CPIM Academy

CPIM

Center For Public Investment Management

A PROGRAM BROUGHT TO YOU BY:

Josh Mandel

Treasurer of Ohio

CASH 120

Internal Controls / Fraud Prevention

2015

Introduction

Angela M. Gillis

- CPA, CIA, CFSA, CGAP
- Manager, Internal Audit and Risk Advisory Services
- Schneider Downs & Co.
- 18 years experience in external and internal auditing, accounting and financial management, risk advisory and consulting services

Agenda

- Fraud
  - The Basics, Statistics and Examples
  - Red Flags
  - Prevention Techniques
- The Fraud Risk Assessment
- Internal Controls
  - The Basics and Types of Internal Control
- Case Studies

Disclaimers

IRS CIRCULAR 230 DISCLOSURE: Any tax advice contained in this communication (or in any attachment) is not included or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code, or (ii) for promoting, marketing or recommending to another party any transaction or other matter addressed in this communication (or in any attachment).

The views expressed by the presenter do not necessarily represent the views, positions, or opinions of Schneider Downs & Co., Inc. These materials, and the oral presentation accompanying them, are for educational purposes only and do not constitute accounting, tax or legal advice or create an accountant-client or attorney-client relationship.

Fraud – The Basics

Fraud CAN and DOES happen

Fraud – The Basics

A fancy term for:

<u>Lying</u>

<u>Cheating</u> and

<u>Stealing</u>

Fraud – The Basics

It's never "black and white"

Fraud – The Basics

Occupational Fraud

"The use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets."

Fraud – The Basics

- Consider this …. .
  - Fraudsters can be creative
  - Fraudsters can appear trustworthy
  - Fraudsters can be long-standing, reliable employees
  - Fraudsters can be active members of the community
  - Fraudsters are sitting in the cubicle next to you
  - Fraudster are becoming more tech-savvy

Fraud - Prevention

Ethics and Fraud are so inter-connected. Without a strong ethical culture, fraud risk exponentially increases.

In most fraud cases uncovered, indicators that a fraud was occurring were evident to others. However, human nature is to continue to trust those around us even when faced with evidence to the contrary.

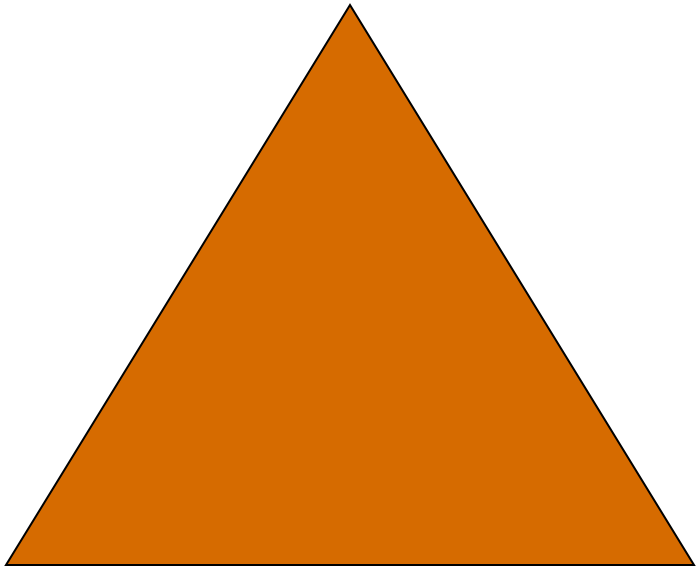
Misplaced Trust is a Great Facilitator of Fraud

Fraud – The Basics

The Fraud Triangle

Rationalization

(Justification of Act)



Opportunity

(Process and Controls)

Need/Pressure/ Motivation

(Influences /Incentives)

Fraud – The Basics

- An organization CANNOT control a fraudster's rationalization for his/her actions
- An organization CAN control the opportunities for the fraudster to commit the crime
- Consider the *capability* for the fraudster to commit the crime (the competence to execute)

Fraud – The Basics

- Consequences
  - Job loss
  - Reduction in future funding
  - Civil law suits
  - Criminal prosecution
  - Destroyed reputation (of the entity AND the individual)

Fraud – The Basics

Government fraud refers to illegal acts that intentionally divest the government of funds through deception or scams. When the government gets swindled,

<u>taxpayers pay the price.</u>

Fraud – The Basics

"There is no kind of dishonesty into which otherwise good people more easily and more frequently fall than that of defrauding the government."

