

CPIM

CENTER FOR PUBLIC INVESTMENT MANAGEMENT



A PROGRAM BROUGHT TO YOU BY:

JOSH MANDEL

TREASURER OF OHIO

SEC 210: Fraud Detection and Prevention

Introduction

Donald R. Owens

Shareholder

Internal Audit and Risk Advisory Services

CPA, CFF, CIA, CFSA, CRMA, CBA

Schneider Downs & Co., Inc.

41 S. High Street

Suite 2100

Columbus, OH 43215

Email: dowens@schneiderdowns.com

Work Phone: (614) 586-7257

Cell Phone: (614) 271-8551

Fax: (614) 621-4062

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

Strange new trend at the office. People putting names on food in the company fridge. Today I had a tuna sandwich named Kevin.



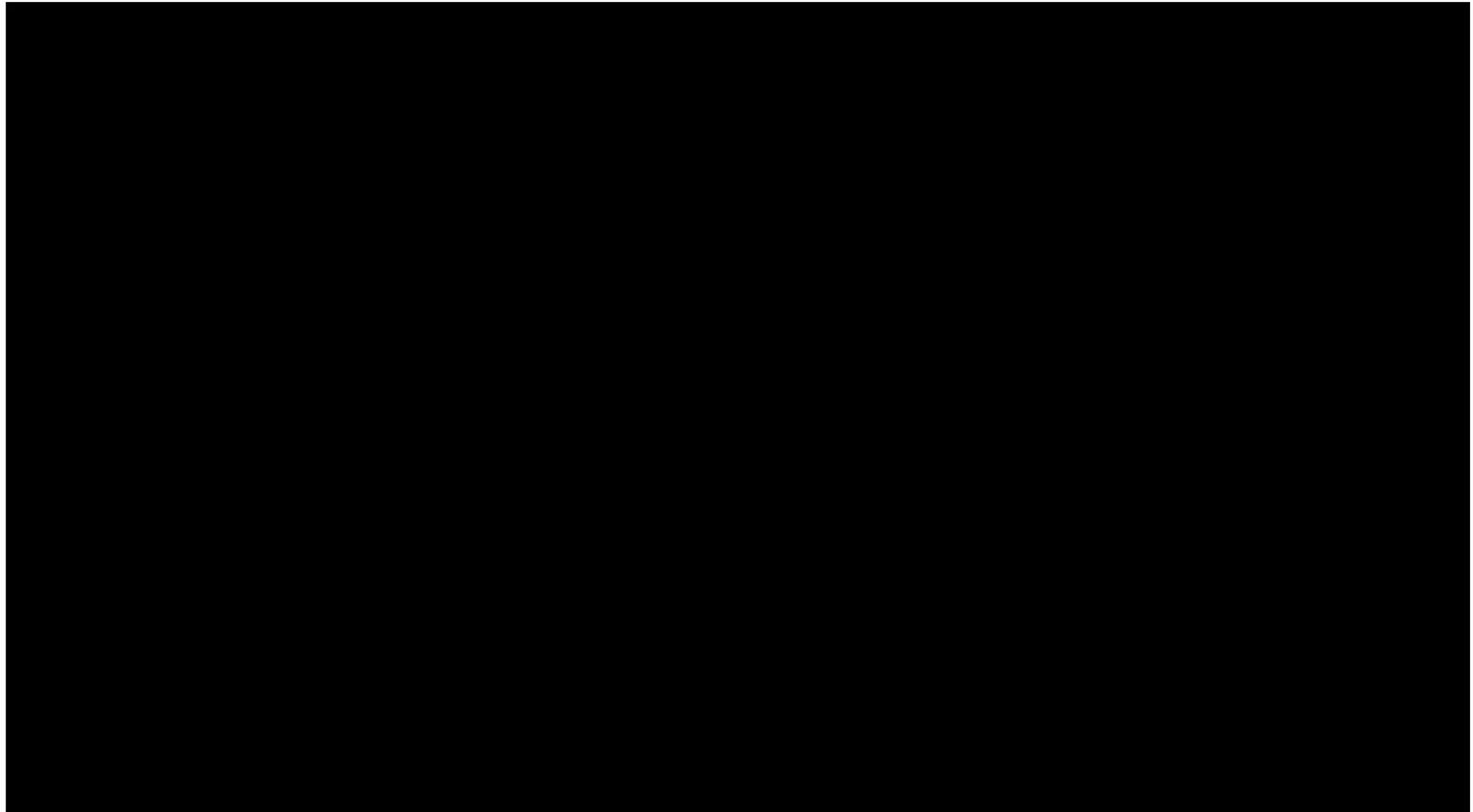
your  cards
someecards.com

Presentation Take-Aways

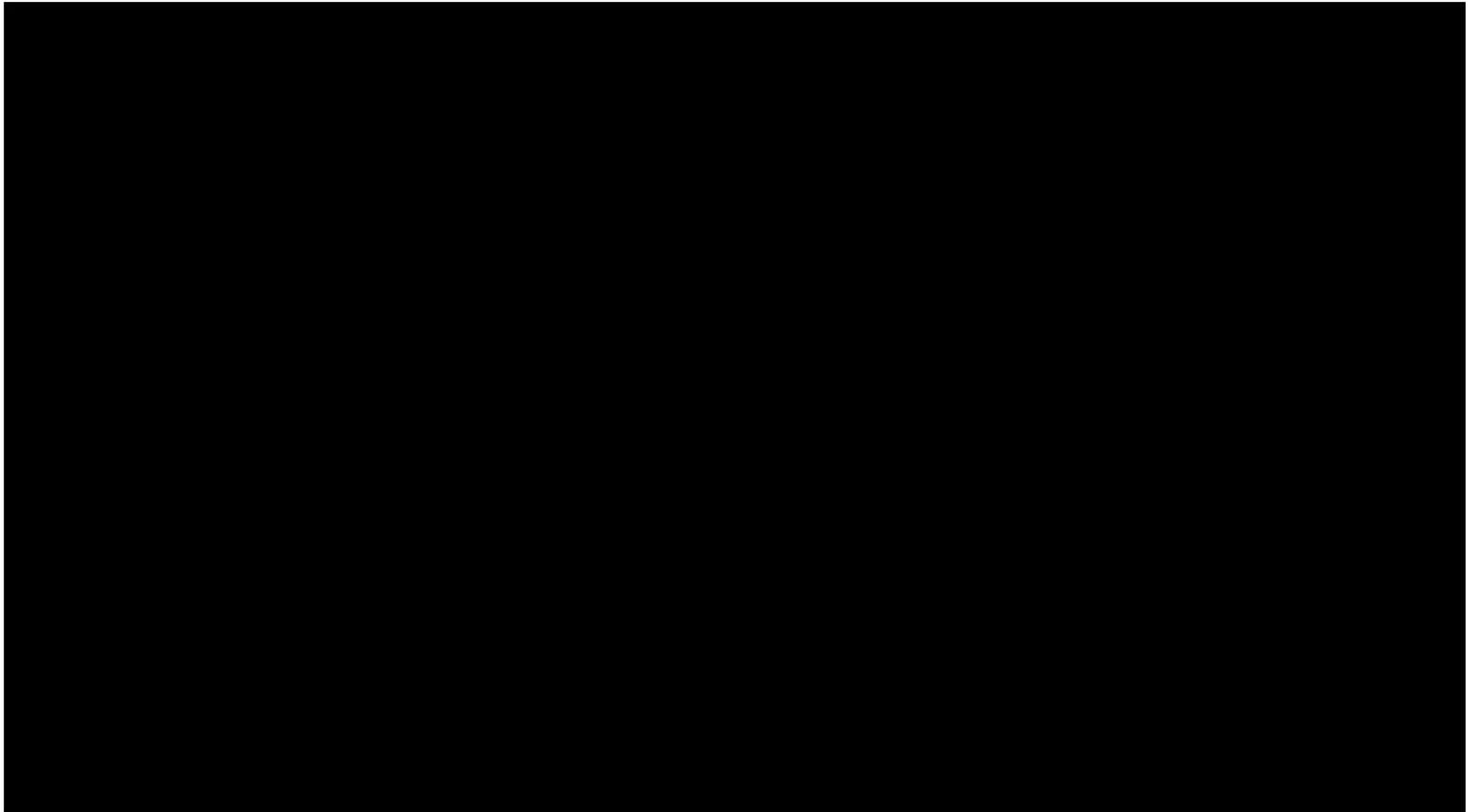
- Recognizing and assessing fraud threats in your environment
- How to effectively design and conduct fraud risk assessment
- Evaluating factors that contributed to frauds



