

**Guam
Professional
Development
Conference**

**“Trends, Tools,
and Techniques
in Today’s
Financial
Environment”**

**September 17 to
19, 2014**

**Hotel Nikko
Guam**

Government Fraud Risk



Lealan Miller, CGFM, CPA

Speakers retain the copyright for all of the following materials. Any replication without written consent is unlawful. Comments and opinions expressed by the speaker do not reflect the positions, opinions or beliefs of the AGA and should not be construed or interpreted as such. The materials contained in this presentation should not be considered to be in the public domain. Speeches and presentation materials here are proprietary works copyright by the individual or entity who presented the materials at the conference. All rights are reserved. The authorized use of materials on this page is limited personal reference by authorized users of the conference materials. Reproduction, redistribution, reuse, reposting or resale by any party in any form, format or media, without the express permission is strictly prohibited.



FRAUD RISKS

GOVERNMENT UNDER SIEGE

Presented by:

Lealan Miller, CPA, CGFM



CPAs & BUSINESS ADVISORS

Specialization

What is Forensics?



What is Forensic Accounting?

“CSI” Television Show

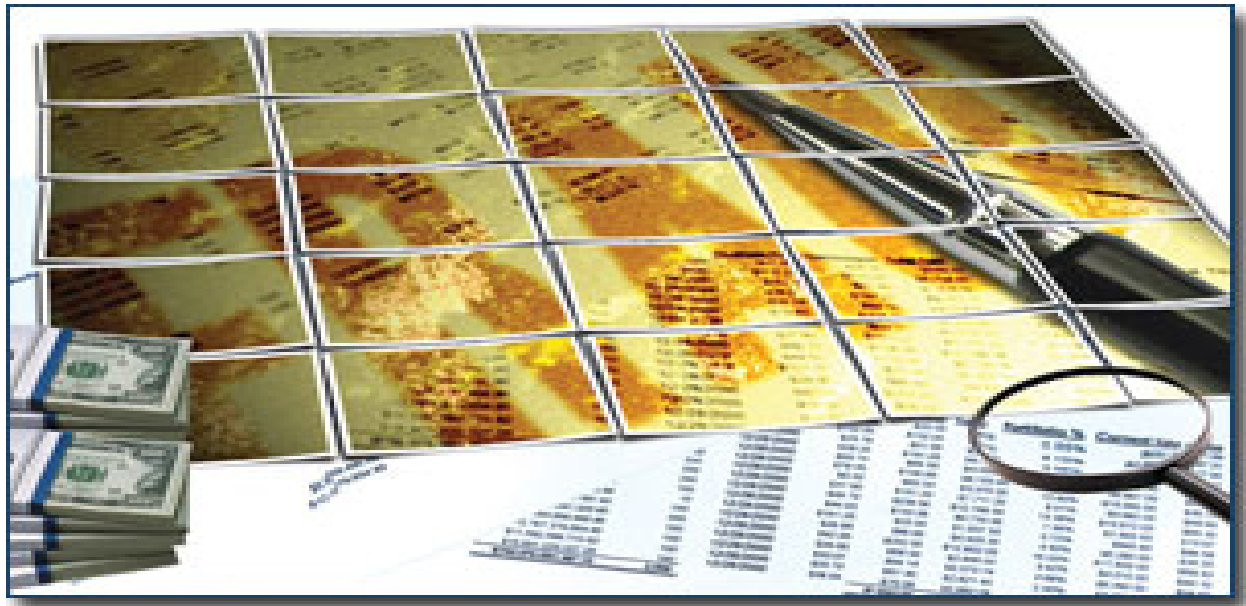


What does it look like?



Agenda

- **Impact of Fraud – The Big Picture**
- **Fraudster Profiles**
- **Trends – What's Hot**
- **Fraud Prevention**
- **What's in it for you!**



What will you do?



When this happens...*ON YOUR WATCH?*

EFFECTS OF FRAUD

Impact of Fraudulent Activity



Fraud Survey

What is your “acceptable” fraud loss?



Medicaid Program \$1.4 Billion

What is your “acceptable” fraud loss?