- **Benjamin Franklin**

Fraud – The Statistics

- Typical organization loses 5% of revenues each year to fraud
- More than 42% of frauds are detected by tips
- In 58% of cases reported in 2014, the victim organizations have seen no losses recovered
- 85% of cases are due to asset misappropriation, but with the smallest loss
- 9% of cases are due to financial statement fraud, but with the largest loss

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2014)

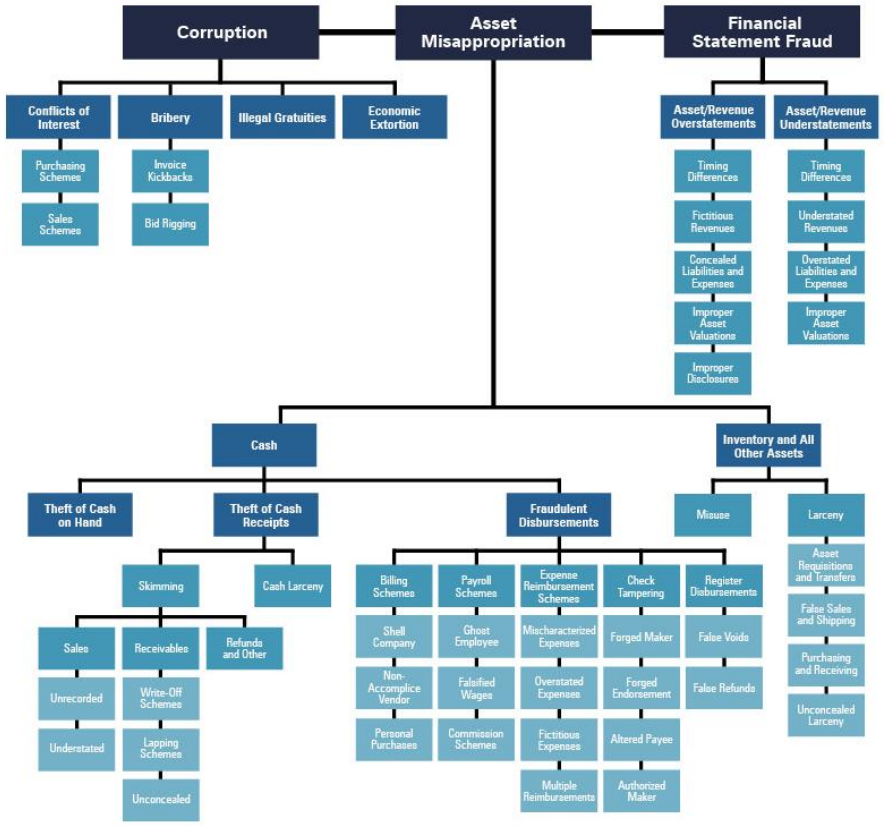
Fraud – The Statistics

- 82% of fraudsters had never previously been punished or terminated by an employer for fraud-related conduct
  - That means that 18% HAD been previous punished or terminated

Source: ACFE Report to the Nations on Occupational Fraud and Abuse (2014)

Fraud – The Fraud Tree

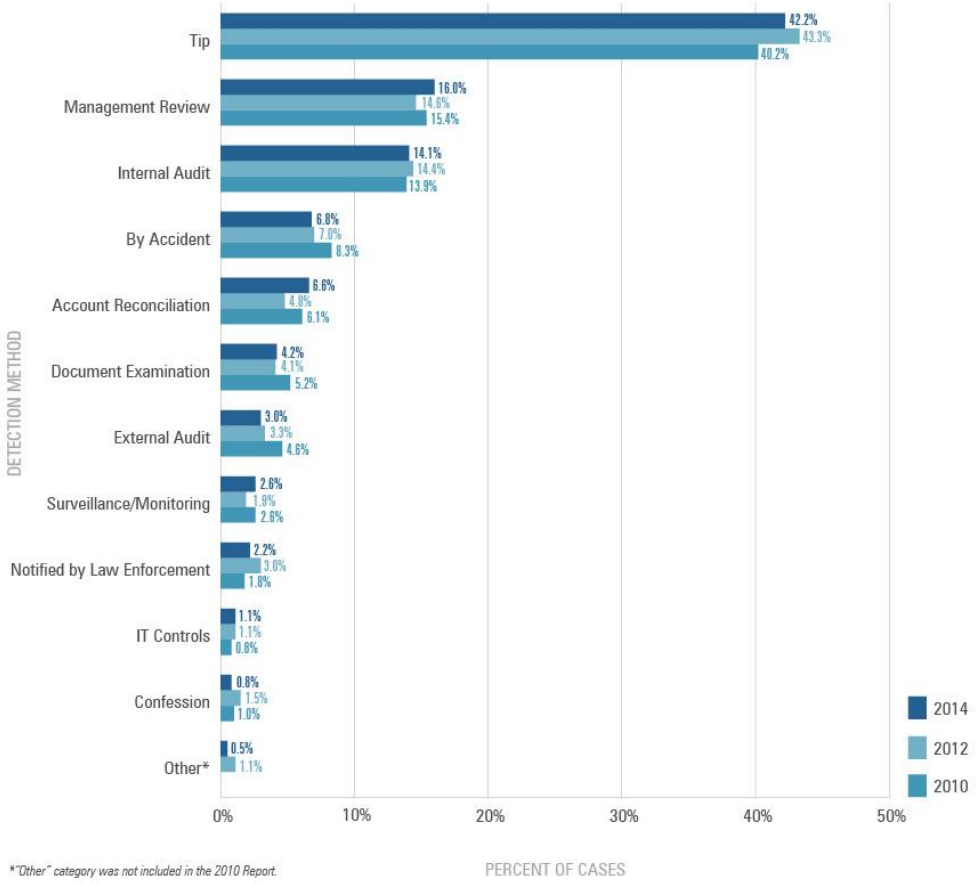
Figure 3: Occupational Fraud and Abuse Classification System (Fraud Tree)