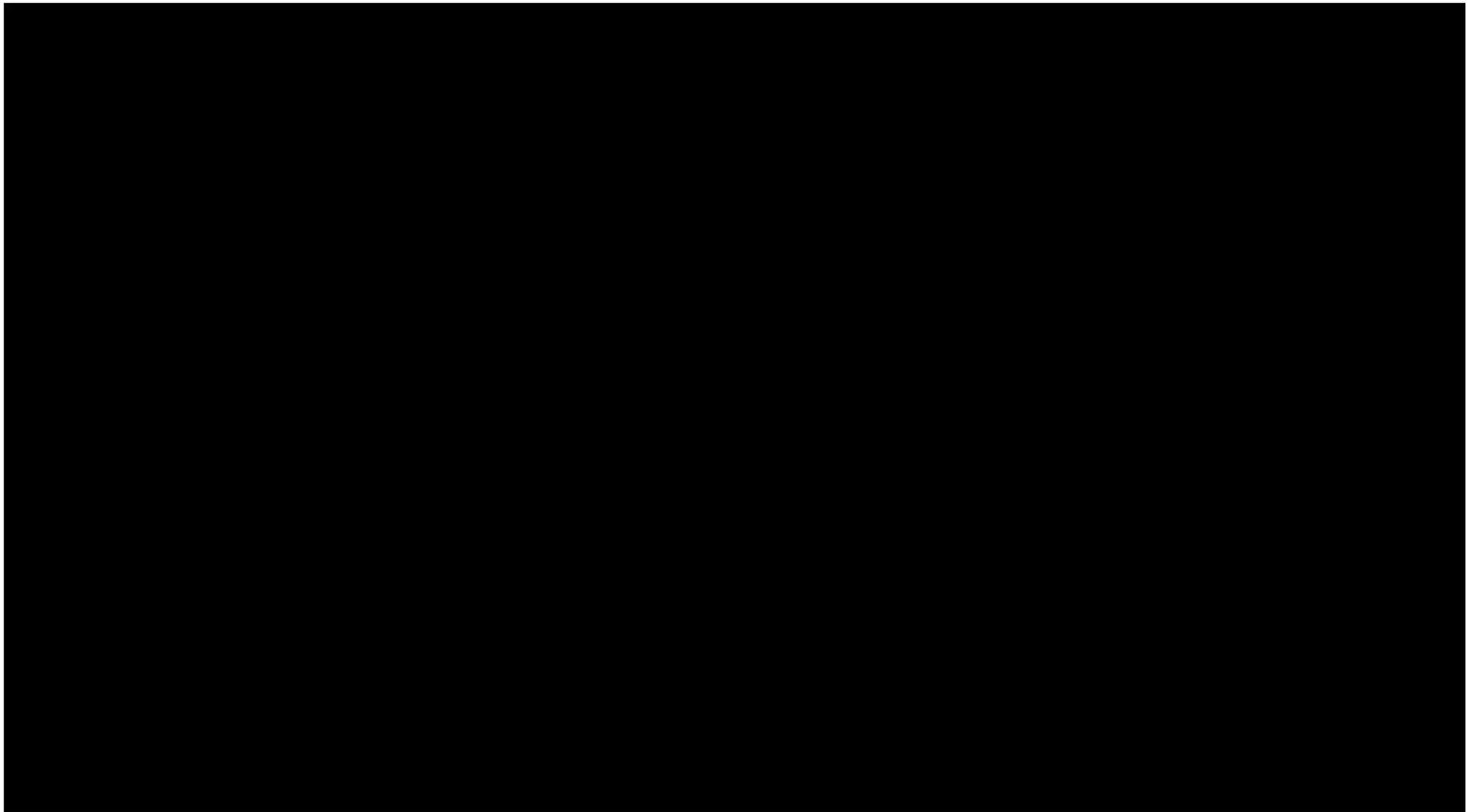
Recognize A Threat



Recognize A Threat

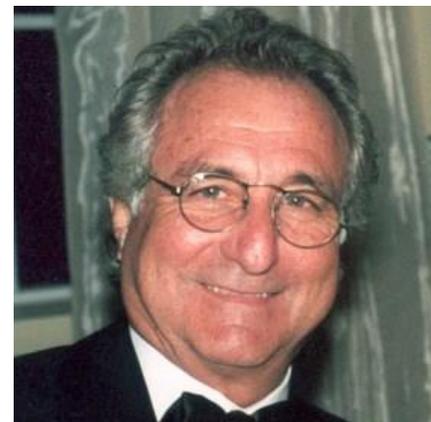


Recognize A Threat



Fraud and Its Faces

- Deliberate deception to secure unfair or unlawful gain
- Intentional deception of a person or entity by another made for monetary or personal gain
- Intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right



Fraud

“Fraud and stupidity look an awful lot alike.”



**- Alan Bachman, CFE, MBA
Education Manager at ACFE**

Fraud

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

When the government gets swindled, taxpayers pay the price.

Fraud

“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

Public Corruption – “It’s our top priority among criminal investigations”

Public corruption poses a fundamental threat to our national security and way of life. It impacts everything from how well our borders are secured and our neighborhoods protected... to verdicts handed down in courts... to the quality of our roads, schools, and other government services. And it takes a significant toll on our pocketbooks, wasting billions in tax dollars every year.

Agenda

- Fraud
 - Types of Fraud
 - Basics of Fraud
 - Statistics
 - Red Flags
 - Prevention
- Fraud Risk Assessment
- Internal Controls
- Whistleblower Program
- Resources



Types of Fraud

<u>Fraudulent Financial Reporting</u>	<u>Misappropriation of Assets</u>	<u>Corruption</u>
<ul style="list-style-type: none"> • Revenues • Expenses • Improper valuation or misclassification 	<ul style="list-style-type: none"> • Cash theft • Fraudulent disbursements • Payroll fraud • Expense reimbursement • Capital assets/inventory 	<ul style="list-style-type: none"> • Bribery • Bid rigging/Kickbacks • Illegal payments • Conflicts of interest • Aiding and abetting fraud (money laundering)
Almost always material - <u>directly impacts the financials</u>	May or may not be material - <u>directly impacts financials</u>	May or may not be material - <u>indirectly impacts the financials</u>
Almost always involves senior management	Can involve any level of employee	Can involve any level of employee
Controls are less effective in preventing and detecting fraud	Controls can be effective, particularly with regard to those below top management	Controls can be difficult and expensive to implement. Requires close scrutiny of employee activities and cost to do business

Types of Fraud

<u>Theft of Sensitive Data</u>	<u>Defrauding Customers</u>	<u>Compliance</u>
<ul style="list-style-type: none"> • Customer and employee personal information • Proprietary information/trade secrets • Patents, copyrights, other legally protected intellectual property 	<ul style="list-style-type: none"> • Intentionally misrepresenting products and services • Inflating invoices/duplicate billings • Shorting orders/product 	<ul style="list-style-type: none"> • Undocumented employees • Unrecorded wages • Unreported accidents • Manipulation of data • Unfair, deceptive acts
May or may not be material/measurable - <u>indirectly impacts the financials</u>	May or may not be material - <u>directly impacts financials</u>	May or may not be material - <u>indirectly impacts the financials</u>
Can involve any level of employee	Can involve any level of employee	Can involve any level of employee
Controls can be difficult and expensive to implement	Controls can be effective, particularly with regard to those below top management	Controls can be effective at all levels

Types of Fraud

Key Areas of Concern

- Credit and Debit Cards
- Corruption
- Billing
- Cash theft
- Payroll
- Personal expenses
- Third Party Vendors
- Related Parties



Basics of Fraud

Know that...