10%

\$140,000,000

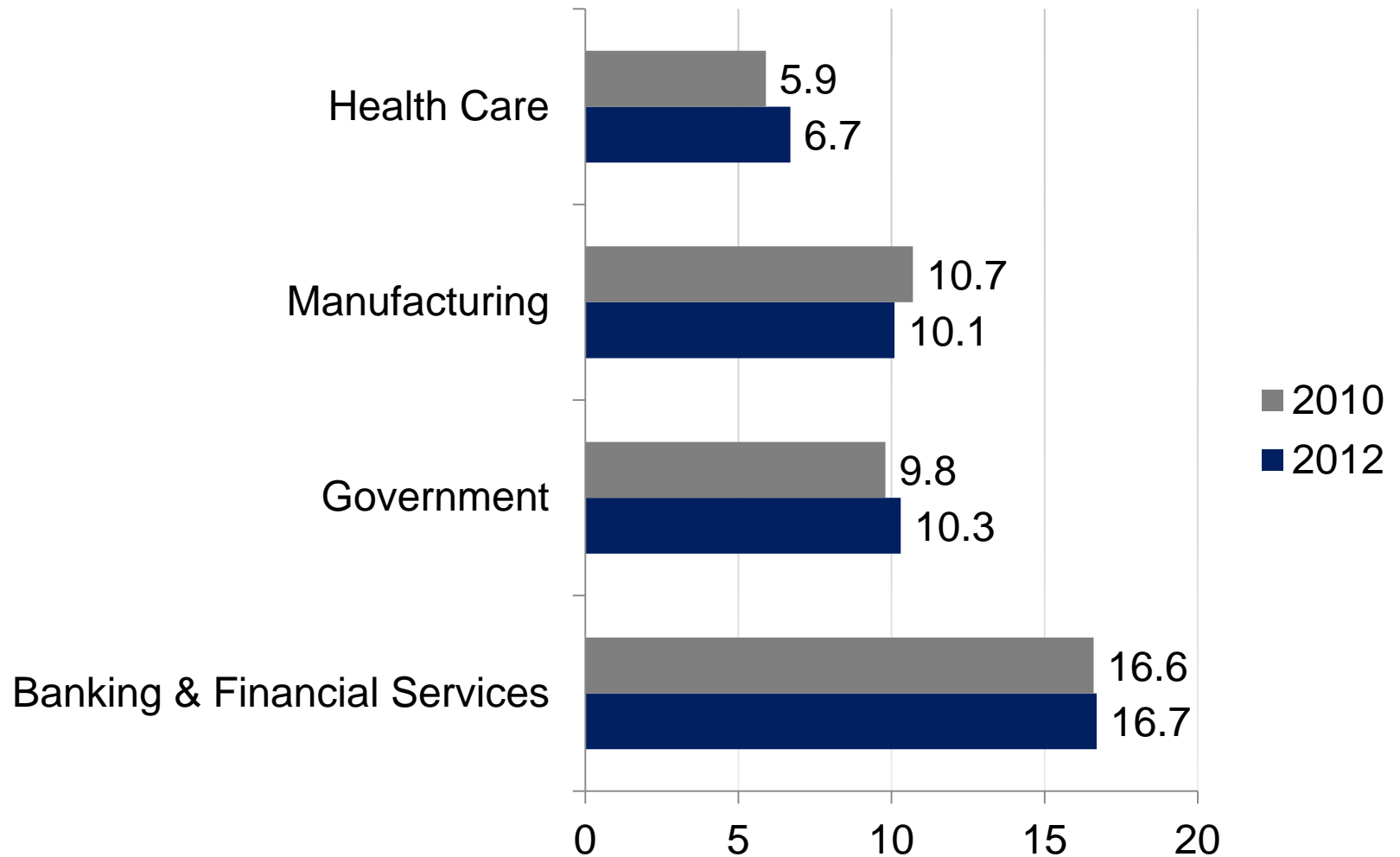
Fraud Survey – Government

- Estimated 3/4 of organizations fall victims of fraud
- Government rates #2 on “Top Ten List”
- 18-24 months before detection
- 5% of total revenue
- < 1,000 people – median loss \$100,000