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

Fraud – Sources of Detection

Figure 11: Initial Detection of Occupational Frauds

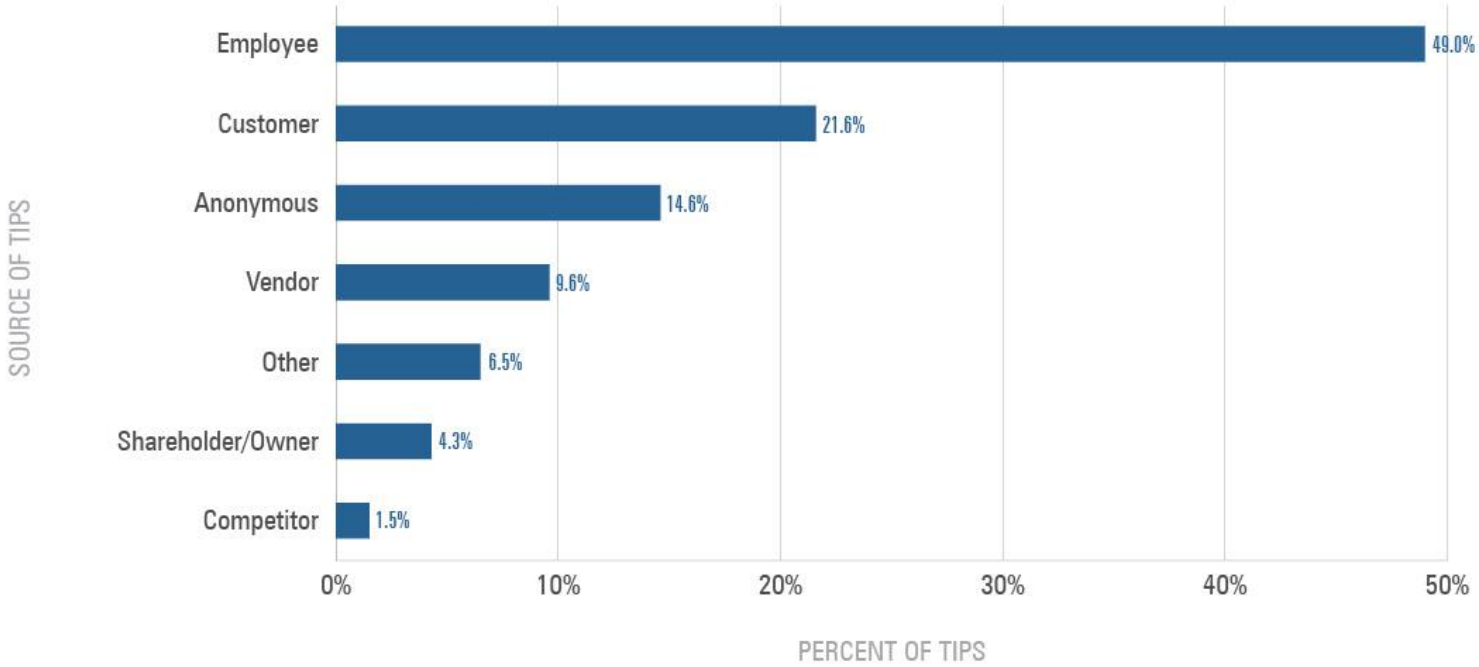


*"Other" category was not included in the 2010 Report.

© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

Fraud – Sources of Tips

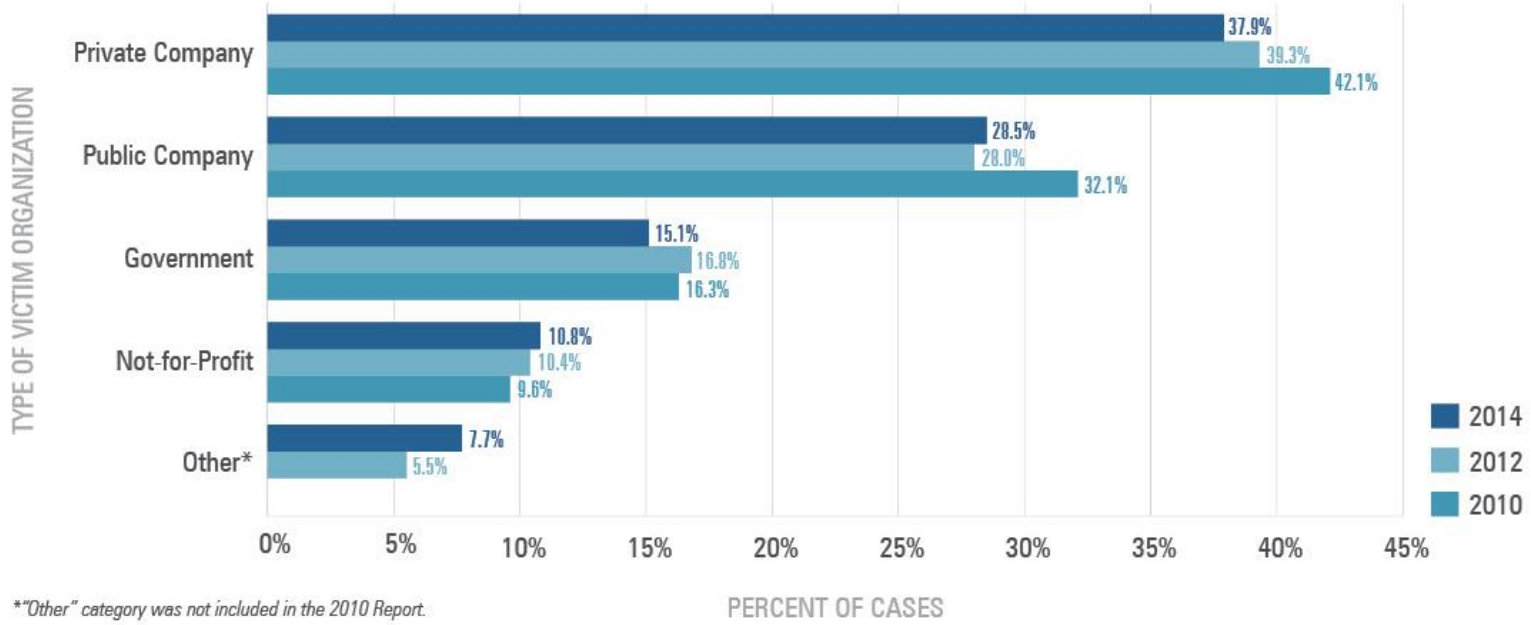
Figure 13: Source of Tips



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

Fraud – Type of Victim Organization

Figure 17: Type of Victim Organization — Frequency

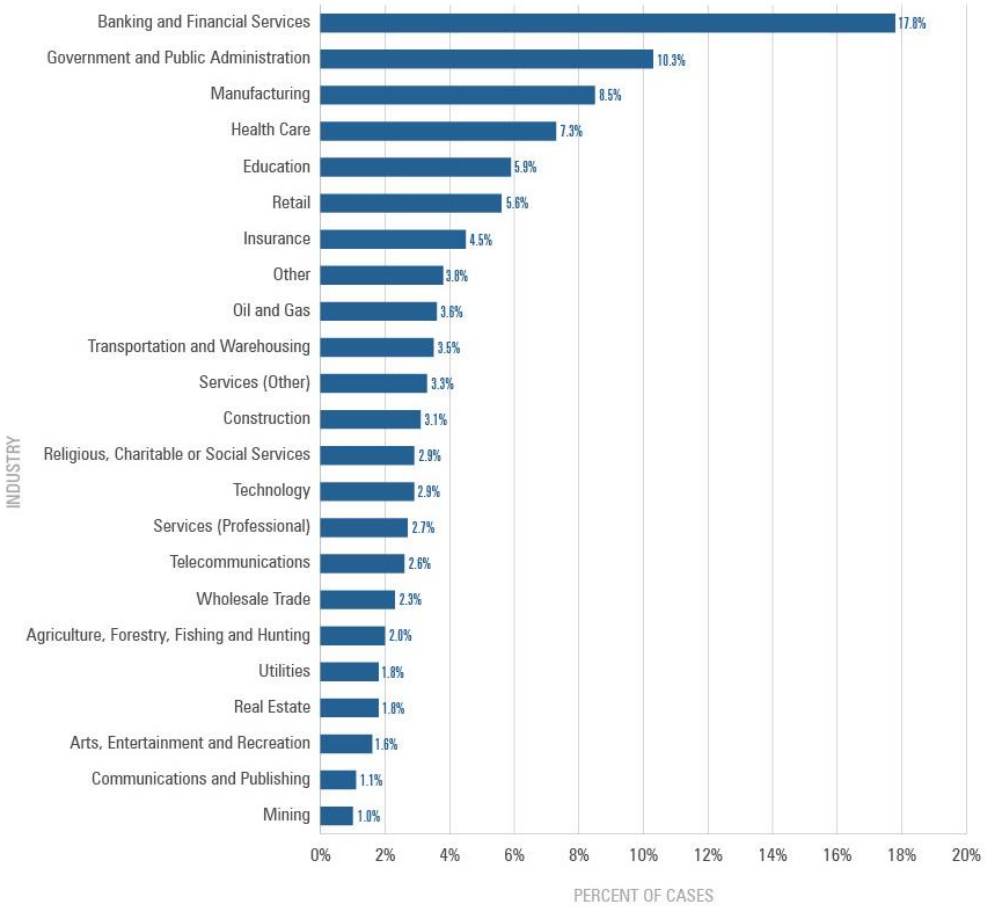


*"Other" category was not included in the 2010 Report.

© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

Fraud – Industry of Victim Organization

Figure 22: Industry of Victim Organizations



© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

Fraud - Examples

- Treasurer writes unauthorized checks to a business that he/she owns
- Clerk steals cash from the safe and creates fake deposit slips
- Treasurer diverts money received into personal accounts
- Use of government facilities for personal business
- Receiving kick-backs from vendors

Fraud – Red Flags

- Employees
  - Lifestyle or behavior changes
  - Personal debt or credit problems
  - Refusal to take vacation or sick leave
  - Excessive overtime
  - Lack of segregation of duties
  - Does not produce information voluntarily
  - Volatile, arrogant, confrontational or aggressive when challenged
  - Lack of a back-up for the role

Fraud – Red Flags

- Management
  - Reluctance to provide information
  - One individual is dominating decisions
  - Override of internal controls
  - High employee turnover
  - Unusual transactions made outside of the system
  - Financial distress/exhibits stress

