

# Nurturing Relationships and Modernizing Internal Controls

BY DAVID M. ROSS



We all have different relationships in our lives—friends, family, work colleagues, and so on. How well they turn out often depends on how much we put into them. Whatever kind of relationship you have, nurturing it helps keep it strong.

When we don't put much effort into our relationships, it's often because we think that if nothing bad has happened so far, everything must be okay. But that's far from accurate. For example, if you don't pay enough attention to your spouse, they might not say anything—until they tell you they're leaving.

An organization's relationship with its internal control environment is just that—a relationship—and the effort you put into it makes a difference. Sometimes

the results will be fine, but other times they can be devastating. And the negative results might not reveal themselves for years because of the covert nature of fraud incidents. When they are revealed, they catch the organization's senior officials off guard and often result in immediate changes to internal controls. While these changes might be for the better, proactively addressing unknown weaknesses is a better approach.

Finance professionals understand the importance of internal controls. Most everyone likely thinks their controls are at least adequate, possibly because they have a clean audit and nothing has ever been discovered. Unfortunately, that mindset has led to some devastating results. See Exhibit 1 for just three examples of interviews with government officials after embezzlement was discovered in their organizations.

## Annual Audit Limitations

Professional finance officials understand that internal controls are important and know that the annual audit report is not designed to provide an opinion on the effectiveness of the government's system of internal controls; the organization's management is responsible for designing a system of effective internal controls. Local government annual audits are important, but comprehensive internal controls require a different approach.

## A Real Issue for Local Governments

According to the Association of Certified Fraud Examiners 2018 Report to the Nations,<sup>1</sup> 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.

Why is a proactive approach to ensuring modern and comprehensive internal controls important if an annual auditor gives an unqualified opinion in the audit report and does not list any significant deficiencies or material weaknesses? The reason is that there have been hundreds of recent local government fraud cases, including ransomware attacks, vendor payment fraud schemes (fraudulent changes to a vendor payment account), and occupational fraud incidents in which government employees steal and get away with it for years. This includes many organizations with clean annual audits.

A data review of known occupational fraud cases where government employees embezzled from their employer revealed that the employee who was stealing worked in a variety of classifications throughout their organizations, their ages generally were between 40 and 60, and the dollar amount embezzled was certainly enough to get the attention of residents (numerous cases of more than \$100,000, and many in the millions of dollars). The most infamous known case is that of Rita Crundwell, who embezzled \$53.7 million over 20 years from the City of Dixon, Illinois. These incidents occurred in local government organizations with professional finance staff and regular annual audits.

If you really want an eye opener, type "city," "county," or "school district" into a search engine, followed by "embezzlement," "fraud," or "scammed" (i.e., "city scammed" or "county embezzlement"). Then click on the news link. You will be able to scroll through hundreds of known government incidents from recent years.

### Exhibit 1: Government Embezzlement, Ripped from the Headlines

#### Former Surprise Employee Stole \$836,000

*"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

#### Why Was She Hired? Was There Oversight? Harrisburg Officials Tightening Controls after \$180k Theft

*"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

#### Columbia County Sheriff's Office Employee Arrested After Embezzlement

*"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

## What Can You Do?

A comprehensive review of your organization's fraud risks and internal control effectiveness should include analyses for more than 200 areas across these main categories:

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

It all comes down to protecting your finances, preserving public trust, and ensuring professionalism. Trusting employees is important; however, “trust but verify” is essential. According to a study of what happened at Dixon, the trust in the city's embezzler was based on our usual propensity to trust others—which facilitated the opportunity to carry out a crime over many years.<sup>2</sup>

There are hundreds of preventive and detective internal controls that should be in place within a local government organization. Below are some things you should consider.

**Make sure all bank statements are reconciled within 30 days of receipt.** This is not only to help identify financial anomalies that need investigation, but also to use the Uniform Commercial Code (a comprehensive set of laws governing all commercial transactions in the United States) to help protect your organization.<sup>3</sup> The government may not be able to file a claim with its bank if it waits more than 30 days to discover and report unauthorized signatures or alterations related to its bank statement.