\$994 billion US annual fraud loss
\$2.9 trillion annual fraud loss globally

Victim Organizations – by Industry



RAISING SUSPICIONS

Recognizing the Signs of Fraud



Foundations for Internal Fraud

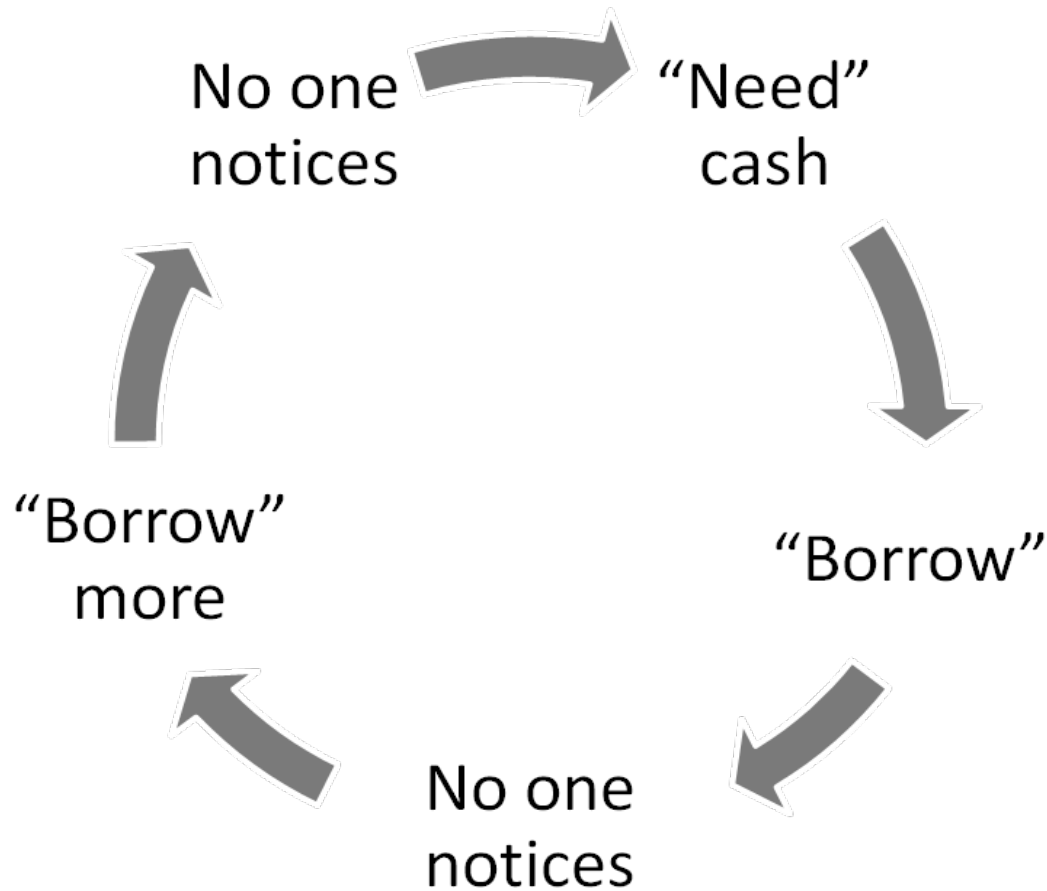
- **Employee Traits**

- Financial pressure
- Exploitable opportunity
- Rationalization available

- **Most Common Perpetrator Traits**

- Most “trusted” employee
- Star performer
- Long term employee

How People “Cross the Line”



Red Flags – Financial

- Cash Flow Problems
- Records not produced upon demand
- Source Documents lost
- Problems with Financial statements
- Unexplained lack of profit



Red Flags - Employee

- Employee does NOT miss work
- Family Issues
- Drugs/Alcohol/Gambling
- Living Beyond Means



TYPICAL FRAUDS

Top Fraud Schemes

Is it just the money?

Do you need to be concerned?

Embezzlement \$810,000

Bookkeeper forgery & bank fraud!

Embezzlement – check kiting – tax evasion

- Unauthorized withdrawals & transfer of funds
- Credit cards/credit accounts false bank representation
- Failed to report illegal income on tax returns



Government Fraud Trends

- **Corruption Schemes**
 - Use of influence for personal benefit
- **Billing Schemes**
 - Payments of inflated or fictitious invoices
- **Expense Reimbursements**
 - Reimbursement for inflated/fictitious expenses

Expense Report – Busted!



What will you do?

Fraud Detection:

Learn how fraudsters conceal their schemes

Focus on known methods first



Internal Control Weaknesses

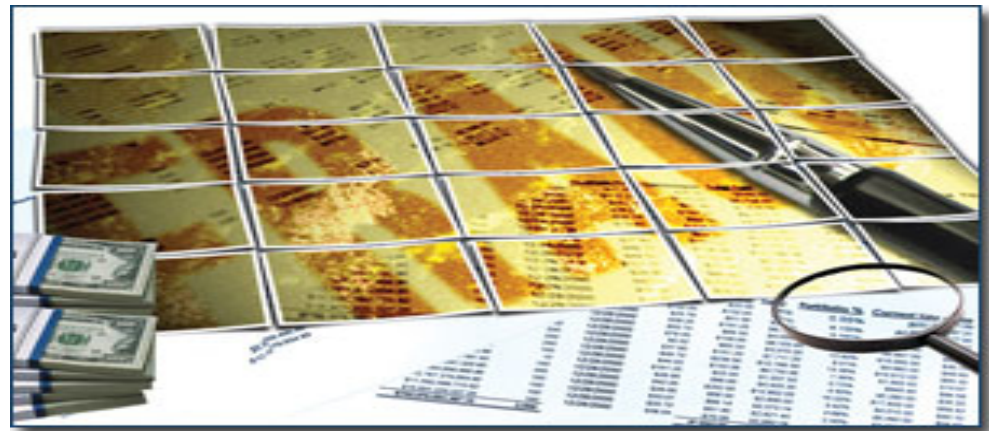
Accounts Receivable - Example:

- Key supervisor makes daily bank deposit
- Most likely to succeed in fraud



Major Internal Control Weaknesses

- **Key employees do too much**
Access to and control all revenue
- **Managers do not monitor their work**
Employees operate in secret while in plain sight of everyone
- Why?.....



Trust but Verify Concept

Managers use “blind trust”

- Tell employees what to do

- Expect them to do it

- Never monitor actions to see if expectations are met

Managers should use “trust but verify”

- Monitor employee actions

- Chinese saying: “It’s OK to trust employees, just always keep one eye open!”

