Internal Audit Report 18-06
Fraud Risk Assessment
December 2018

City of Sioux Falls
Internal Audit Department
Carnegie Town Hall
235 W. 10th Street
Sioux Falls, SD 57117-7402
www.siouxfalls.org/council/internal-audit

FRAUD RISK ASSESSMENT
INTERNAL AUDIT REPORT 18-06

INTRODUCTION

The City of Sioux Falls' (the City) Fraud Control Policy requires Internal Audit to perform a fraud risk assessment every five years. Fraud, in this policy, is defined as dishonest activity or other intentional misconduct causing actual or potential financial loss or reputational loss to the City. Examples would be embezzlement, theft of any asset, or authorizing or receiving compensation for hours not actually worked.

BACKGROUND

The Association of Certified Fraud Examiners (ACFE) classifies fraud into three broad categories:

- Asset misappropriation
- Financial statement fraud
- Corruption

Examples of asset misappropriation would be stealing cash or assets such as laptop computers or power tools. Financial statement fraud could involve presenting a false revenue and expense report to make an organization look more profitable that it truly was. It is often called "cooking the books." This might be done to increase the share price of a publically traded company. Corruption involves such things as the acceptance of bribes to the detriment of an organization. Within these three broad categories are numerous subcategories.

The ACFE estimates that organizations globally lose about 5% of their total revenue to fraud. This is based upon yearly surveys of organizations. The median loss for all organizations according to the ACFE in 2016 was $150,000. The median duration of the frauds was 18 months. However, the longer the fraud lasted, the greater the damage. The most common fraud scheme was asset misappropriation. The least common fraud reported was financial statement fraud. In cases where the government is a victim, the median loss at the federal level was $194,000. At the state level the median loss was $100,000. The local level median loss was $80,000. According the ACFE, local governments are a commonly victimized organization.

There is no typical profile for a fraudster. They come from every demographic and racial group. They typically have no criminal record prior to being caught. Only 5% of perpetrators in this ACFE survey had previously been convicted of a fraud-related crime. The number one way that frauds are uncovered is through a tip. The presence of anti-fraud controls was correlated in the ACFE survey with lower fraud losses and quicker detection.

Many managers believe that no one in their organization is stealing from them. They are convinced that their organization is different than others. They may say "we trust our employees." However, trust is an emotion; it is not a control activity. According to Peter D. Goldmann, founder and president of White-Collar Crime 101 LLC:

In reality, no organization is immune to fraud. Some organizations have less than others. But anyone in the anti-fraud profession will tell you that if a company, not-for-profit, or government agency says they have no fraud, they are either out-right lying or hopelessly naïve.[1]

OBJECTIVES

The objectives of this assessment were to:

1. Identify types of fraud cases the City, as an organization, has experienced.
2. Identify City assets, situations, or processes that may have moderate or high inherent fraud risk.
3. Identify key controls or control activities related to fraud prevention and detection.
4. Research a list of leading practices related to fraud prevention and detection and assess whether the City uses these practices.
5. Identify action steps related to fraud prevention and detection going forward.

SCOPE AND METHODOLOGY

The scope of this audit included fraud control policies and activities as they currently exist in the City. Our methodology included:

- A review of the literature concerning fraud and ways in which organizations are victimized.
- Research into leading practices related to fraud control.
- A review of fraud losses experienced by the City in years past.
- A review of past fraud risk assessments performed by Internal Audit.
- Interviews with City directors and their management teams.

Due to the constraints of available time and resources, we assessed inherent risks only. We did not assess residual risk. Residual risk is the risk remaining after controls are applied to the inherent risks.

RESULTS

Fraud cases the City has experienced

Corruption

An attempt at bid rigging was made approximately 20 years ago. An out-of-state contractor approached a local contractor about colluding on the bidding for a City contract. The local contractor reported this meeting to the City's elected officials. Law enforcement and the state's attorney were brought in. The decision was made to have the local contractor go along with the scheme so as to make a case for charging and arresting the out-of-state contractor. The contractor was charged and convicted.

[1] *Anti-Fraud Risk and Control Workbook,* p. 5 by Peter D. Goldmann with Hilton Kaufman, 2009.

Asset misappropriation-Sioux Falls Regional Landfill
Two cases of skimming customer cash payments at the Landfill came to light because of tips from the public. One case occurred about 1996 and resulted in the termination of the employee stealing cash. The other case was investigated by City internal auditors in 2001. That Landfill employee was arrested and charged by the Sioux Falls Police. The employee pled guilty in court and was terminated from City employment. The court-ordered restitution of $19,500 was eventually paid to the City by this former employee.

Asset misappropriation-Municipal golf course
The City owns three public golf courses. The courses are operated by a management company, not by City employees. However, the City does receive a percentage of the gross revenue generated by the golf courses. In the late 1990s a supervisor of the management company identified a cash skimming situation at one of the public courses. A seasonal employee of the management company was stealing green fees. The amount was estimated at approximately $15,000. The City required the management company to absorb the loss; that is, no public funds were lost.

