

First Friday Fraud Facts

September 2, 2011



QUESTIONS OR COMMENTS:

Matt McBride, CGFM
Financial Specialist
P.O. Box 83720
Boise, ID 83720-0011

Phone: (208) 332-8805

Fax: (208) 334-3415

E-mail: mmcbride@sco.idaho.gov

Inside this issue:

Welcome	1
Fraud Exposure	1
IT Risks	1
Evaluating Fraud Potential	2
Using Technology as a Tool	3

The Oregon State Controller's Office created this newsletter. With their permission, the Idaho State Controller's Office edits and distributes this newsletter as a cost-effective method of increasing awareness about ways to detect and prevent fraud, waste, and abuse in government.

Welcome to First Friday Fraud Facts (F⁴). This edition will cover some of the risks advanced technologies have created and ways technology can be used to help prevent and detect fraud.

FRAUD EXPOSURE

Every organization is exposed to the risks of fraud in processes involving human interaction. The extent of the fraud exposure depends on the inherent risks in the business processes, the presence of effective internal controls to prevent or detect fraud, and the honesty and integrity of those involved in the processes. The exposure to fraud risks applies to all areas of an organization.

INFORMATION TECHNOLOGY (IT) RISKS

Technology has made many aspects of business operations much more efficient and streamlined. However, the increasingly digital environment in which we do business has also made it much easier for individuals to access confidential information for personal or malicious use. Much of the valuable information within an organization is collected, created, used, stored, maintained, disclosed, and discarded in a digital format. This information can be at risk from outside threats and individuals with unauthorized access.

Individuals within an organization that have legitimate access to the organization's information, systems, and networks can pose a significant risk, should they choose to use the information in an inappropriate manner. As covered in previous issues of F⁴, the motives to commit fraud range from financial pressures to revenge. Technical staff with access to systems and the ability to use their knowledge to sabotage systems or networks can result in an increased risk.



Several areas can pose increased risk for fraud when it comes to technology. Some of these include:

- Access to systems or data for personal gain
- Changes to system programs or data for personal gain
- Fictitious billings for services or misappropriations of employee, customer, or company confidential data for personal gain

EVALUATING FRAUD POTENTIAL

According to the Institute of Internal Auditors (IIA) Global Technology Audit Guide (GTAG) 13, "Fraud Prevention and Detection in an Automated World," two basic approaches are used to evaluate fraud schemes from the perspective of a fraud perpetrator: the control weaknesses approach and the key fields approach. Both approaches are designed to address who has the potential to commit fraud, what action the perpetrator would need to take, and what the indicators would be. Brainstorming with employees from key operational areas can also be a useful technique for assessing fraud risks and can be used with both approaches.

- The control weaknesses approach reviews the potential for fraud by examining key controls, determining who could take advantage of weaknesses, and how an individual could circumvent a control that may not be working properly.
- The key fields approach reviews fraud potential by considering the data being entered, which fields have potential to be manipulated, which individuals have the ability to manipulate fields, and what the effect would be if the fields were manipulated.

In addition to evaluating potential fraud from the perspective of the perpetrator, management may also consider the following fraud evaluation tools:

- Complete an agency-wide fraud risk assessment of all the significant areas of the organization and update regularly
- Ensure key elements, such as fraud risks, controls, and gaps are documented and updated
- Establish a process for remediation efforts
- Institute periodic security and fraud awareness training for employees at all levels
- Enforce segregation of duties

- Restrict access to systems and data to those with legitimate business purposes
- Implement strict password and identity management policies and practices
- Log, monitor, and audit employees' network actions
- Use extra caution with system administrators and other privileged users that could override controls
- Promptly deactivate computer access upon an employee's separation from employment

USING TECHNOLOGY AS A FRAUD DETECTION TOOL

Although technology can increase risks in some areas, technology can also be used to help prevent and detect fraud. Data analysis technology enables users to review data and obtain insights into the operating effectiveness of internal controls and to identify indicators of fraud risks or actual fraudulent activities.

According to the IIA's GTAG 13, the following analytical techniques can be highly effective in detecting fraud:

- Calculating statistical parameters to identify outlying transactions that could indicate fraud (i.e. averages, standard deviations, highest and lowest values)
- Classifying data to find patterns and associations of data elements
- Stratifying of numeric values to identify unusual values (i.e. excessively high or low values)
- Digital analysis using Benford's Law to identify statistically unlikely occurrences of specific digits in randomly occurring data sets
- Joining different data sources to identify inappropriately matching values such as names, addresses, and account numbers in disparate systems
- Duplicate testing to identify simple and complex duplications of business transactions such as payments, payroll, claims, or expense report line items
- Gap testing to identify missing numbers in sequential data
- Summing numeric values to check control totals that may have been falsified
- Validating data entry dates to identify posting or data entry times that are inappropriate or suspicious