**Use multi-factor authentication for changes to established vendor payment accounts.** Requiring multi-factor verification for any vendor payment change to an already established payment account is a way to reduce the risk that a fraudster will convince you or your employees to change a vendor's bank account information, causing you to send your actual vendor's payment to the fraudster. Multi-factor authentication, which can be done in a variety of ways, requires the person requesting a change to existing bank account information to provide verification of who they purport

to be. Examples of multi-factor verification that can work in a government setting include:

- Using a third-party account verification service (to verify ownership of the newly changed account information)
- Using a personal identification number (PIN), password, and/or security question that was set up when the vendor initially provided its information with the government, to verify identity
- Routing outgoing SMS (which stands for short message service, a text messaging service component of most telephone, Internet, and mobile device systems) messages or phone calls to a predetermined phone number, set up at the time the original account data was provided, for verification
- Using a branded form that the vendor completes and returns to you, having provided a secure password or details about prior payments received that only they should know
- Confirming data received on the branded automated clearing house (ACH) form by calling or emailing (The ACH is an electronic funds-transfer system that facilitates payments in the United States.)
- Never hit “reply” to answer an email from a vendor that asks to modify its account information. Always type in your 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.

**Use positive pay or payee positive pay.** These fraud-prevention systems are offered by most commercial banks to companies to protect them against forged, altered, and counterfeit checks. The company provides a list to the bank of the check number, dollar amount, and account number of each check. If you aren't familiar with either of these technologies, ask your government's bank about how they can help protect your organization from check fraud.

**Use universal payment identification codes (UPIC) to encrypt your bank account information and ACH blocks and filters to help reduce your risk.**

A UPIC acts like a U.S. bank account number and protects sensitive banking information. It reduces the risk of unauthorized ACH debits, demand drafts, and fraudulent checks on the government's bank accounts through the use of encryption of the government's bank account information. An ACH debit block or filter protects against unauthorized ACH transactions. The government specifies which companies are authorized

to make debits from its accounts, including the dollar range of authorized debits, and the bank then filters and blocks all unauthorized transactions.

**Evaluate internal controls related to any new technology your organization has recently implemented.** Failure to do so could leave your organization vulnerable to fraud, waste, or abuse.


**Consider nurturing your relationship with your organization's internal controls.** Here are three ways to do it.

- Follow the Committee of Sponsoring Organizations of the Treadway Commission's Internal Control Integrated Framework to assess the government's existing internal controls. This includes understanding each of the Framework's five integrated components: 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. Reducing the opportunity for someone to commit a fraud is one of the best actions you can take.
- 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 isn't conducted because of any particular known fraudulent scheme; it is a means for the government to assess its own 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). Think about COVID-19 and whether the government has changed the way it provides services. Any changes could result in weakened or less effective controls.
- Complete a comprehensive review of the government'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 and in all types of job classifications. It is realistic to assume that employees in any job classification within your organization could steal from the government. Asset misappropriation, fraud, embezzlement, time theft—none of it looks good to the public.



There are hundreds of preventative and detective internal controls that should be in place within a local government organization.

## Conclusion

Failing to pay enough attention to a relationship can result in unpleasant consequences. This is true for interpersonal relationships and certainly true with your organization's relationship with internal controls—an ever-changing environment that needs and deserves regular attention. 

**David M. Ross** is CEO of 65th North Group. He has investigated more than 400 fraud cases and has completed numerous internal control and fraud risk assessments for local governments. He is a Certified Fraud Examiner and a Certified Internal Control Auditor who holds a COSO Certificate in Internal Controls. Dr. Ross completed Harvard University's Senior Executives in State and Local Government program and has a PhD in Financial Management with a dissertation in local government internal controls. He can be reached at 480-386-5344 or [dross@65thnorth.com](mailto:dross@65thnorth.com).

<sup>1</sup> Report to the Nations 2018 Global Study on Occupational Fraud and Abuse, Association of Certified Fraud Examiners, 2018.

<sup>2</sup> David M. Ross, *A Case Study of Municipal Government Financial Management and Effective Internal Controls*, 2016.

<sup>3</sup> U.C.C. Article 4—Bank Deposits and Collections Part 4: Relationship Between Payor Bank and its Customer §4-406, 2004.