler was based on coworkers' and others' usual propensity to trust, which facilitated the opportunity to carry out such a crime over many years[3].

Of the hundreds of preventive and detective internal controls that should be in place within a local government organization, here are a couple of recommendations:

- Does your organization ensure all bank statements are reconciled within 30 days of receipt of the statement? Most have policies that require timely reconciliations, but are they actually completed on-time every month? This is not only to help identify financial anomalies that need investigation, but also to use the Uniform Commercial Code to help protect your organization (U.C.C. Article 4 – Bank Deposits and Collections (2002) Part 4 Relationship Between Payor Bank and its Customer §4-406). Failure to discover and report unauthorized signatures or alterations to the bank within 30 days of receiving your bank statement could result in your organization's inability to file a claim with its bank.

- Does your organization employ multi-factor authentication for changes to established vendor payment accounts? Is your multi-factor authentication policy modern and free of significant vulnerabilities? Several local governments have recently been victimized by this fraud scheme, including highly professional ones here in Arizona. Requiring multifactor verification for any vendor payment change to an already established payment account is a way to reduce the risk that a

---

[3] Ross, D.M. (2016). A Case Study of Municipal Government Financial Management and Effective Internal Controls. Published in ProQuest #10092247.

fraudster will convince a local government employee to change a vendor's bank account information, causing the local government to send an actual vendor's payment to the fraudster. Multifactor authentication can occur in a variety of ways, and it requires the person requesting a change to existing bank account information to provide verification of whom they purport to be. Examples of multifactor verification that can work in a local government setting include:

1. Using a third-party account verification service (to verify ownership of the newly changed account information).

2. Using a PIN, password, and/or security question that was established when the vendor initially sets up their information with the local government to verify identity.

3. Outgoing SMS messages or phone calls to a predetermined phone number, set up at the time the original account data was provided, for verification. **Even better**, since text message verification can be subject to SIM card hijacking, using an authentication application provides the advantage of not relying on a cell phone carrier. Examples of these apps include Google Authenticator, Microsoft Authenticator, or Authy.

4. Using a branded form that they complete and return to you, having provided a secure password or details about prior payments received that only they should know. This form should be mailed to the known vendor address.

5. Confirm data received on the branded ACH form by calling or emailing known numbers and email addresses. Never hit "reply" to answer an email from a vendor wanting to modify their account information. Always type in

the known vendor's contact email address, and do not let it auto-populate in case a fraudster's email is similar and is already in your system.

- Have you considered the benefits of using Universal Payment Identification Codes (UPIC) to encrypt your organization's bank account information and how the use of ACH blocks and filters can help reduce risk? The use of UPIC and ACH blocks and filters are an excellent way to help protect your organization's finances from falling victim to payment fraud.

- Has your organization implemented any new technology recently? Implementation of new technology means a need to evaluate internal controls related to that technology. Failure to do so could leave your organization vulnerable to fraud.

Remember, an examination of your organization's fraud risks and controls includes hundreds of areas for examination and just because you have policies in these areas – do staff actually follow the policy and are your policies actually best practice for known recent fraud risks?

Additional Recommendations:

1. Follow the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control Integrated Framework to assess your existing internal control environment. This includes understanding and assessing each of the Framework's 17 principles within 5 integrated components within your organization: control environment, risk assessment, control activities, information and communication, and monitoring activities. Weaknesses in any of these areas can create a situation in which you unintentionally facilitate someone's ability to steal from your organization.

2. Perform an annual fraud risk assessment for your entire organization, using the Framework to guide that assessment. Technologies change, fraud schemes become more elaborate, and your risk environment is fluid. An annual fraud risk assessment is not associated with any particular known fraudulent scheme but rather is a means for the government to assess its risks, to discuss ways in which misconduct can occur, to determine the likelihood it will occur based on existing controls, to determine how significant it will be to the organization if something happens (in terms of both financial and reputational harm), and to identify areas in which additional controls might be appropriate (or conversely, existing controls are no longer necessary).

3. Complete a comprehensive review of your organization's internal controls, in all departments, at least every three years. Data show that those accused of government embezzlements work in a wide variety of departments in all types of job classifications. It is realistic to assume that employees in any job classification within your organization could steal from you and it is a certainty that fraudsters from outside your organization often look for organization's they consider to be the "low hanging fruit" when they try to commit their frauds. Asset misappropriation, embezzlement, ACH payment fraud, ransomware attacks, time theft — it can lower employee morale, cause negative news headlines, cause financial harm and an inability for the organization to effectively get things accomplished in the future, and unfortunately people have lost jobs and elected officials have lost re-elected.

Internal controls are an ever-changing environment and they deserve regular attention. While internal control and fraud risk assessments are time consuming and might not be viewed as "exciting," you will be helping to best protect your organization.

About the Author

Dave Ross is CEO of 65th North Group, a local government consulting firm specializing in fraud risk reduction and internal control modernization. He has investigated over 400 fraud cases, he is a certified fraud examiner, a certified internal control auditor, holds a COSO Certificate in Internal Controls, completed Harvard University's Senior Executives in State and Local Government program, is an ICMA credentialed manager, and has a PhD in financial management with a dissertation in local government fraud risk reduction and internal control. He can be reached at dross@65thnorth.com or 480-386-5344.