Employee Types

- Two types of employees:
 - **Doers** - most internal controls exist here
 - **Reviewers** - few or no controls
 - Managers monitor supervisors differently
 - Not reviewed like subordinates
- Fraudsters ignore/compromise internal controls
- Fraudsters do not play by the rules

Crossing the Line – Honest to Dishonest

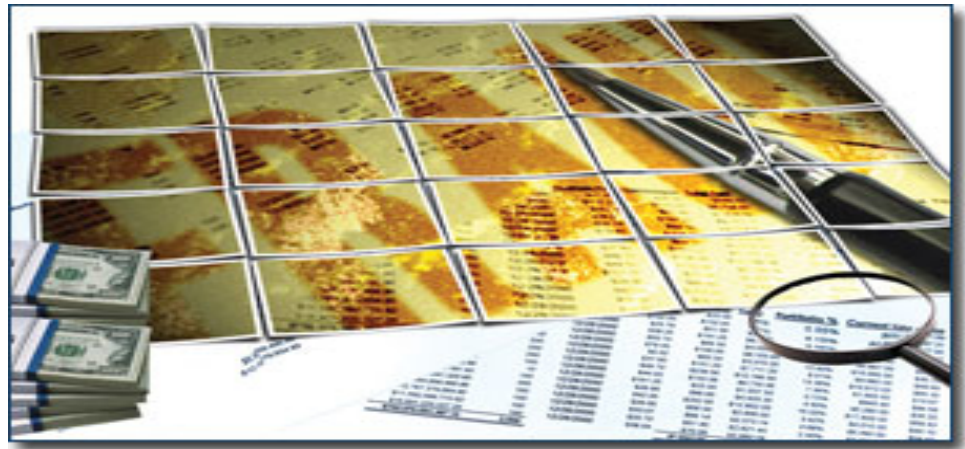
- What happens when – manager does not monitor supervisor, and the supervisor makes the daily bank deposit?

Key employee often crosses line to become dishonest

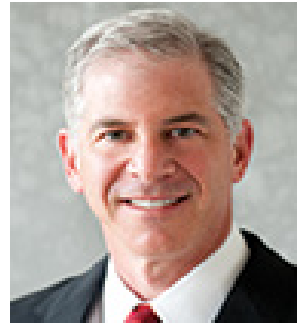
Key employee manipulates deposit detail

Key employee defrauds employer by misappropriating

- **Result is fraud!**



What's Legal vs. What's Right



Andrew Fastow – Former Enron CFO insights

Just because it's legal, does that make it right?

Approvals – Management/Accountants/Attorneys

There is a line – legal vs. intent of what's right

Filter used – “Am I following the rules?”

Filter not used – “Is this the purpose of the rules?”

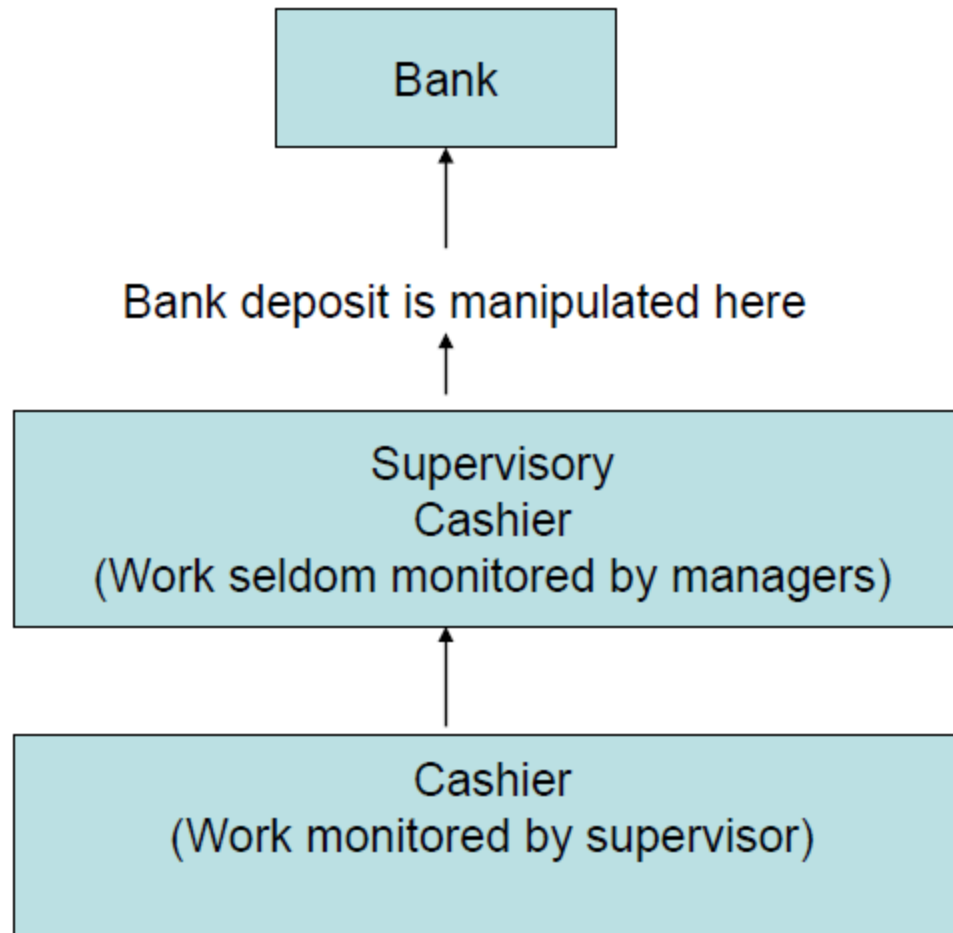


Internal Control Risks

- Expect doers to follow rules
- Expect supervisors to monitor work of doers
- Supervisor makes bank deposit
- We think we are done.....wrong assumption!