Fraud – Red Flags

- Operations Indicators
  - Large number of write-offs
  - Discrepancies between bank deposits and postings
  - Excessive/unjustified cash and/or adjusting entries
  - Incomplete/untimely bank reconciliations
  - Lack of support or tracking of transactions

Fraud – Red Flags

- Cash Receipts and Disbursements
  - Lack of segregation of key duties
  - Missing deposits
  - Absence of a cash receipt log
  - Lack of controls over management signature
  - Uncontrolled access to blank checks

Fraud – Red Flags

- Purchasing
  - Lack of segregation of key duties
  - Excessive/unusual exceptions to purchasing policies
  - Uncontrolled access to the vendor master file
  - Vendors with employee names/addresses
  - Duplicate purchase orders
  - Copies of invoices used to pay vendors
  - Less than arms-length transactions and conflicts of interest
  - Undue influence

Fraud – Red Flags

- Fixed Assets
  - Lack of segregation of key duties
  - Lack of periodic inventories
  - Lack of asset tags/tracking
  - Lack of physical security

Fraud – Basic Prevention Techniques

- Tone at the top
- Open door policy
- Culture of compliance and ethics
- On-going and <u>required</u> anti-fraud training
- Fraud reporting tool (hotline)
- Fraud risk assessments
- **Strong internal controls**

Fraud – Basic Prevention Techniques

- **Strong internal controls**
- Adequate resources
- Robust hiring practices
- Periodic audits/reviews
- Identification of conflicts of interest
- Insist on adequate documentation