- Fraudsters are creative
- Fraudsters appear trustworthy
- Fraudsters are long-standing reliable employees
- Fraudsters are active members of the community
- Fraudsters are sitting in cubicles near to you
- Fraudsters are becoming more tech-savvy

Basics of Fraud

“82% of fraudsters had never previously been punished or terminated by an employer for fraud-related conduct.”



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

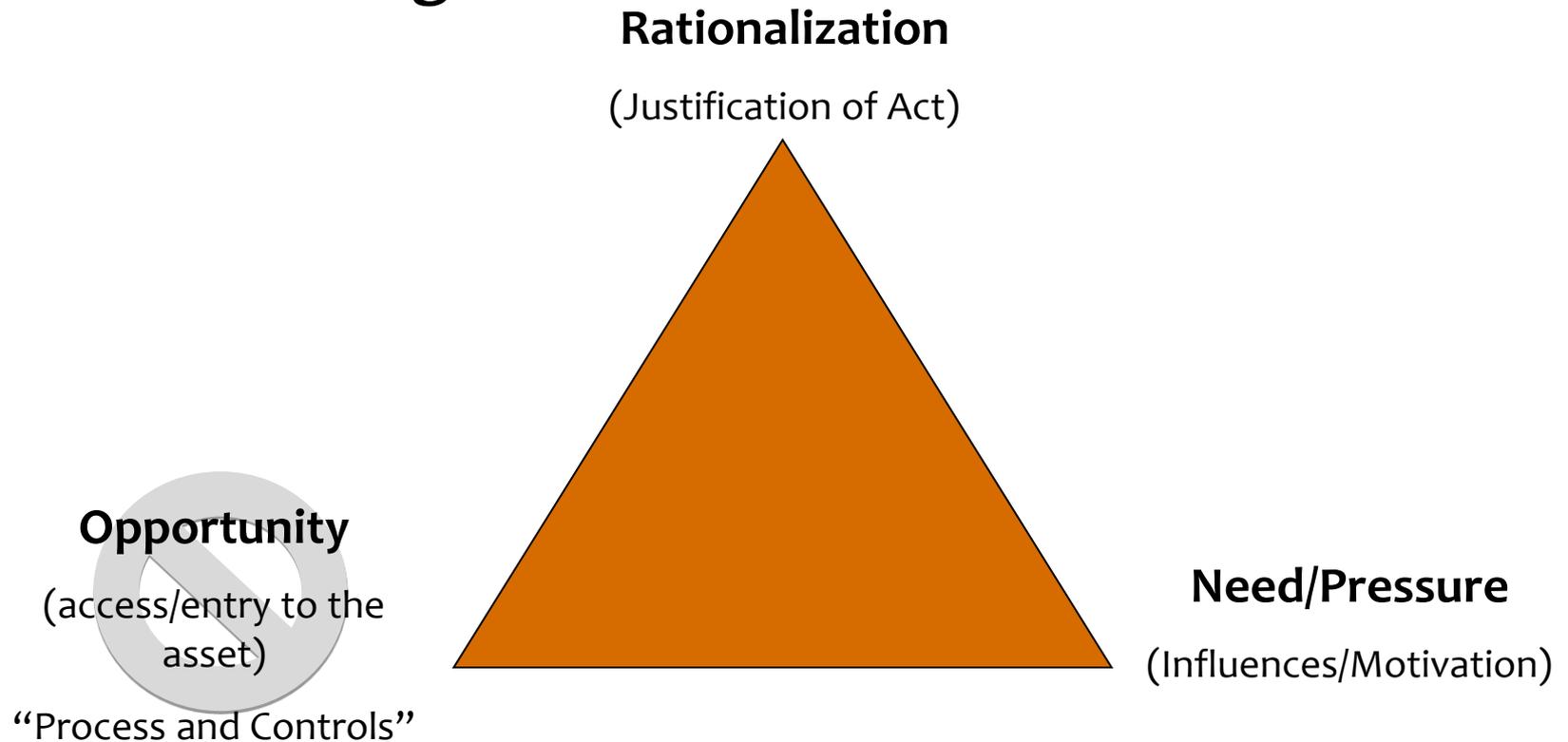
Basics of Fraud

Fraud or Not

- Teller removes cash from vault for personal use
- Finance Director withdraws funds from operating account and payroll, creates unsupported receivable entries to balance the records and conceal the action
- Risk Manager receives lucrative gifts from vendors
- Procurement Manager directs payment to his accounts
- Executive uses agencies assets for personal business

Basics of Fraud

The Fraud Triangle



Basics of Fraud

The Fraud Diamond/Rectangle

Incentive
(Influences/Motivation)

Rationalization
(Justification of Act)

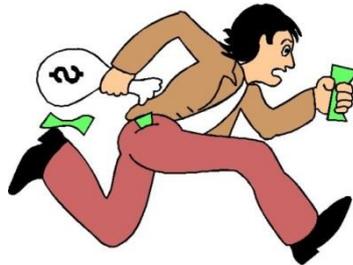


Basics of Fraud

- 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 *capabilities of employees* to commit the crime (competence to execute)

