

First Friday Fraud Facts

December 4, 2009

Share your stories

If you have a case you would like to see shared in *First Friday Fraud Facts*, please let us know.

QUESTIONS OR COMMENTS:

Erin Haney, CIA
Statewide Financial Internal
Controls Officer
155 Cottage St NE, U50
Salem, OR 97301

Phone: 503-378-3156 ext. 277

Fax: 503-378-3514

E-mail: erin.d.haney@state.or.us

Inside this issue:

Welcome	1
Fraud Exposure	1
IT Risks	1
Evaluating Fraud Potential	2
Using Technology as a Tool	3
Training Opportunities	4

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

FRAUD EXPOSURE

Every organization is exposed to the risks of fraud in each process that involves 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, if not most, of the most 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 individuals with authorized access, as well as outside threats.

Individuals within an organization that have legitimate access to the organizations 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, there can be various motives from financial pressures to revenge, to mention a few. There can be an increased risk resulting from technical staff that not only have access to systems but the ability to use their knowledge to sabo-



tage systems or networks.

There are several areas that 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,” there are two basic approaches to evaluating fraud schemes from the perspective of a fraud perpetrator. These include 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 additional fraud evaluation tools. Some common tools include:

- Completing an agency-wide fraud risk assessment, this should include all significant areas of the organization.
- Ensure key elements such as fraud risks, controls, and gaps are documented
- Establish a process for remediation efforts
- Instituting periodic security and fraud awareness training for employees at all levels

- Enforcing segregation of duties
- Restricting access to systems and data to those with legitimate business purposes
- Implementing strict password and identity management policies and practices
- Logging, monitoring, and auditing employees' network actions
- Using extra caution with system administrators and other privileged users
- Promptly deactivating computer access upon an employee's separation from employment

USING TECHNOLOGY AS A FRAUD DETECTION TOOL

Although technology can increase risks in some areas, there are also several ways in which technology can be used to help in the prevention and detection of 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, there are a number of analytical techniques that can be highly effective in detecting fraud.

- Calculation of statistical parameters to identify outlying transactions that could indicate fraud (i.e. averages, standard deviations, highest and lowest values)
- Classification of data to find patterns and associations of groups of data elements
- Stratification 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 time that are inappropriate or suspicious



TRAINING OPPORTUNITIES

Information Technology Controls Forum—An Overview and Introduction to IT Controls

Date: December 8, 2009

Location: Oregon Employment Department—Auditorium

Cost: FREE

CPE: 3.0 credit Hours

This event is being sponsored by the Department of Administrative Services Internal Audit, State Data Center, and Enterprise Information Strategy & Policy Division. In collaboration with the Salem Chapter of the IIA, Oregon University System Internal Audit, and the Portland Chapter of the Information Systems Audit and Controls Association (ISACA).

Topics include: introduction to internal controls; IT controls and oversight; COBIT; ITIL; and an overview of enterprise security plans, programs, standards, and policies. For more information and to register for this event, visit the Salem Chapter of the IIA's website:

<http://www.theiia.org/chapters/index.cfm?act=home.page&cid=291>

**FIRST FRIDAY FRAUD FACTS IS
PUBLISHED BY THE STATE
CONTROLLER'S DIVISION**

Statewide Financial Services

155 Cottage Street NE

Salem, OR 97301

Phone: 503-378-3156

Fax: 503-378-3514

<http://www.oregon.gov/DAS/SCD/>

WHO CAN YOU CALL FOR HELP?

The State Controller's Division reminds state agencies that it is always available to answer internal control questions. If you have an internal control problem or an audit finding and need help in resolving it, please contact:

Erin Haney

**Statewide Financial Internal Control
Officer**

erin.d.haney@state.or.us

503-378-3156 x277

Internal control tools are on the Web!

http://www.oregon.gov/DAS/SCD/internal_controls.shtml