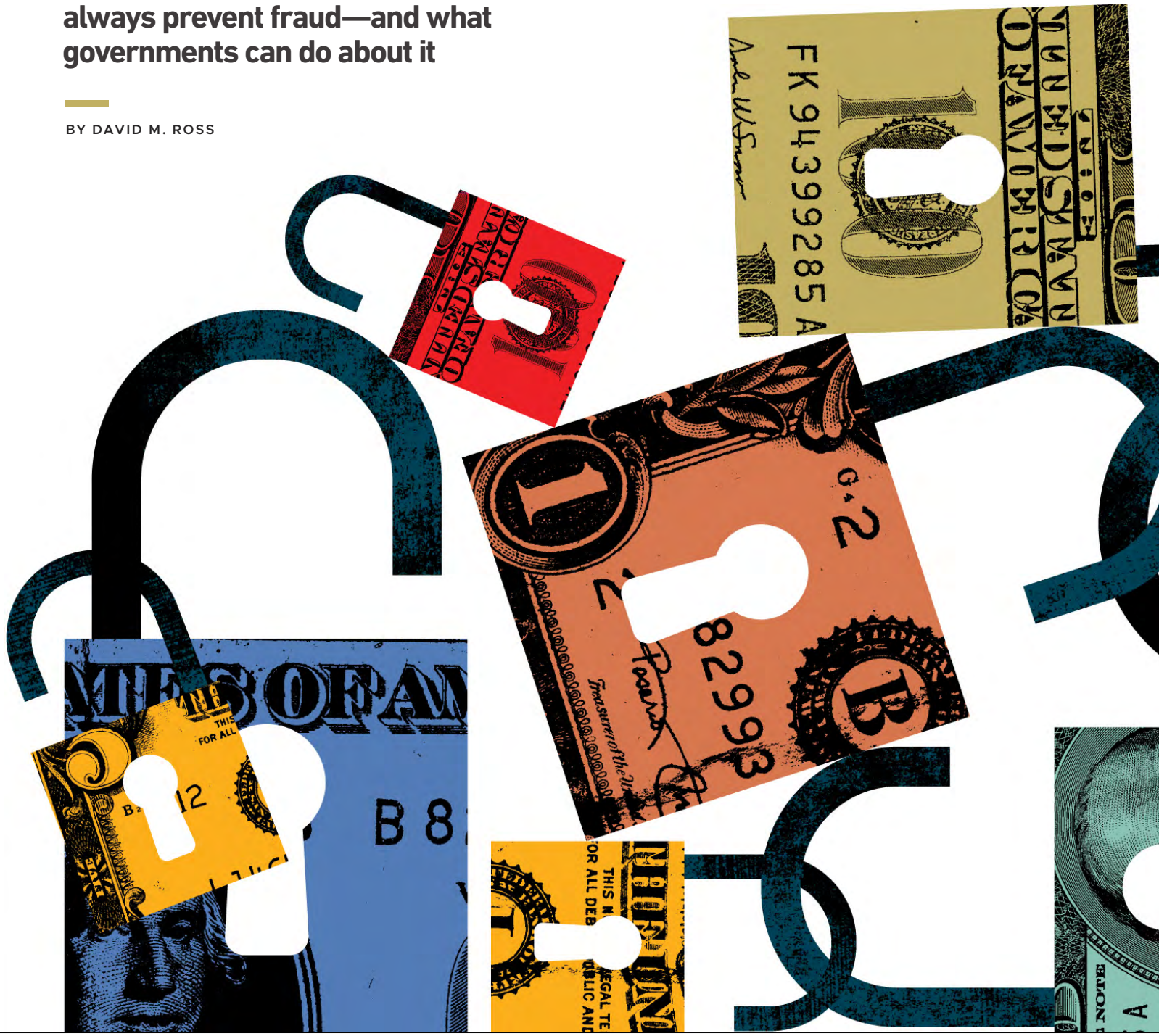
Reducing Risk

Why internal controls don't always prevent fraud—and what governments can do about it

BY DAVID M. ROSS



Do you fully understand the level of risk your organization faces? More governments are facing events like theft of cash, theft of fuel, ransomware attacks, successful spear phishing schemes, ACH vendor payment frauds, expense reimbursement schemes, purchasing and fraudulent return schemes, theft of inventory… It's a long and worrisome list, and many of the recent local government fraud and embezzlement cases are for tens of thousands, hundreds of thousands, or even millions of dollars.

This may be more of a senior management issue than we would like to believe. The lack of ethical decision-making on the part of the person committing the fraud is obviously the primary factor in these cases, but there's a problem when senior management believe their organization is well-protected without really knowing its vulnerabilities.

Not just a finance concern

Fraud and embezzlement incidents have occurred in numerous departments and are often perpetrated by long-time employees, in organizations with regular annual audits and established policies that "must be working" because the audits are "clean." Fraud can occur and go undetected over a period of years—or even decades. When these cases come to light, the reputational harm they cause the organization can be worse than the financial hit. Exhibit 1 highlights the financial and reputational harm that can come from an incident happening in your organization with quotes from news articles. (The incidents shown aren't recent, out of respect for the governments that have dealt with similar situations over the past few years.)

Do you believe everything is okay?

Local government organizations receive regular annual audits. They have established policies to protect against wrongdoing. They have trusted long-time employees. Fraud has never been found in the organization. So, managers believe that everything must be okay.

In general, we have a strong desire to believe that things are okay. We may also suffer from a touch of head-in-the-sand syndrome at times because we are busy and do not necessarily want to think about fraud, because the audit is "clean." And, of course, there are many other reasons.