Basics of Fraud

Escalation Fraud Theory



Basics of Fraud

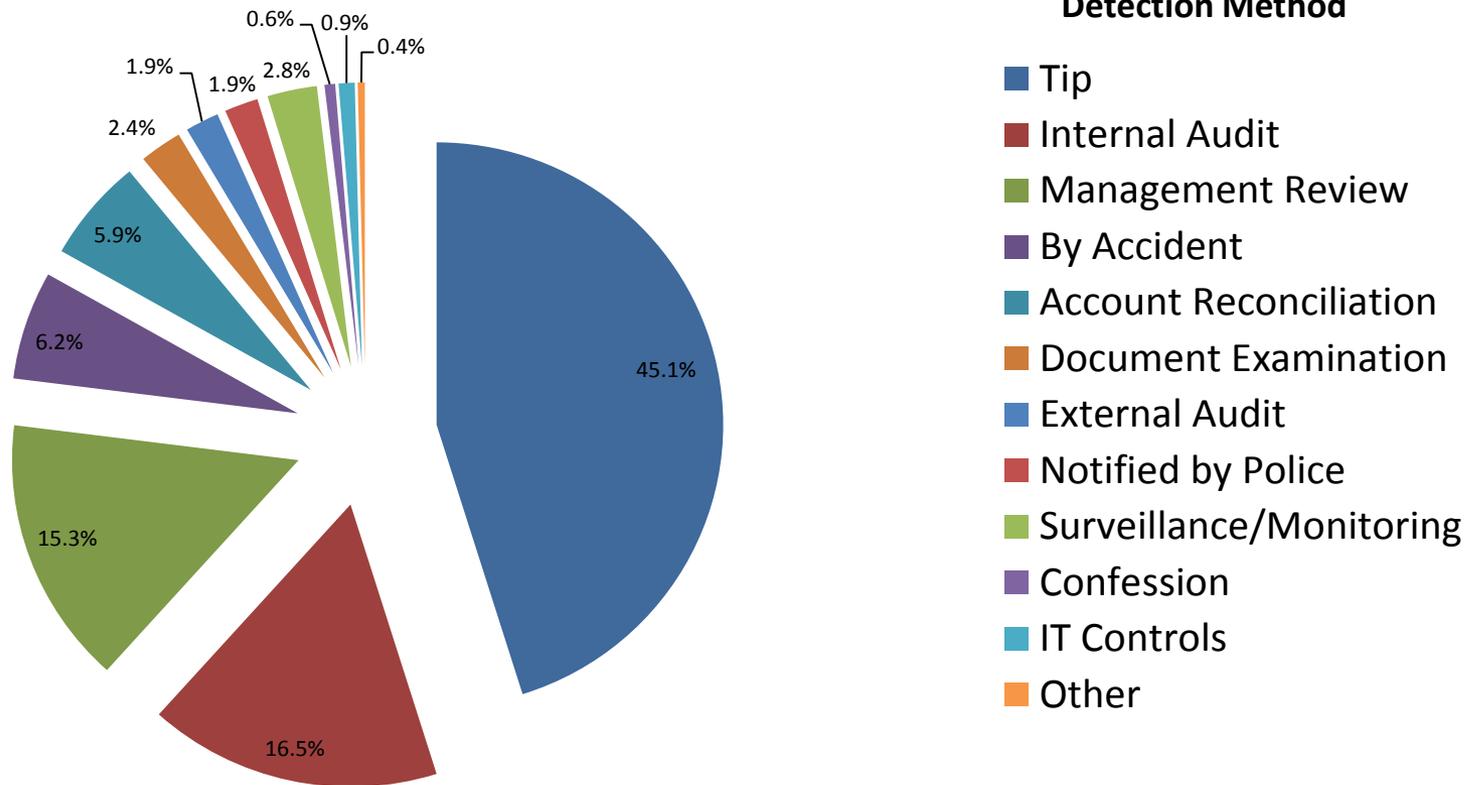
Consequences

- **Loss of assets**
- **Destroyed reputation** (both entity AND the individual)
- Job loss
- Civil law suits
- Criminal prosecution



Fraud Statistics

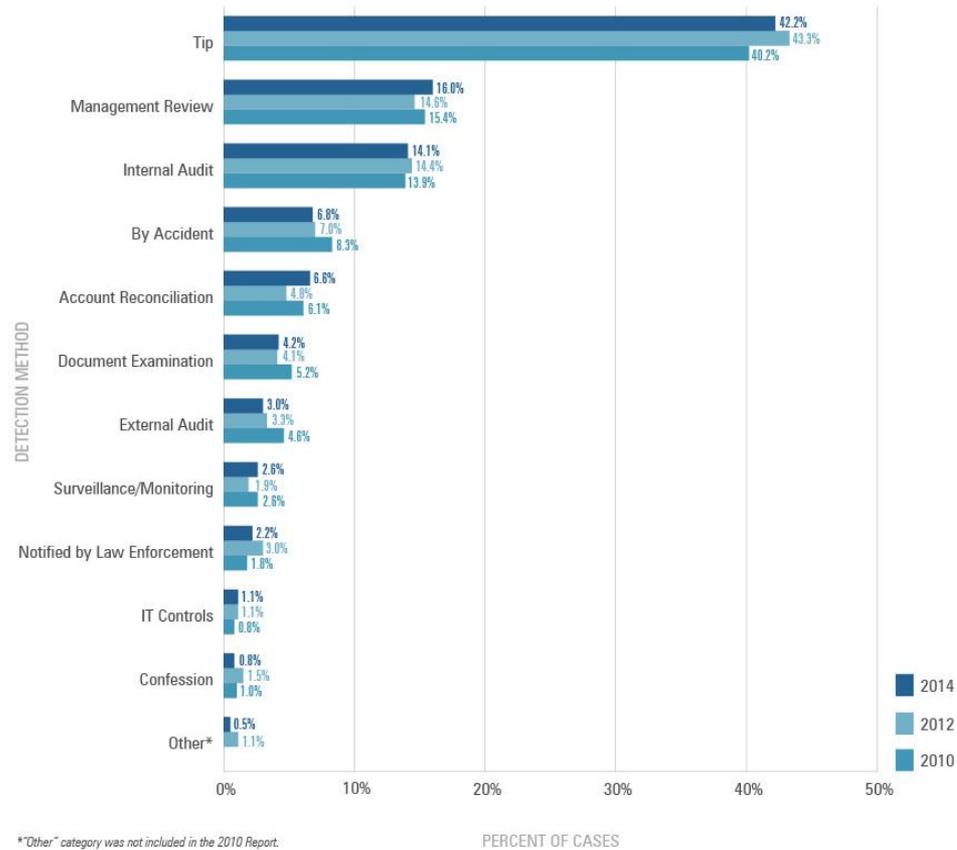
Sources of Detection



2014 Association of Certified Fraud Examiners Fraud Study

Fraud Statistics

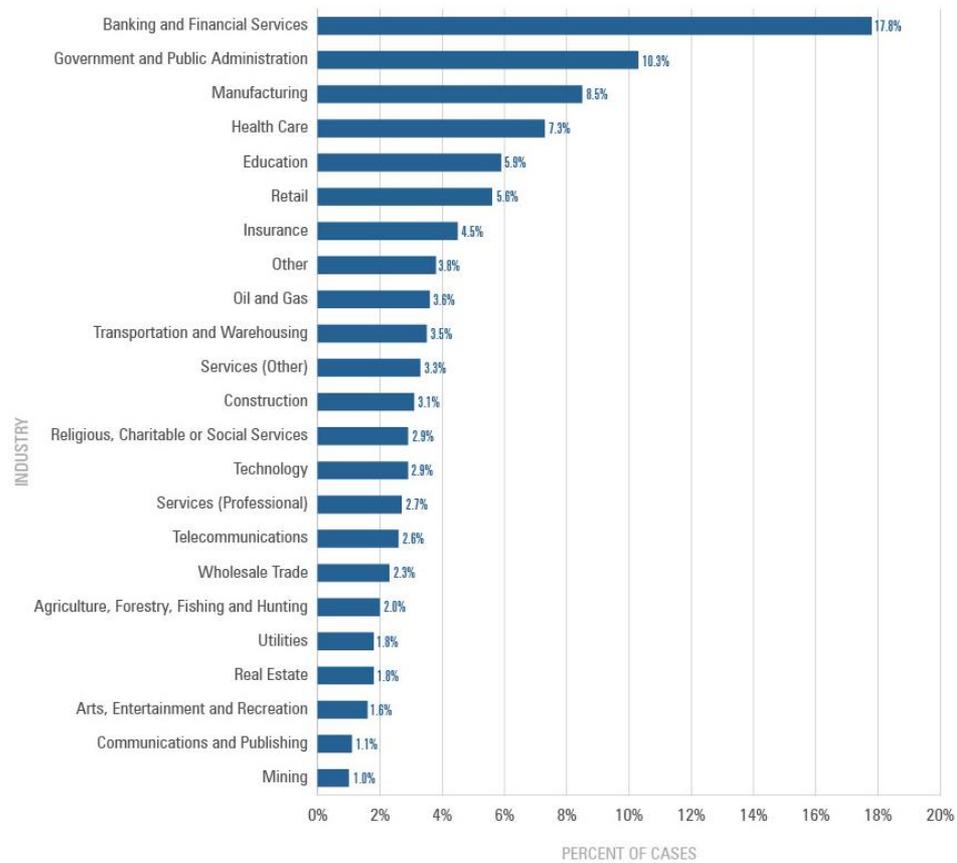
Figure 11: Initial Detection of Occupational Frauds