Asset misappropriation-improper use of organization credit card
Several cases have occurred in the past ten years of City employees using a City purchasing card (P-card) to buy items for personal use with the intent that the City pay for these items. These situations were discovered through the monthly review of P-card purchases (the usual control activity). The City has terminated the employment of employees caught doing this.

Asset misappropriation-Automated Clearing House fraud scam
In April 2018, the City Finance Department received, via email, a vendor update request that appeared to legitimately come from a local approved vendor authorized to conduct business with the City. The request was to update the vendor's electronic payment information. The City later transferred two payments to the new bank routing address for legitimate work performed by the vendor. When the legitimate vendor did not receive expected payments, the scam was discovered. Automated clearing house (ACH) scams are a common fraud experienced by organizations. City Finance immediately reviewed and strengthened protocols and trained staff on the new procedures. The crime is being investigated by local and federal law enforcement and the City expects recovery of stolen funds either through recovery from the fraudsters or insurance coverage through the South Dakota Public Assurance Alliance.

City assets, situations, or processes with moderate or high inherent risk
We identified the following as having moderate fraud risk:

- **Cash or cash equivalents**. This would be defined as currency, coin, checks and credit/debit cards. Currency and coin have high value, are portable, and lack ownership markings. Checks and credit/debit cards are often processed by employees in high volumes. Dishonest employees may be tempted to convert such assets to their own use through a variety of schemes.
- **Investments**. These have high value and dishonest employees may be tempted to steal these funds if control activities are not robust and actively monitored.

- **Payroll**. This area would be considered moderate risk due to the possibility of management override of controls and the volume of funds processed. This would include all aspects of payroll: processing, changing employee pay records, and the recording of time worked by employees.
- **Purchasing cards**. These are also known as P-cards. P-cards are City credit cards entrusted to specific City employees to make small and routine purchases of supplies and materials. P-cards improve efficiency because the City saves the cost of processing purchase orders and invoices. However, they have an inherent moderate risk of fraud. Larger City purchases are done through the use of requisitions and purchase orders and have significant controls in place. P-cards do have controls but due to the nature of these cards, the risk of fraud can be reduced but not eliminated.
- **Grant funding**. These would also be considered moderate risk due to management override.
- **Capital assets**. If reasonably portable and useful for conversion to private use, some of the City's capital assets would be considered moderate risk for fraud.
- **Entities managing City facilities** or collecting and remitting funds on the behalf of the City. Organizations performing these functions are not under the internal control framework of the City. They may lack staffing to permit ideal segregation of duties. Staff and management in these situations may lack training in fraud awareness.

We identified **cyber threats** as having high inherent fraud risk. Computer security is a constantly evolving field. Fraudsters are continually developing new strategies for overcoming controls. This is a serious threat to municipalities. In March 2018 the City of Atlanta was the victim of a massive cyberattack. This particular attack was a ransomware attack.[2] City officials were forced to complete paper forms by hand due to the severity of the attack.

Overall, we would assess the City to be most at risk of victimization by corruption schemes or misappropriation of assets rather than financial statement manipulation. Financial statement manipulation is the least common fraud scheme according to the ACFE and City managers do not have any direct financial motivation (such as bonuses linked to financial results) to alter results. Additionally, external audits are performed yearly on the City's financial statements.

Key controls or control activities

We identified the following as key controls and control activities related to fraud prevention and detection:

- **Bank reconciliations** of all City-owned bank accounts. This is the procedure for comparing and matching figures from accounting records with those on a bank statement.
- **Master vendor file**. This file lists all the vendors authorized to do business with the City. Access and authority to make changes should be severely limited.

[2] Ransomware is a type of malware that infects a computer system and restricts access until the victim pays a ransom to the fraudster. When the ransom is paid, the computer system is "unlocked".

- **Personnel master file**. This file lists all authorized employees including their authorized pay. Access and authority to make changes should also be severely limited.
- **Segregation of duties**. This is a key control concept. No one employee should have control over two or more phases of a transaction or operation.
- **Control environment**. This is the most important element of the Committee of Sponsoring Organizations (COSO) framework of internal control. It is better known as "corporate culture" or "tone at the top". It is management's philosophy and operating style and its commitment to competence. It also involves the promotion of a positive workplace environment where employees are valued, properly trained, and engaged in their work. Engaged employees care about their work and the mission of the organization. They are less likely to consider defrauding their organization or tolerate those who do.

Leading anti-fraud practices

Based upon our research, review of past Internal Audit work, and interviews with City management we present the following leading anti-fraud practices and the current status of these practices:

1. Establish an **audit committee and an independent internal audit** function.
   Status: Implemented in 2006 and continuing to present.
2. Establish an **Employee Assistance Program (EAP)**.
   Status: Implemented in 2006 by Executive Order 11-06, the City has had continuing contracts with local providers to offer free or very affordable counseling sessions to employees struggling with addiction or difficult financial or family situations. Some employees are tempted to initiate fraud schemes in desperation because of these pressures. These services are strictly confidential.
3. Establish **segregation of duties** such that employees' work is checked by someone else. This is sometimes referred to as "checks and balances".
   Status: Implemented for the most part. Finance management regularly reviews this and Internal Audit reviews when performing audit work. In isolated situations, ideal segregation of duties is not practical. Compensating controls are implemented to address these situations.
4. Obtain **employee dishonesty insurance**.
   Status: Implemented. The City is required by State law to have this coverage.
5. Require **random drug screenings** and testing of employees.
   Status: Implemented.
6. Require **background checks** on all new hires.
   Status: Implemented. The type of checks is based upon the sensitivity of the position.
7. Maintain accurate and up-to-date **fixed asset inventory records** and review regularly. Unique asset numbers should be assigned and affixed to the assets. Spot checks should be performed and an annual verification of all assets should also be performed.
   Status: Implemented.
8. Placement of **surveillance cameras** in areas of inventory and cash handling.