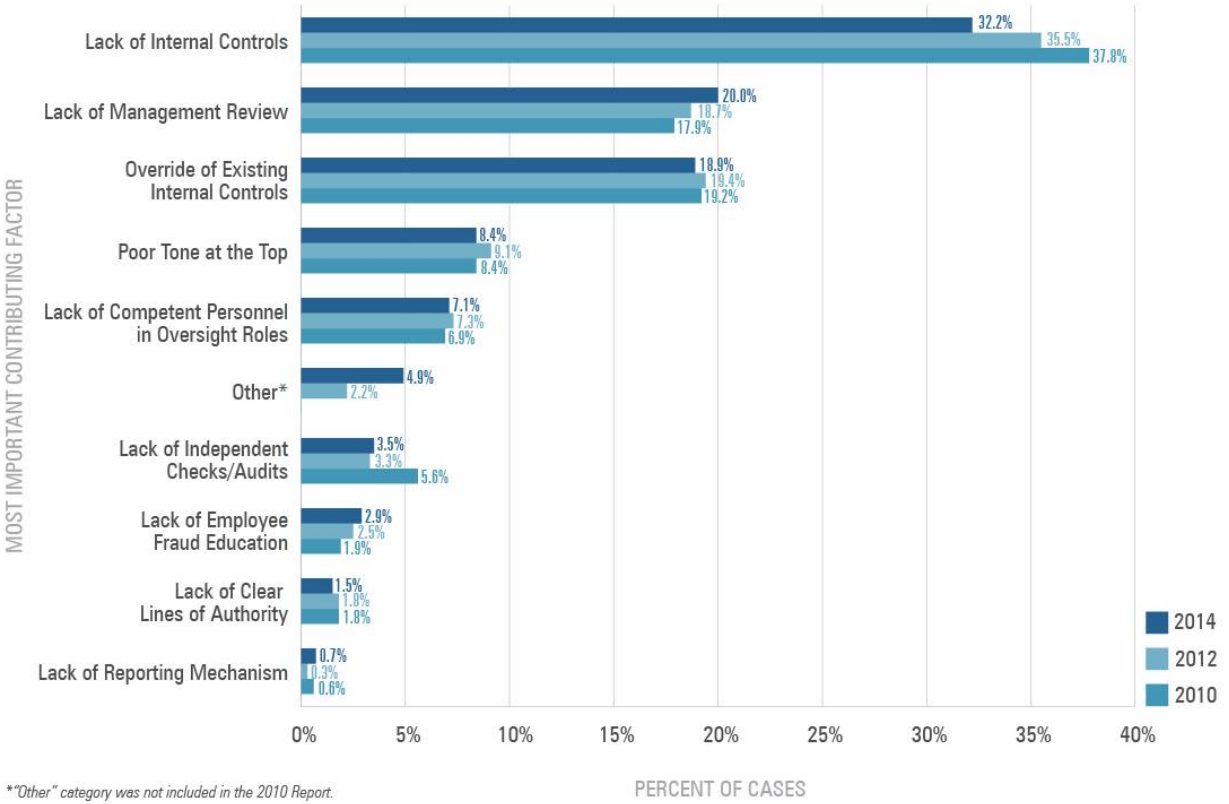
Fraud – Basic Prevention Techniques

- **And one more …**

Strong internal controls!!

Fraud – Contributors to Fraud

Figure 39: Primary Internal Control Weakness Observed by CFE



*"Other" category was not included in the 2010 Report.

© 2014 Association of Certified Fraud Examiners, Inc. All rights reserved.

The Fraud Risk Assessment

Step 1: Identify inherent fraud risk — Gather information to obtain the population of fraud risks that could apply to the organization.

Step 2: Assess likelihood and significance of inherent fraud risk — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes and interviews with staff.

Step 3: Respond to reasonably likely and significant inherent and residual fraud risks.

Step 4: Perform a cost-benefit analysis to decide what the response should be to address the identified risks and design controls.

The Fraud Risk Assessment

- **Identify Opportunities to Commit Fraud**
  - Create a profile that includes a list of the different areas in which fraud may occur and the types of fraud that are possible in each area (brainstorming, analysis of prior frauds, public information/Google alerts)
  - Consider the various types of schemes and scenarios that could occur within an organization
  - Don’t overlook information technology impact (enabler or deterrent)

The Fraud Risk Assessment

- Measuring Fraud Risk Tolerance

Probability/Likelihood

Prior instances, prevalence, and other factors, including volume of transactions and complexity, and number of people involved in the process should be considered

- Remote
- Reasonably possible
- Probable

The Fraud Risk Assessment

- Factors of Measuring Probability
  - Companies are downsizing
  - Budgets are decreasing
  - Companies are doing more with less
  - Increased government regulation
  - Stressed and disaffected employees
  - Stock pressure

The Fraud Risk Assessment

- Measuring Fraud Risk Tolerance

Severity/Impact

Should include financial, monetary, operational, reputational as well as criminal, civil and regulatory liability considerations