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

Fraud Statistics

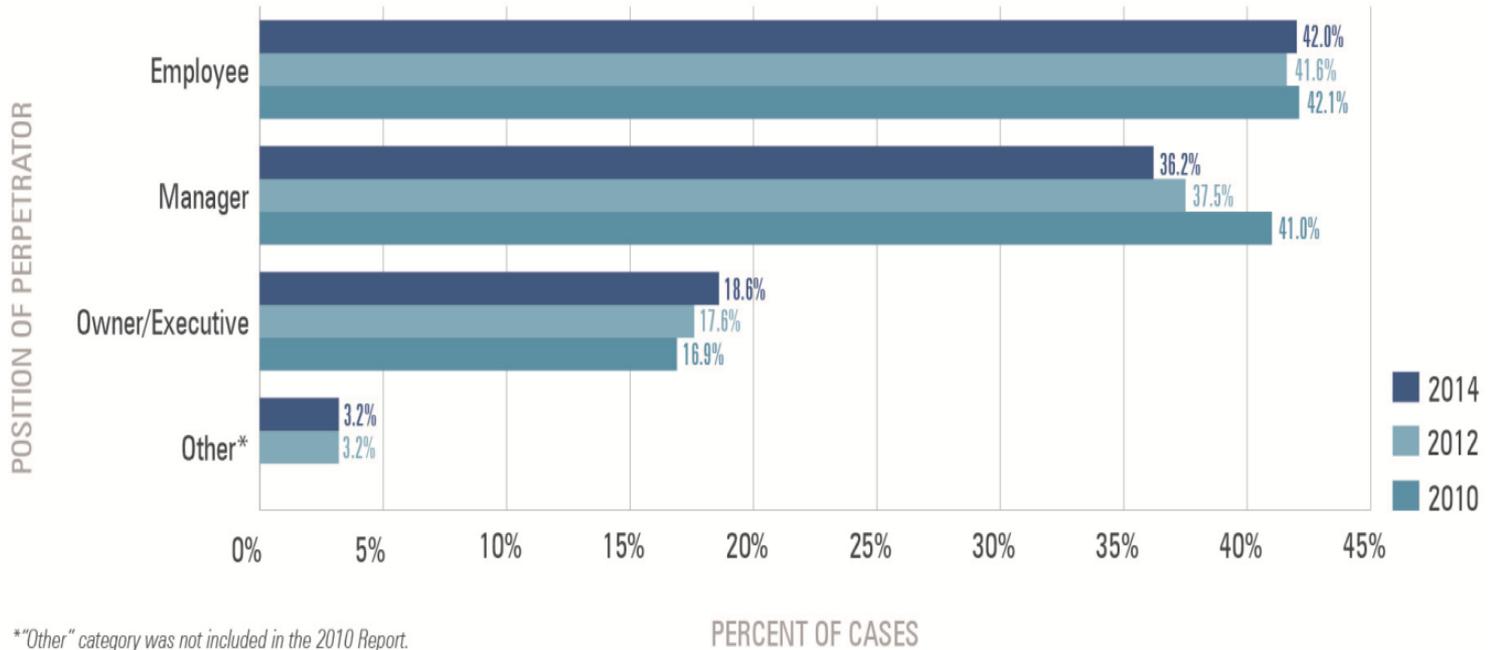
Figure 22: Industry of Victim Organizations



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

Fraud Statistics

Figure 40: Position of Perpetrator — Frequency



Fraud Statistics

Figure 41: Position of Perpetrator — Median Loss



Fraud



Fraud Red Flags

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 Red Flags

Fraud Opportunity

Employee's years of service

X

Number of key responsibilities residing with the employee

X

Organization's complacency level with respect to validating controls
and monitoring activities

=

Potential for fraud to be committed

Fraud Red Flags

Employee Habits

- Lifestyle or behavior changes
- Personal debt or credit problems
- Refusal to take vacation or sick leave
- Excessive overtime
- Does not produce information voluntarily
- Volatile, arrogant, confrontational or aggressive when challenged
- Indignant with respect to training a back-up

Fraud Red Flags

Management

- Reluctance to provide information
- Dominates all decisions
- Overrides internal controls
- High employee turnover
- Unusual transactions made outside of the system
- Exhibits unusual stress
- Retains excessive authorities and duties (Lack of segregation)

Fraud Red Flags

Operational Indicators

- Large number of write-offs
- Discrepancies between bank deposits and postings/book
- Excessive/unjustified cash adjusting entries
- Incomplete/untimely bank reconciliations
- Lack of support for transactions
- Missing or presumed misplace equipment

Fraud Red Flags

Cash Receipts and Disbursements

- **Lack of segregation of key duties**
 - **Physical/Manual Duties**
 - **System Capabilities**
- 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 inventory of assets
- Lack of asset tags/tracking
- Lack of physical security

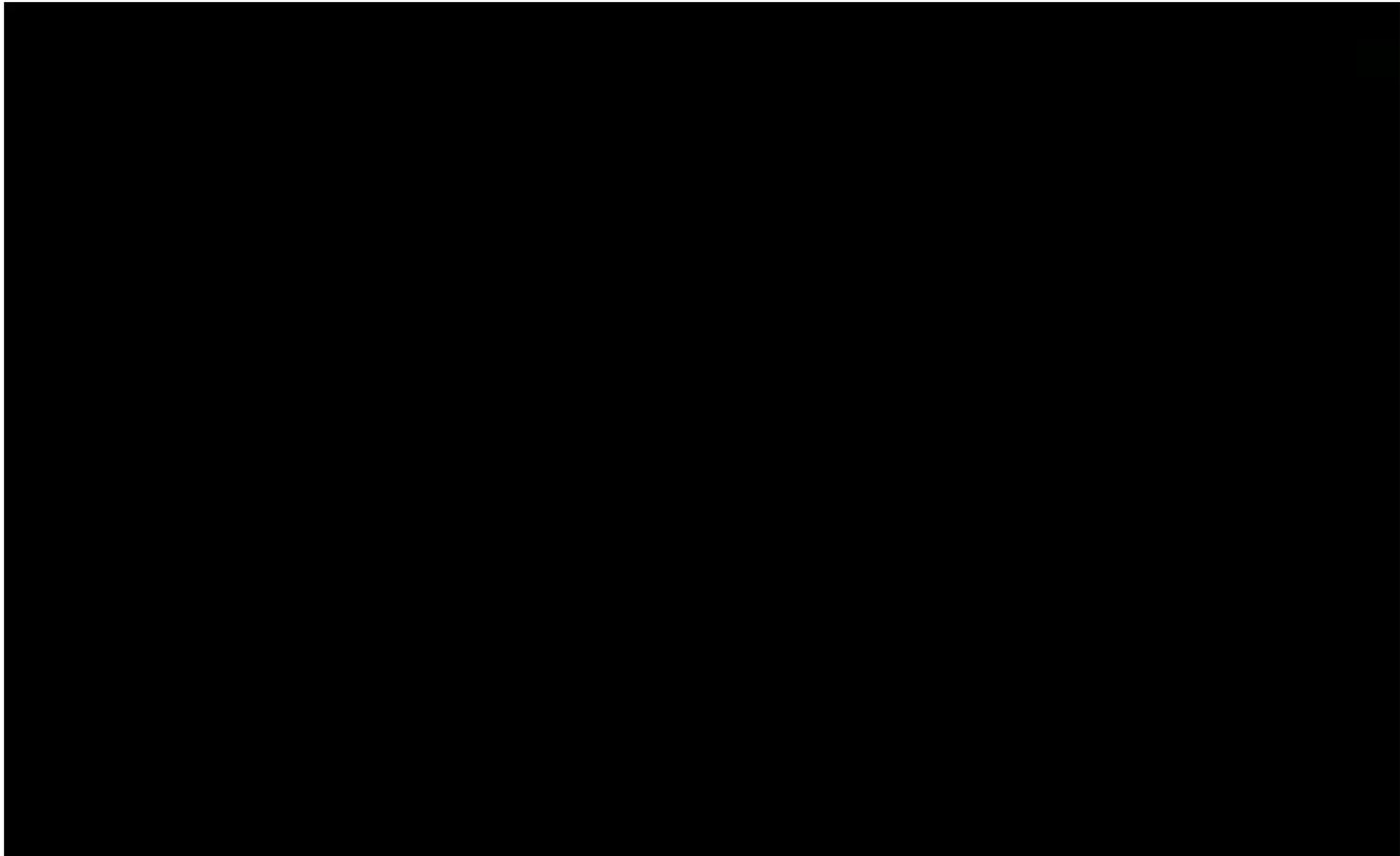


Fraud Prevention

MAIN TAKE-AWAY

“Awareness”