Status: Implementation in higher risk areas such as the Sanitary Landfill scale house (where cash is received and processed).

9. Limiting **access to key data**.
   Status: Implemented. Access is reviewed to ensure that only employees with a need to know as part of their duties have access to key data whether financial, personnel, or other sensitive data.
10. **Regular review** of departmental/division revenue, expenses and budget performance.
    Status: Implemented. This is done by departmental/division management and business analysts in the Finance department.
11. Establish a **fraud, waste, and abuse hotline** for employees to report concerns anonymously.
    Status: Implemented in 2008 and continuing to present.
12. Ensure that **computer security** measures including firewalls are in place and up-to-date. Security policies should be reviewed and updated regularly. Other measures including antivirus protection should be continually updated and monitored.
    Status: Implemented. Internal Audit and the City's external audit firm, Eide Bailly, have performed audits of Information Technology. Management uses qualified consultants to perform penetration testing and review the City's protocols and protection of information technology systems.
13. Implement a **Code of Conduct** and **Fraud Policy.**
    Status: Ethics ordinances and a Board of Ethics exist. The City Council adopted a Fraud Control Policy by resolution on 11/20/2012.
14. Educate employees about fraud through **fraud awareness training.**
    Status: Implemented on a limited basis. Training was offered to management and Finance department employees in 2013. Finance department employees received training in 2018.

Action steps

Internal Audit will perform the following action steps and keep the Audit Committee informed of the status of completion:

1. Based upon our work on this assessment, we identified a few, isolated cases where the City may be receiving revenue in the form of checks that were not invoiced and were not necessarily expected. These "orphan checks" are inherently vulnerable to misappropriation.
2. We will determine if the level of employee dishonesty insurance coverage could and should be increased.
3. As part of our follow up to the citywide risk assessment report, we will identify opportunities for more continuous auditing of payroll, procurement, and accounts payable activities. This would involve data analysis software to identify anomalies in transaction for further investigation. This has been done on a limited basis in past years by Internal Audit but could be expanded and formalized.
4. A P-card audit is next on the Internal Audit schedule. It should be started in late 2018 and completed in spring 2019.

5. We will continue to advocate that periodic training for City employees in fraud awareness is offered. Information Technology will be conducting training for City employees in 2019 specific to phishing scams.[3]
6. We will review the administration's efforts to promote a work environment that results in an engaged workforce and a positive workplace environment.
7. We will review management's plans to offer ethics training to all City employees. The last citywide ethics training was conducted in 2007.
8. We will work with management to arrange for a "death audit" of pension recipients and beneficiaries. A death audit is a check of all individuals that receive a pension benefit to determine if they are still alive. A fraud scheme in this area involves a family member or close associate of a pensioner who has control or access to the pensioner's bank account. Should a pensioner pass away, this person is tempted to not inform the City that a pensioner has died and spends the pension money instead. A death audit involves hiring a firm that specializes in this work to search various data bases to determine if any pensioners appear to be deceased. The last death audit of the City's pension system was performed in 2003. These audits are typically modest in cost. A death audit should be performed on a regular schedule.

CONCLUSION

The City is robust in developing, implementing, and monitoring anti-fraud controls and activities. Any large and complex organization such as the City of Sioux Falls will have inherent risk in regards to fraud which can never be completely eliminated. However, current activities and continual monitoring and improvement can help protect City assets and limit damage as fraud schemes are identified.

AUTHORIZATION

The Sioux Falls City Council approved this assessment by resolution in February 2018 as part of the 2018 Annual Audit Program. The Internal Audit Division operates under the authority of an Internal Audit Charter adopted by City Council resolution 11-13.

AUDIT STANDARDS

Internal Audit conducts our work in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.

STATEMENT OF INDEPENDENCE

Internal Audit is administratively and operationally independent of the programs and departments it audits, both in appearance and in fact. The Internal Audit Manager is

[3] Phishing is the way that fraudsters get sensitive information like user names and passwords. They can use such information to steal money. It is often done by electronic mail. Both individuals and organizations are victimized by phishing scams.

accountable to an Audit Committee appointed by the City Council per section 32.022 of the Code of Ordinances of Sioux Falls, SD.

DISTRIBUTION OF REPORT

This report is intended for the information and use of the Mayor and City Council, management, and others within the City of Sioux Falls. However, the report is a matter of public record and its distribution is not limited.

PERFORMED BY

Rich Oksol
Internal Audit