- High
- Moderate
- Low

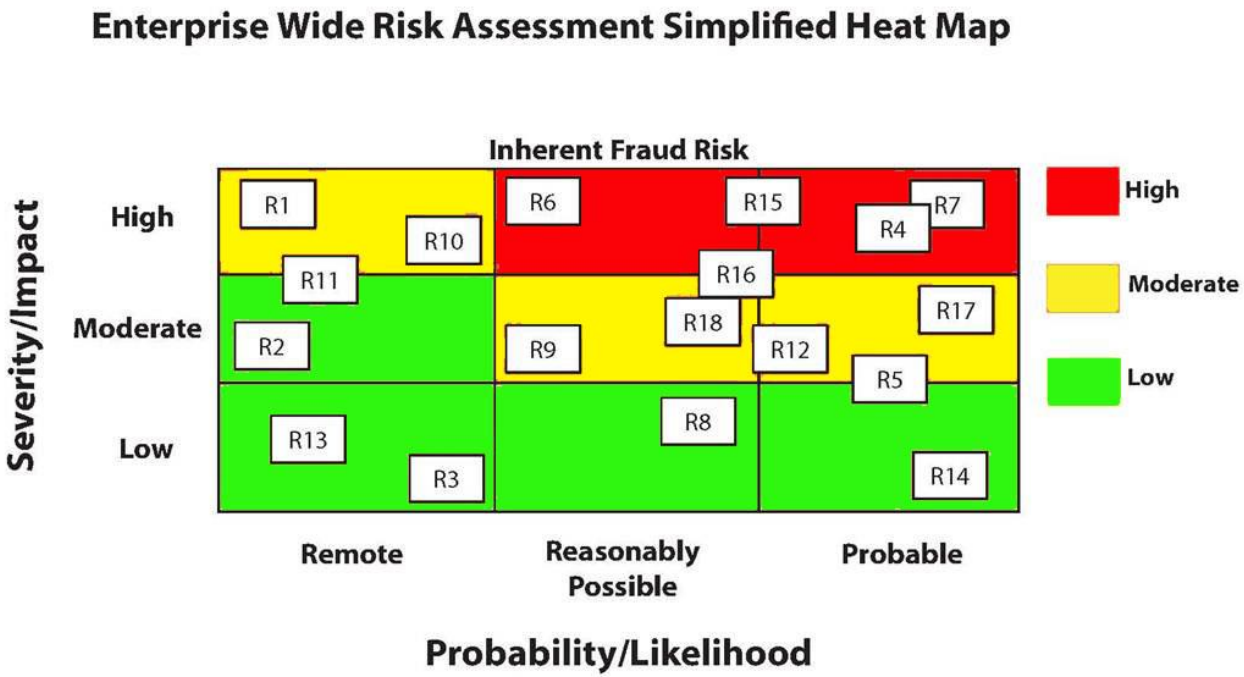
The Fraud Risk Assessment

Activity Name	Fraud Risk Assessment
Preparer	XXXX
Preparation Date	X/X/20XX
Updated by	XXXX
Last Revision Date	X/X/20XX

Potential Fraud Risk	Examples	Susceptible Process	Fraud Type	Potential Impact/ Severity (H,M,L)	Probability of Fraud Occurrence (H,M,L)	Inherent Fraud Risk (H,M,L)	Controls to Mitigate Inherent Risk	WP REF	Residual Fraud Risk (H,M.L)	Comment / Control Gap
Improper application of GAAP	Secure credit based upon improper accounting (falsify meeting the debt	Financial Reporting	Fraudulent Financial Reporting	H	M	H	Insert Control 1 Insert Control 2		H	
Inappropriate top-sided journal entries	Manipulation of financial performance	Financial Reporting	Fraudulent Financial Reporting	H	H	H	Insert Control 1 Insert Control 2		L	
Willfully miscalculating tax liabilities	Understating tax liabilities	Financial Reporting/Procurement/ Tax	Fraudulent Financial Reporting/Corruption	H	L	L	Insert Control 1		L	
Theft fixed assets	Taking of inventory without authorization, improper disposal of fixed assets	Fixed Asset Management/Financial Reporting	Fraudulent Financial Reporting/ Misappropriation of Assets	H	L	L	Insert Control 1 Insert Control 2 Insert Control 3 Insert Control 4 Insert Control 5		L	
Embezzlement	Check kiting; forgery	Procurement	Misappropriation of Assets	M	M	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Vendor abuse	Bribery, related-party collusion, extortion, kickbacks, preferential treatment, skimming, fictitious vendor billings	Procurement/Legal	Corruption/Misappropriation of Assets	H	L	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Related party transactions	Transactions not at "arms-length"	Procurement/Legal	Corruption	H	L	L	Insert Control 1		L	
Theft of proprietary confidential information	Trade secrets and customer lists sold to a competitor	Sales Management, Production	Theft of Sensitive Data	M	H	M	Insert Control 1 Insert Control 2 Insert Control 3		L	
Use of company assets for personal gain	Using company vehicles at side-business	Fixed Asset Management	Misappropriation of Assets	M	L	L	Insert Control 1		L	
Theft from company's operating account	Fraudulent disbursements to fictitious vendors	Cash and Treasury Management/ Accounts Payable	Fraudulent Financial Reporting	H	H	H	Insert Control 1		M	
Intentional manipulation, corruption and/or destruction of data	Destruction of customer records	Data Processing	Theft of Sensitive Data	H	M	H	Insert Control 1		M	