Fraud Prevention



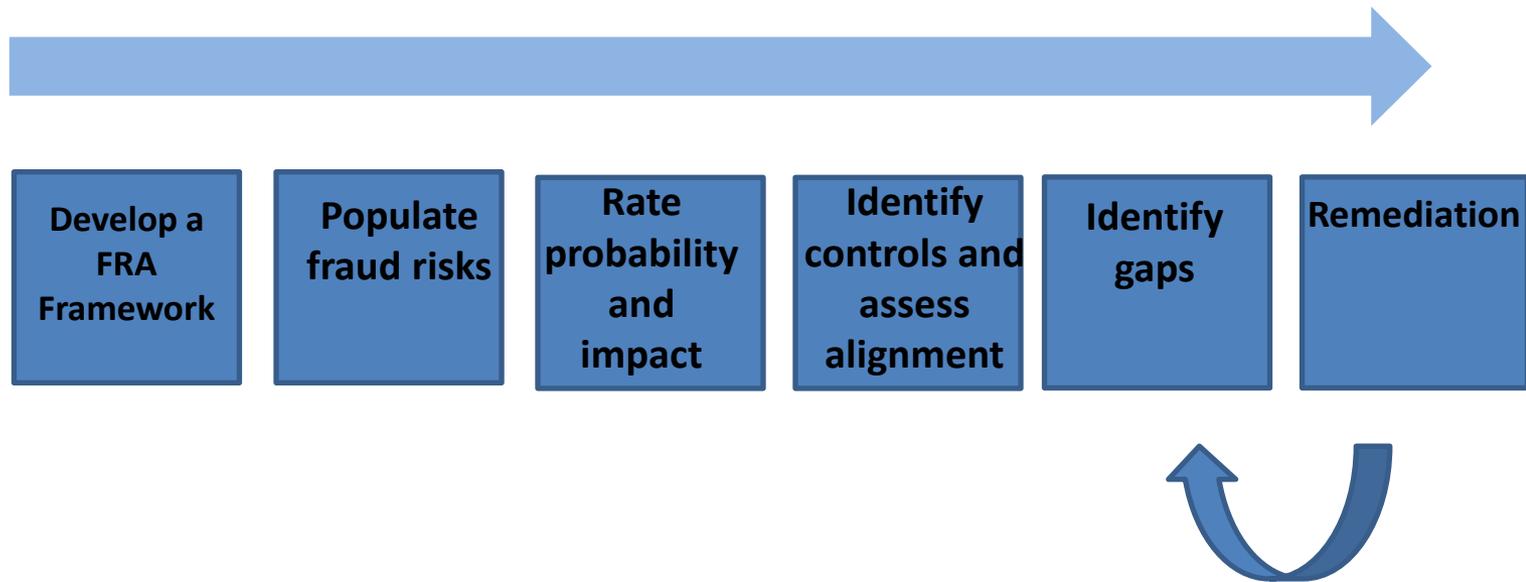
Fraud Prevention

Practices to Consider

- Adequate resources
- Robust hiring practices
- Periodic audits/reviews
- Conflicts of interest policies and practices
- Insist on adequate documentation
- Tone at the top
- Open door policy
- Culture of compliance and ethics
- On-going and required anti-fraud training
- Fraud reporting tool (hotline)
- Fraud risk assessments
- **Strong internal controls**



Fraud Risk Assessment



Fraud Risk Assessment

Identify the 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)

Fraud Risk Assessment

Measuring Fraud Risk

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

Fraud Risk Assessment

Factors to Measure Probability

- Controls or lack of
- Integrity of the organization
- Organizations are downsizing
- Budgets are decreasing
- Organizations are doing more with less
- Stressed and disaffected employees

Fraud Risk Assessment

Measuring Fraud Risk

Impact/Severity

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

- High
- Moderate
- Low

Fraud Risk Assessment

Other Measures to Consider

- Velocity/speed
- Frequency/persistence
- Direction of fraud risk



Fraud Risk Assessment

Fraud Risk Assessment
For period ending 12/31/XX
Last revised: XXXX/14
By:

LOW RISK
MEDIUM RISK
HIGH RISK

Refer to Risk Rating Guidance tab

Type of Fraud	Fraud Risk Number	Risk	Examples of Threat	Fraud Risk Measurement			Combined Inherent Risk Measurement Score	Overall Fraud Rating	Control(s) to Mitigate Inherent Risk	Control Support(w/p Reference(s))	Comments		
				Potential Impact (High - 3, Medium - 2, Low - 1)	Factors Considered to Determine Potential Impact Rating	Probability of Fraud Occurrence (High - 3, Medium - 2, Low - 1)						Factors Considered to Determine Probability of Fraud Occurrence Rating	
1) Fraudulent Financial Reporting (FFR)	1.1	Improper application of GAAP for corporations benefit	Secure credit based upon improper accounting (debt covenants); fixed asset disposals/useful lives (overstated); inventory valuation (over/understated); revenue recognition (overstatement); liabilities (understated)	3		3		6	HIGH RISK	Insert Control 1	Remediation: Observation #XXX; ICFR #X - w/p XXX	XXXX/14 - Pending response to Observation	
	1.2	Inappropriate top-sided entries	Manipulation of financial performance	2		1		3	MEDIUM RISK	Insert Control 2			
	1.2	Timing differences	Revenue recognition in incorrect period, known liabilities unrecorded at month/quarter end		1		1		2	LOW RISK	Insert Control 3		
	1.4	Improper accounting estimates or reserves	Manipulation of financial performance; under-estimation of contingent liabilities		3		3		6	HIGH RISK	Insert Control 4		
	1.5	Willfully miscalculating tax liabilities	Under-estimation of liabilities; fraudulent tax reporting		3		3		6	HIGH RISK	Insert Control 5		
	1.6	Incompetency of personnel; unethical personnel	Sign-off on reconciliations not reviewed; reconciliations tied up to gl balance without consideration of transactions/reconciling items; circumventing control activities; breach of duty		3		3		6	HIGH RISK	Insert Control 6		
2) Theft/Destruction of Data/Intellectual Property	2.1	Manipulation of data	Terminated or disgruntled employees gain access to systems in an effort to alter data to deceive	2		1		3	MEDIUM RISK				
	2.2	Deliberate discard/corruption of company records	Removal or destruction of information (emails containing incriminating information, defects, performance) in an effort to deter discovery of facts	3		3		6	HIGH RISK				
	2.3	Computer hacking	Unauthorized backdoor access to retrieve server/system data	3		3		6	HIGH RISK				
	2.4	Theft of proprietary/confidential information; use of company assets for personal gain/detriment	Sell of or handing over student/client listing to competitor; theft of patent/recipe (e.g. syllabus, perfume, product)	3		3		6	HIGH RISK				
	2.5	Trade secrets stolen	Obtain trade secrets for product launch, personal gain	3		3		6	HIGH RISK				
3) Defrauding Customers	3.1	Larceny	Sale of services with no intent to fulfill order	1		1		2	LOW RISK				
	3.2	Intentional sale of substandard products/services	Rush registration/orders to make registration quota/incentive bonus compromising education criteria/quality requirements	1		1		2	LOW RISK				
				1		1		2	LOW RISK				
				1		1		2	LOW RISK				
				1		1		2	LOW RISK				
4) Misappropriation of Assets	4.1	Embezzlement	Check kiting, forgery, falsifying settlement costs, skimming (theft prior to recording), larceny (theft after recorded), signature alteration on company checks for personal gain	1		1		2	LOW RISK				
	4.2	Vendor abuses	Invoice payment skimming, fictitious vendor billings	1		1		2	LOW RISK				
	4.3	Asset theft	Intentional short shipments with the product shortage stolen	1		1		2	LOW RISK				
	4.4	Separation of duties opportunities	Cross training of employees provides opportunities such as: Cash disbursement/Accounts receivable; Shipping/Receiving/Inventory Counts; ACH initiation/approval/performance of cash and/or bank reconciliations	1		1		2	LOW RISK				
	4.5	Fraudulent disbursements	Creation of fictitious vendors/invoices/payment made for personal gain	1		1		2	LOW RISK				
	4.6	Payroll fraud	Ghost employee in payroll master file; inflation of wages	1		1		2	LOW RISK				
5) Vendor Abuses	5.1	Vendor abuses	Bribery, related party collusion, extortion, kickbacks, preferential treatment, bid rigging	1		1		2	LOW RISK				
	5.2	Related party transactions	Transactions are not at "Arms-length"	1		1		2	LOW RISK				