Bank Deposit Process



“At Risk” Employees

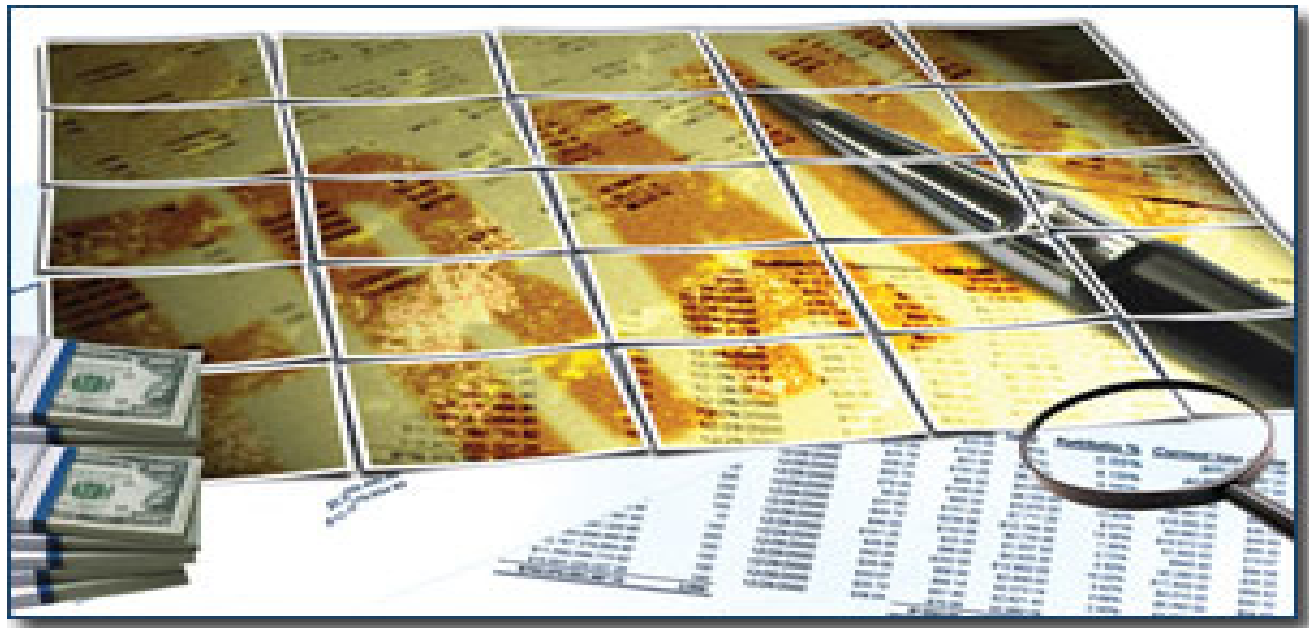
- Work Habits of “At-Risk” Employees - who do you know?
 - Arrives early to work and leaves late
 - Works nights & weekends
 - Does not take vacations or sick leave
 - Reports to office during brief absences
 - Asks others to “hold work” while away from office



Identifying “At Risk” Employees

Work Habits of “At-Risk” Employees – conclusion:

Key Issue - **control of work environment**



“At Risk” Use of PC’s

- Personal computers used for accounting purposes
Small organizations use PC’s
No internal controls – no audit trail
- Resulting fraud – missing or destroyed documents



“Off-Book” Accounts Receivables

- A/R collection of funds from current account balances
 - Delinquent A/R sent to collection agency – limited staff
 - Delinquent A/R not recorded in accounting system
 - Delinquent A/R not reported on financial statements
- Resulting fraud – revenue from delinquent A/R is prime target
 - Lack of monitoring by managers

Segregation of Employee Duties

- Three person operation – **ideal controls**
 - Billing & posting
 - Collecting & depositing
 - Independent supervisor reconciles accounting information
- Independent Reconciliations
 - Paid accounts marked “paid” – amount of bank deposit
 - Payment reconciliation of records vs. money
- Fraud quickly detected – unless review is performed out of sequence

Segregation of Employee Duties

- Two person operation – **some controls**
 - Billing & posting
 - Collecting & depositing
- Independent reconciliations – who should reconcile and why?
 - Billing & posting
 - Generally no access to money
 - Lower risk** - will generally report differences
 - Collecting & depositing
 - Higher risk** - will not self-report differences