The Fraud Risk Assessment

Fraud Risk Assessment Heat Map



Threat	Level	Risks
High		5
Moderate		8
Low		5

Internal Controls – Development

- Designing and Implementing Controls
  - **Control Design**
    - Aligned with relevant fraud risks
    - Executed by competent and objective individuals
  - **Control Effectiveness**
    - Evidence available to support whether control is operating as intended
    - Control executed at a frequency appropriate to the fraud risk

Internal Controls – The Basics

- **Preventive** – Intended to reduce the risk of fraud occurring to an acceptable level
- **Detective** – Intended to flag potential risk that a fraud occurred in a timely manner
- **Persuasive** – Tone and culture of the organization, its belief system

Internal Controls – The Basics

- **Preventive Controls**
  - Human Resources procedures
    - Recruiting/hiring – smart, honest, ethical
    - Background investigations
    - Anti-fraud training
    - Exit interviews
  - Restricted Access
  - Segregation of duties (limit keys to the kingdom)
  - Authority limits
  - Transaction-level controls – approvals, reviews

Internal Controls – The Basics

- **Detective Controls**
  - Variance analysis – with communication and follow-up on unusual variances or items outside of thresholds
  - Comparison of internal data to external sources
  - Reconciliations
  - "Surprise" audits
  - Whistleblower hotline
  - Exit interviews (HR)

Internal Controls – The Basics

- **Detective Controls**
  - Independent reviews
  - Physical inspections and counts
  - Special audits – (e.g., expense reports, P-card activity)

Internal Controls – The Basics

- **Persuasive Controls**
  - Formal code of ethics/conduct
  - Management setting appropriate example
  - Positive workplace environment
  - Honest and constructive feedback and recognition
    - Eliminate fear of delivering "bad news"
    - Treat employees with fairness
    - Organizational responsibilities clearly defined
    - Strong communication practices and methods
    - Direct communication vs. innuendo

Case Study #1

- **School Employee**
  - Tax Evasion
  - Embezzlement of federal funds
  - Did not have signature authority, BUT had the trust of the supervisor with the signature authority
  - Supervisor signed blank checks
  - Payable to “cash” or fictitious employees
  - Concealment – false check register entries

Case Study #2

- **Chief Technology Officer of a municipality**
  - Wire fraud, bribery and falsified tax return
  - Manipulated procurement system for programs receiving federal funds
  - Receiving kickbacks and bribes for payment for technology services to a particular vendor

Case Study #3

- **Vendor Fraud**
  - Embezzlement of public funds paid to a vendor
  - Direction of funds paid to the vendor to a personal bank account

Resources

- **Ohio Auditor of State**
  - https://ohioauditor.gov/fraud.html
  - fraudohio@ohioauditor.gov
  - Call 1-866-Fraud-OH (1-866-372-8364)
  - 88 East Broad Street, PO #1140, Columbus, OH 43215

Resources

- **U.S. Government Accountability Office (GAO)**
  - http://www.gao.gov/fraudnet/fraudnet.htm
  - fraudnet@gao.gov
  - Call 1-800-424-5454
  - GAO FraudNet
    441 G Street NW
    Mail Stop 4T21
    Washington, DC 20548

Resources

- **Association of Certified Fraud Examiners (ACFE)**
  - http://www.acfe.com/rttn.aspx
  - Report to the Nations on Occupational Fraud and Abuse – 2014 Global Study
  - Download the full report or illustrations

Resources

- **The Association of Government Accountants (AGA)**
  - https://secure.agacgfm.org/tools/fraudprevention/
  - Fraud Prevention Toolkit

Contact Information

Angela M. Gillis
Manager
Internal Audit and Risk Advisory Services
CPA, CIA, CGAP, CFSA

Contact Information:
agillis@schneiderdowns.com
Work Phone: 614-586-7209

Business Address:
Schneider Downs & Co., Inc.
41 S. High Street
Suite 2100
Columbus, OH 43215