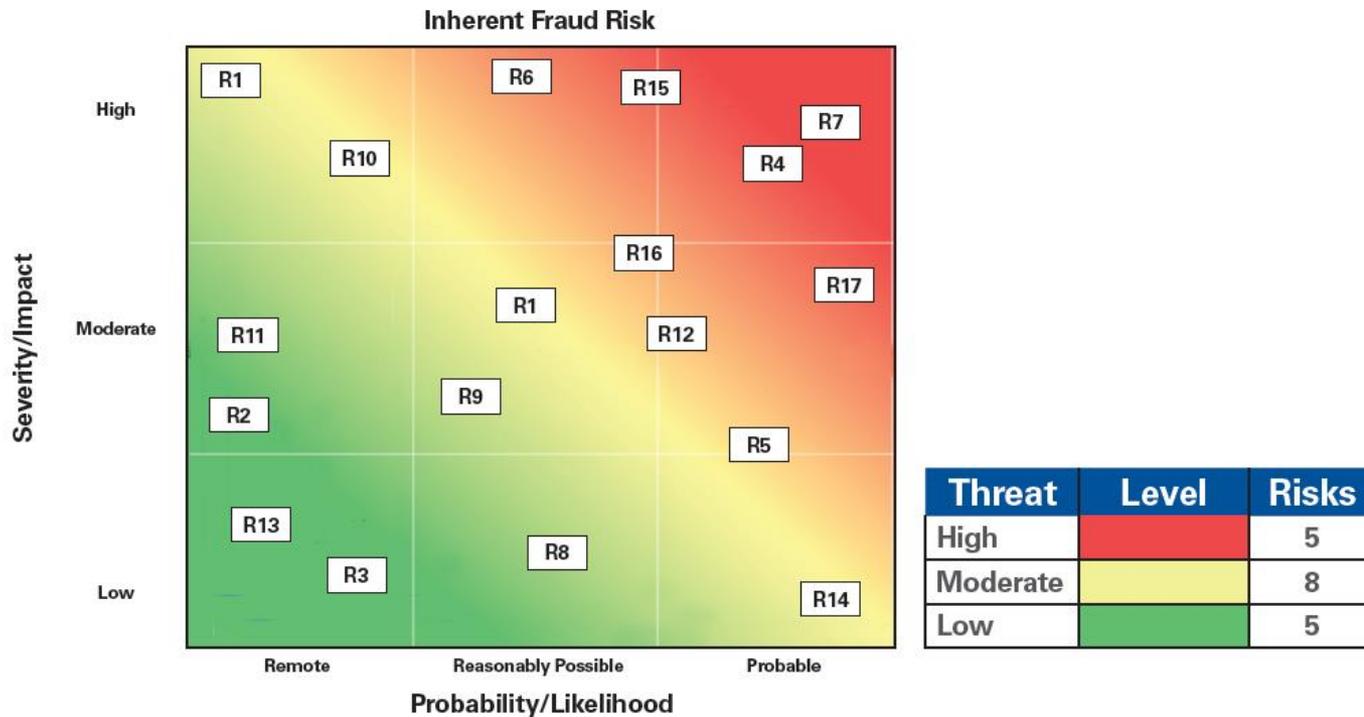
Fraud Risk Assessment

Type of Fraud	Fraud Risk Number	Risk	Examples of Threat	Potential Impact (High - 3, Medium - 2, Low - 1)	Factors Considered to Determine Potential Impact Rating	Probability of Fraud Occurrence (High - 3, Medium - 2, Low - 1)	Factors Considered to Determine Probability of Fraud Occurrence Rating	Combined Inherent Risk Measurement Score	Overall Fraud Rating	Control(s) to Mitigate Inherent Risk	Control Support/w/p Reference(s)	Comments
5) Corruption	5.3	Economic extortion	Sell of or handing over client/student listing to competitor, theft of patent/recipe (syllabus, perfume, product)	1		1		2	LOW RISK			
	5.4	Conflict of interest	Procure product or services from an officer of the company's relative at a higher cost	1		1		2	LOW RISK			
				1		1		2	LOW RISK			
				1		1		2	LOW RISK			
6) Compliance	6.1	Labor/HR	Under the table wages	1		1		2	LOW RISK			
	6.2	Occupational/Safety, environment	Falsification of data in order to conceal defect	1		1		2	LOW RISK			
	6.3	Regulatory	Changing data to comply with program requirements in order to gain incentive, compensation and/or accreditation	1		1		2	LOW RISK			
	6.4	Deliberate discard of company records to deter discovery of information; Contempt	Records removed or destroyed to deter discovery of evidential matter (defects, performance)	1		1		2	LOW RISK			
				1		1		2	LOW RISK			