Segregation of Employee Duties

- One person operation – **no controls**
- One person does everything
- Independent monitoring is required
 - Manager
 - Board member or governing body
 - Outside volunteer

Segregation of Employee Duties

- **Danger** of employee duties:
- **Internal controls “self-destruct” at lunch & breaks –**
Record keepers become relief cashiers



Secrets of Detection

- Study internal controls system -
 - Focus on employees who perform too many tasks
 - Determine if managers monitor their work
- If PC'S are used for accounting -
 - Compare manual & computer accounting records for agreement
 - Confirm transactions with customers
 - Obtain copies of checks & review endorsements
 - Subpoena employee's personal bank records

Secrets of Detection

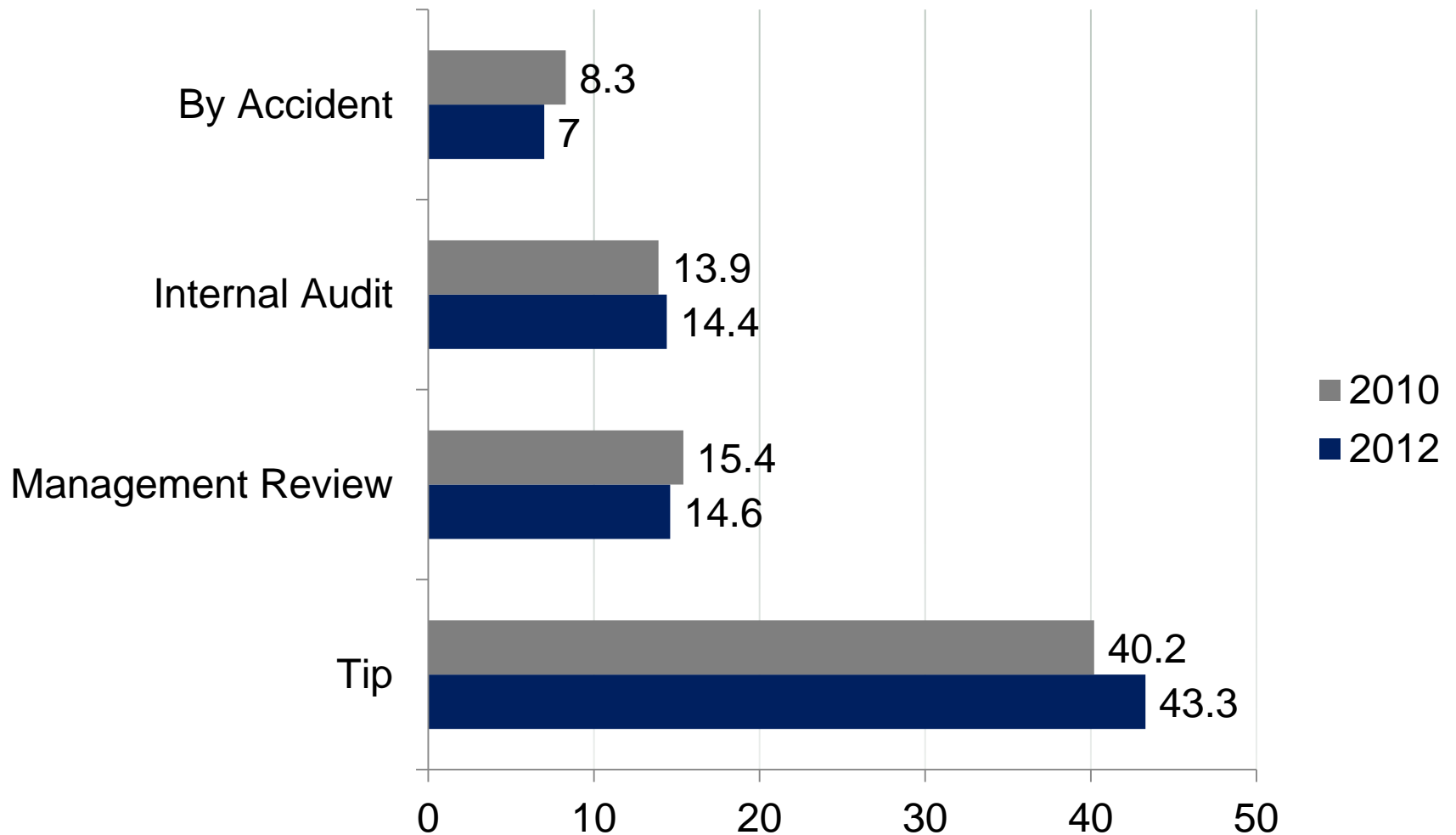
- Additional review steps include -
 - Observe employee changes in behavior/attitude
 - Observe employees with access/control & make deposits
 - Observe & listen others to identify “at risk” employees
 - Inquire about who performs relief cashier duties
 - Determine if employees are required to take vacations & cross-train employees by switching duties
 - Verify if there is a “last look” policy to analyze daily bank deposit contents after being prepared/before actual deposit
 - Search for “off-book” accounts receivables