But imagine for a moment that fraud is happening in your organization, or could happen soon, because of weaknesses in the control environment of which you are not aware. You honestly believe things are okay, but hundreds of managers are wrong about this every year. It is very possible

EXHIBIT 1 | FRAUD COVERAGE IN THE NEWS

"It's pretty embarrassing for the city to have that happen right under our noses."

– Councilman Roland Winters, from an April 27, 2016, azcentral.com news article about how a finance employee is accused of embezzling $836,000 from a city in Arizona.

"When 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?'"

–Commissioner Alex Tardif, from a May 3, 2018, article on iape.org reporting on a sheriff's office employee accused of stealing $650,000 from the organization.

"Whether you are a business or a government agency, you are vulnerable to fraud. You must have strong oversight and robust systems in place to prevent theft. Township government was victimized by this trusted employee, acting merely to amuse herself, and now the taxpayers will foot the bill."

–Chester County District Attorney Tom Hogan, speaking to phillyag.com in an April 6, 2018, piece about a township clerk who was accused of embezzling $250,000.

that the reason fraud has not been discovered is because there isn't any. But that could be because there are vulnerabilities in your organizational processes that nobody has tried to exploit—yet.

Your government may have vulnerabilities that you don't know about, and while annual audits serve an important purpose, ensuring your organization's internal controls are effective is not one of those purposes. The front of the audit report often states that the auditors will not express an opinion as to the effectiveness of the organization's internal controls because that is the responsibility of management. A "clean" external audit does not mean the organization doesn't have vulnerabilities.

External audits are generally ineffective at finding fraud. According to the Association of Certified Fraud Examiners, only about four percent of recent fraud cases were discovered by external audit. This means that 96 percent are discovered through other means.[1] The data shows that numerous local governments that fall victim to fraud find they were victimized for long periods of time, losing hundreds of thousands or millions of dollars, despite having policies in place and being audited annually.

Why do people steal?

People, systems, and processes change—and even with good policies, it is always possible that employees are not actually following them to best protect the organization. But why would a trusted employee steal from the organization? It comes back to the fraud triangle and its three specific legs: pressure, rationalization, and opportunity.

Pressure can be caused by a spouse losing their job, a health issue, a gambling problem, or any of a variety of circumstances that can arise in anyone's life. People don't usually go to work for a government with the intent to steal (although there are several cases where this has occurred). Often, it only happens after they have been there for a while, sometimes for years, and suddenly something happens, and they feel incredible financial pressure. They do not know what to do, but they realize that there are opportunities where they work for them to steal.

Rationalization is what happens when the employee feels the pressure and considers stealing but needs to rationalize it: "I'll only do it this one time," or "I'll just borrow it and pay it back soon," or "I deserve this because I've worked really hard over the years."

Opportunity is the real issue when we look at internal controls. Has the organization done enough to ensure that managers are aware of the vulnerabilities in all aspects of its processes? If the opportunity is there (like an as-yet-unexploited vulnerability that nobody has noticed), then there is internal control residual risk that must be better mitigated.

Reasons for fraud

Fraud comes in all shapes and sizes, and it happens in all departments. The following list is a handful of areas that are known to be vulnerable to embezzlement within local government:

- Fuel use management
- Procurement and purchasing functions, including fraudulent refund schemes
- IT and cybersecurity
- Utility operations and utility billing functions
- Grant management
- Human resource operations
- Permitting operations
- Inventory management, including equipment and small and attractive assets

A "clean" external audit does not mean the organization doesn't have vulnerabilities.

- Payroll management, including use of overtime
- Accounts payable and accounts receivable
- Cash handling in all departments
- Scheduled drug management (fire and EMS operations)
- Evidence handling and management (police operations)

Unfortunately, once a trusted employee embezzles and the act is finally uncovered, the damage is done—and it is real. Loss of public confidence, reputational harm, financial harm (which can include a moratorium on salary increases and deferred capital projects), supervisors and managers being fired, and elected officials losing the next election—these are all very real consequences that governments face.

Senior managers often encourage their employees to do great work and show sincere appreciation for all that they do. We grow to trust the people we work with every day. But ethics in local government demands that we do more than trust. This is because trust is vital for many aspects of our work, but trust is not a control. Combining a mindset of trustfulness with assuming the policies in place and an annual "clean" audit can lead to devastating consequences.

Increased vigilance is especially important because incidents of fraud are becoming more frequent. Fortunately, there are steps to take that will reduce the risk that your organization will be victimized by fraud.

What management can do

Fortunately, a comprehensive fraud risk assessment will often find dozens or even hundreds of legitimate control weaknesses and vulnerabilities. These vulnerabilities are found in highly professional organizations of all sizes, from governments with populations of a few thousand people all the way up to those with populations of more than a million people that have their own internal audit teams in place. Your organization can take the following proactive steps to reduce its risk of fraud and embezzlement.

- Complete a comprehensive fraud risk assessment throughout all levels of your organization—not just finance. Policies and procedures should be vetted by a certified fraud examiner with industry expertise and qualifications (which can be one of your own employees who is free from any conflicts of interest).
- Make sure the organization has an updated and modernized cybersecurity incident response plan, and that your team conducts regular tabletop exercises related to the contents of that plan.
- Make sure the organization has correctly implemented multifactor authentication for a variety of functions, including employee password resets and changing vendor banking information.

Conclusion

Ethics are breached in local government organizations far too frequently. Thinking that things are okay because nothing has happened before and you have long-term employees, established policies, and regular "clean" audits is dangerous. The amount of fraud committed against local governments each year is increasing, and the consequences of it happening at your organization can be significant.

David Ross *is a long-time city and county manager, and now president and chief executive officer of 65th North Group, a local government consulting firm that specializes in fraud risk reduction and internal control modernization.*

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