Fraud Risk Assessment

DELIVERABLES - SIMPLIFIED HEAT MAP

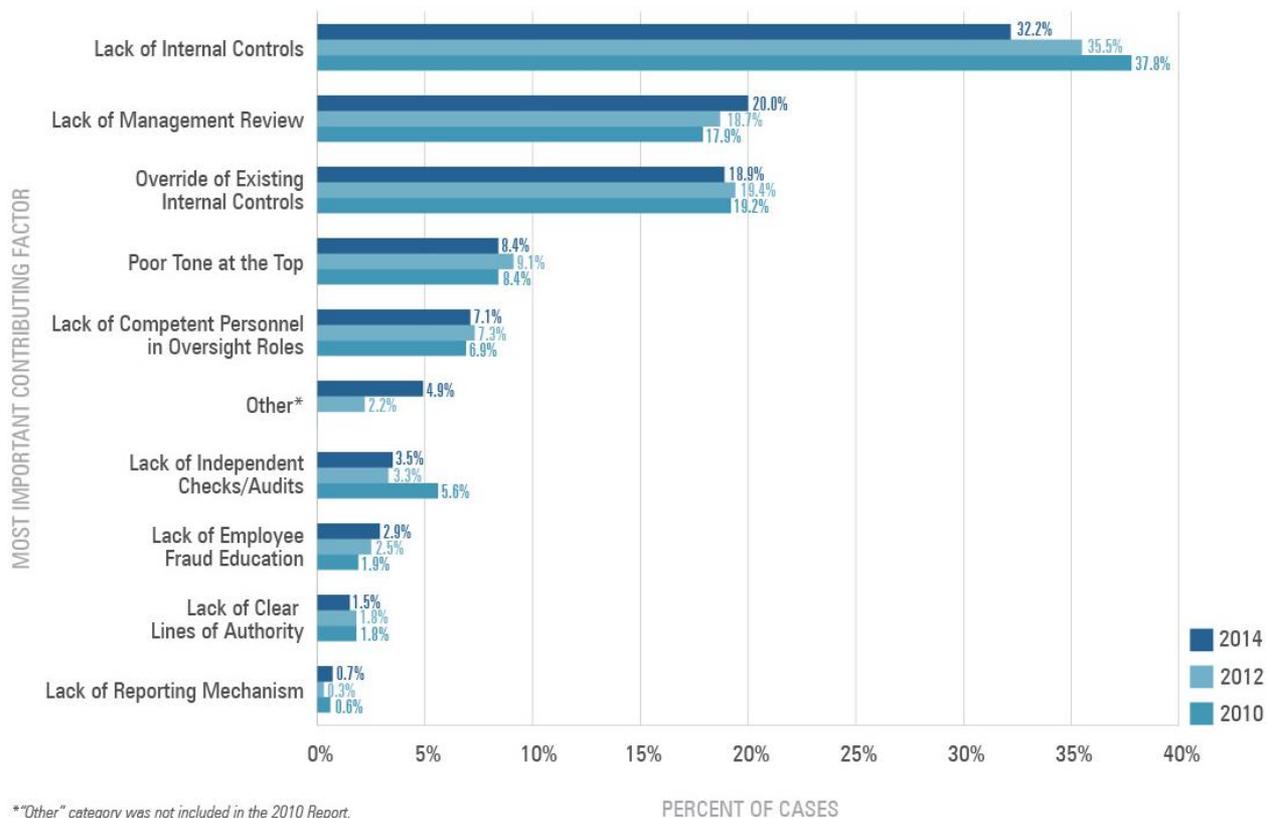
Fraud Risk Assessment Heat Map



R1-R18 are representative of risk factors identified in the Enterprise-wide Risk Assessment. Each Factor would be supported by a detailed description of the respective risk factor.

Internal Controls

Figure 39: Primary Internal Control Weakness Observed by CFE



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

Internal Controls

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

Types of Controls

- **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
- **Competence** – Aptitude to recognize when something is not right

Internal Controls

Preventive Controls

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

Internal Controls

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

Detective Controls (Cont.)

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



Internal Controls

Persuasive Controls

- Formal code of ethics/conduct
- Whistleblower hotline
- 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

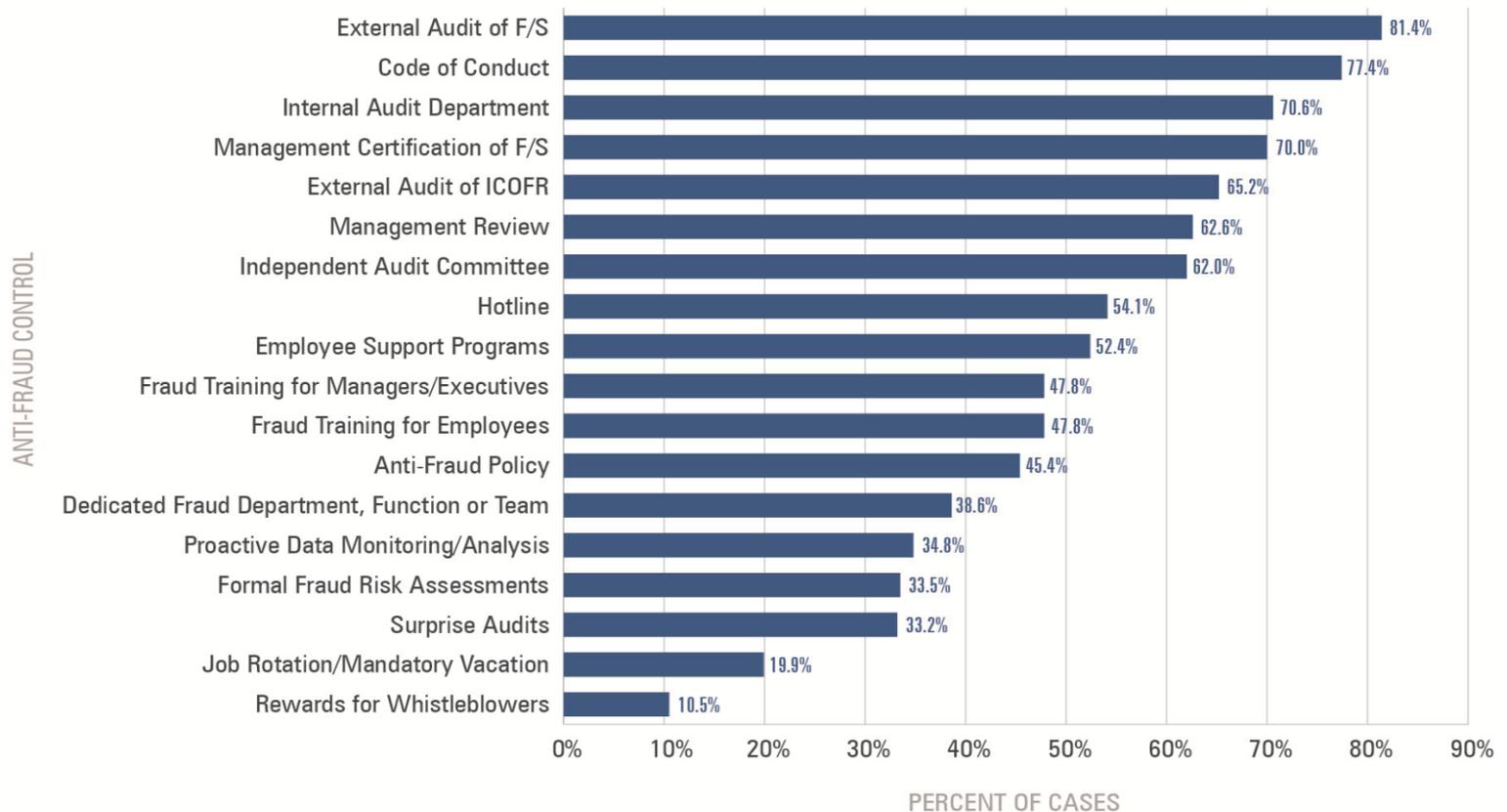
Internal Controls

Competence

- Possesses required skill, knowledge, qualification, and/or capacity
- Requires knowledge of expected outcomes and incentives to report
- Is empowered to report concerns
- Effectively performs the duties of ones positon
- Has an awareness of the duties of those around them

Internal Controls

Figure 26: Frequency of Anti-Fraud Controls



DOJ Whistleblower Programs

False Claims Act (nicknamed the “Lincoln Law”)

- From 1986 to 2014, the United States government recovered \$44 billion under the False Claims Act. More than two-thirds of this, about \$30.3 billion, was recovered in cases filed by whistleblowers under the qui tam provisions of the False Claims Act.
- Whistleblowers have received over \$4.7 billion under the False Claims Act. In 2014 alone, whistleblowers helped recover approximately \$3 billion and were awarded over \$435 million.

Resources

Ohio Auditor of State

<https://ohioauditor.gov/fraud.html>

1-866-Fraud-OH (1-866-372-8364)

U.S. Government Accountability Office (GAO)

<http://www.gao.gov/fraudnet/fraudnet.htm>

1-800-424-5454

The Association of Government Accountants (AGA) - Fraud Prevention Toolkit

<https://www.agacgfm.org/Resources/Tools-To/Prevent-Fraud.aspx>

Resources

Association of Certified Fraud Examiners (ACFE) - Report to the Nations on Occupational Fraud and Abuse – 2014 Global Study

<https://www.acfe.com/rtnn.aspx>

AICPA Fraud Resource Center

<http://www.aicpa.org/INTERESTAREAS/FORENSICANDVALUATION/RESOURCES/>

The Institute of Internal Auditors

<https://na.theiia.org/training/Pages/Fraud-Courses.aspx>

Frank W. Abagnale

<http://www.abagnale.com/company.htm>



As one of the largest certified public accounting and business advisory firms in the region, Schneider Downs serves clients throughout the country and around the world. By integrating high-quality resources, systems and personnel, Schneider Downs has built a reputation of delivering individualized services built on insight, innovation, and experience to meet each client's specific needs.

For more information, visit us at www.schneiderdowns.com

We Are Committed to Your Success
Schneider Downs