Fraud Prevention

Prevention
is easier than
Detection



Detection of Fraud Schemes



Fraud Prevention

- *Basic principle:*
 - People rarely commit fraud if they think they will be caught
- *Perception of detection:*
 - Most effective deterrent to fraud



Increase Perception of Detection

- ***“Tone at the Top”***
 - Managers need to communicate the idea that they are serious about their fraud detection and prevention efforts
- ***Employee Education***
 - Internal controls for monitoring employees
 - Company fraud (ethics) policy



Effective System of Internal Control

Segregation of duties:

- Authorization
- Record keeping
- Custody of assets



Physical control over assets and records

- Secured check stocks
- Controlled access to inventory

The Do's of Internal Controls

- Top level Reviews of Actual Performance
- Reviews by Management at the Functional or Activity Level
- **Management of Human Capital**
- Controls Over Information Processing
- **Physical Control over Vulnerable Assets**
- **Establishment and review of Performance Measures and Indicators**

The Do's of Internal Controls

- Segregation of Duties
- Proper Execution of Transactions and Events
- **Accurate and Timely Recording of Transactions and Events**
- Access Restrictions to and Accountability for Resources and Records
- Appropriate Documentation of Transactions and Internal Control

The Do's of Internal Controls

- **Change computer passwords**
- **Periodic analysis**
- **Require vacations**
- **Cross train employees**
- **Budget vs. actual review**

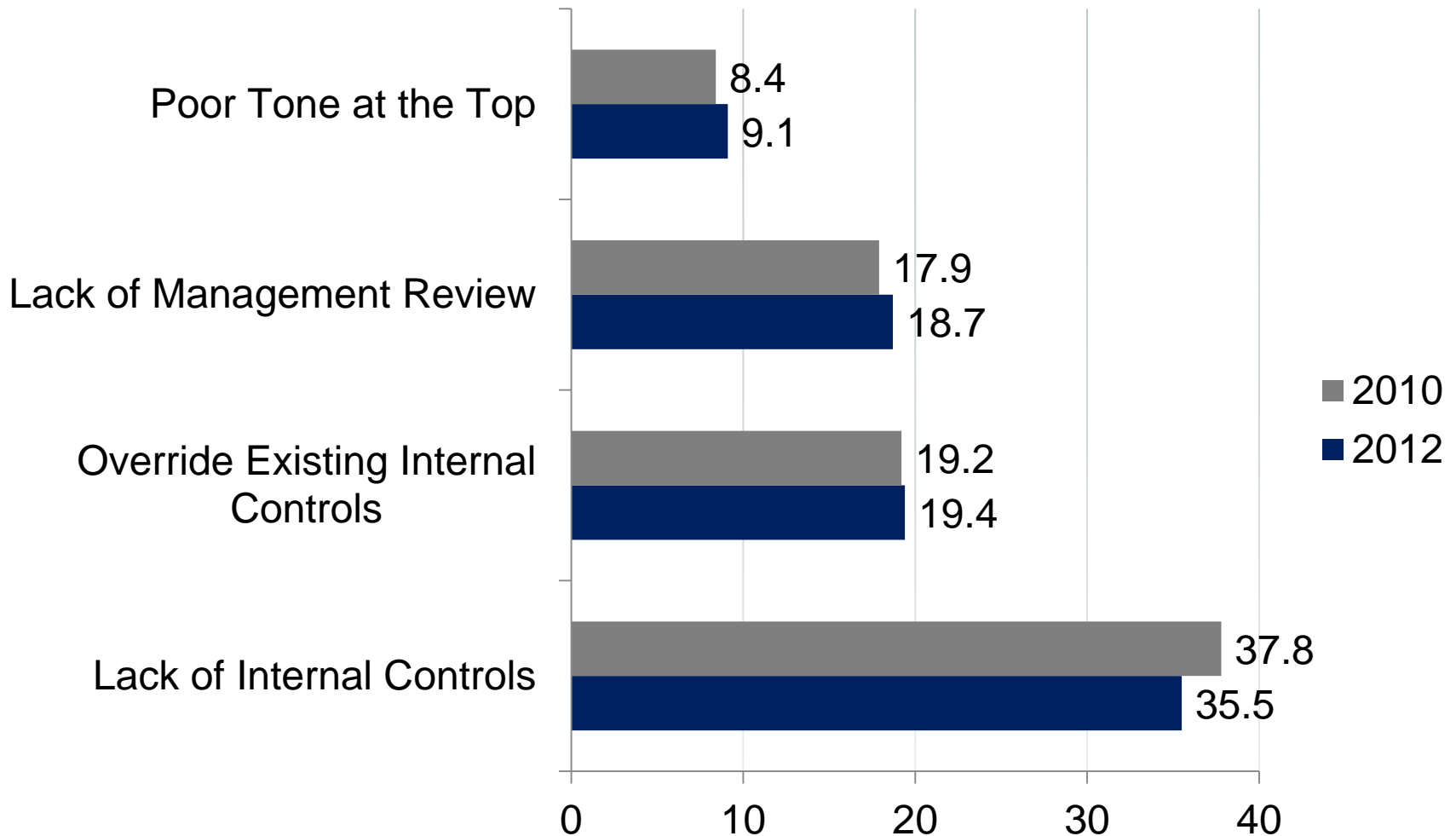


Don'ts

- Subordinates approve boss' travel or expense reimbursements
- Too many controls
- Inversely – not enough controls
- No reconciliations
- Too much trust in one person



Primary Internal Control Weaknesses



Effective System of Internal Control

- **Independent checks** on performance
 - Review & follow-up of financial performance indicators
 - Documentation of follow-up and resolution of issues
- **Reporting program** (hotline, open-door policy)
 - How is program communicated to staff?
- **Vigorously pursue** dishonest acts



The Future of Fraud



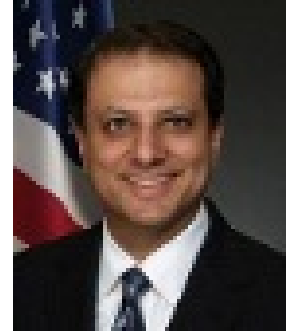
"I'm encouraging him to stay in school and go into white-collar crime."

What will you do?



When this happens...*ON YOUR WATCH?*

Recommendations



Preet Bharara - US Attorney Southern District New York

“The Street Fighter” – Prosecution of financial fraudsters

Today’s Fraud Culture – Do the **“minimum”**

“Minimum” leads to Internal Control breakdown – looking other way

Result is increase in fraud & embezzlement

Change requires commitment to do your best

Reward those who step forward when they see bad things



You can make a difference

Choose to do right

Do your best

“Platinum” rule



Question 6

6. Which of the following may be a sign that an organization is being victimized by a falsified hours scheme?
- a) Several employees appear on the personnel employee roster but are not on the most recent payroll check list.
 - b) The payroll expenses for the company unexpectedly exceed budgeted projections and prior years' totals.
 - c) One employee consistently submits more requests for expense reimbursements than all other employees within the department.
 - d) The FICA tax withheld on several employees' paychecks does not equal 7.65% of the employees' gross pay.

Question 3

3. Which of the following is considered a fraud preventive internal control?

- a) Employee support programs
- b) Segregation of duties
- c) Employee background checks
- d) All of the above

Question 4

4. The concept of the fraud triangle states that, for a fraud to occur, three factors generally are present. Which of the following is NOT one of the three sides of the fraud triangle?

- a) Criminal predisposition
- b) Incentive or pressure
- c) Perceived opportunity
- d) Rationalization

Question 5

5. In general, the best way to prevent fraud is to:
- a) Implement harsh penalties for perpetrators
 - b) Outsource all possible functions
 - c) Increase the perception of detection
 - d) Conduct covert audits

Question 7

7. Which of the following is NOT an element generally included as part of a fraud risk assessment?

- a) Risk identification
- b) Formal fraud policy development
- c) Assessment of likelihood and significance of risks
- d) Risk response

Question 8

8. The three primary categories of occupational fraud are:
- a) Corruption, financial statement fraud and asset misappropriation
 - b) Skimming, money laundering and bid rigging
 - c) Asset misappropriation, identity theft and fictitious revenues
 - d) Financial statement fraud, inventory theft and cash larceny

Question 10

10. Most employees who commit fraud have a history of fraudulent misconduct.

- a) True
- b) False

Part 5 – Question 1

1. In terms of preventing fraud, which of the following components of the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control – Integrated Framework* most adequately embodies an organization's tone at the top?
- a) Control activities
 - b) Monitoring
 - c) Control environment
 - d) Information and communication

Question 3

3. Which of the following internal controls would likely be most effective in helping to prevent fraud?

- a) Hidden surveillance
- b) Secret cash counts
- c) Covert email monitoring
- d) Fake surveillance cameras

Question 5

5. According to the U.S. Department of Justice, which of the following is considered an element necessary to monitor compliance with the antibribery provisions of the Foreign Corrupt Practices Act (FCPA)?

- a) A formal risk assessment
- b) An antibribery policy
- c) Employee anticorruption training
- d) All of the above

Question 7

7. An effective hotline serves as:

- a) A fraud detection control
- b) A fraud prevention control
- c) Both a fraud detection and prevention control

Question 8

8. Which of the following is true regarding employee antifraud training?

- a) Employees at all levels of the organization should receive identical antifraud training.
- b) The training should be catered to the specifics of the organization.
- c) Training all employees at the time of hire is sufficient.
- d) All of the above.

Question 10

10. Which of the following is NOT true regarding ethics policies?

- a. If an organization doesn't truly value integrity, its ethics policy might do more harm than good.
- b. A thorough, well-designed ethics policy is a surefire way to prevent fraud.
- c. An ethics policy should address the specific risks of employee misconduct that were identified in the organization's risk assessment process.

Questions & Comments?

Lealan Miller

208.383.4756

lmiller@eidebailly.com



Thank you to our platinum sponsors



Deloitte.

