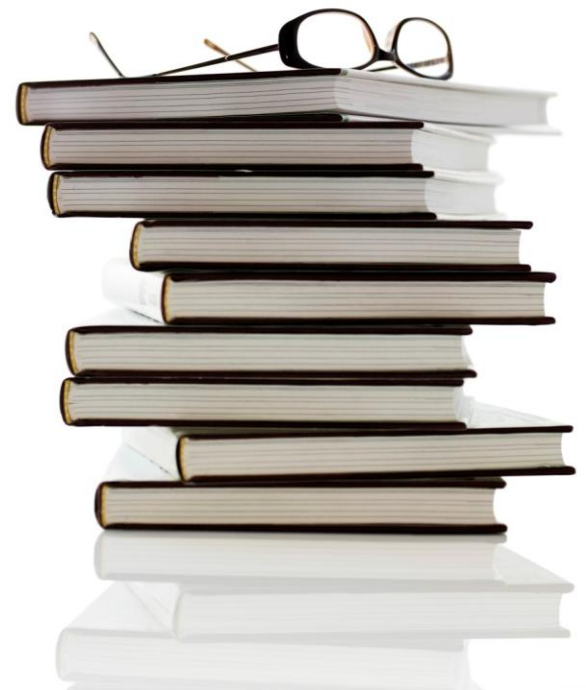




# Developing a Fraud Risk Management Program for Your Organization

**Craig Hirsch**  
**Manager**  
**Deloitte Financial Advisory Services LLP**

**March 18, 2011**



This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte Financial Advisory Services LLP, a subsidiary of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

# Agenda

Making the case for a fraud risk management program

A COSO-consistent approach to fraud risk management:

- Control environment
- Fraud risk assessment
- Anti-Fraud control activities
- Information and communication
- Monitoring

Integrated Case Studies

# Making the Case for a Fraud Risk Management Program

# ACFE Fraud Statistics

- Losses **estimated** to be 5 percent of revenue
- \$160,000 median value per case reported to ACFE
- **18-month median duration**
- Highest impact to small businesses
- **Higher positions = higher loss**

Source: Association of Certified Fraud Examiners 2010 Report to the Nations on Occupational Fraud and Abuse. [www.acfe.com](http://www.acfe.com)

# Perpetrator's Position Drives Scale of Loss



Source: Association of Certified Fraud Examiners 2010 Report to the Nations on Occupational Fraud and Abuse. [www.acfe.com](http://www.acfe.com). Copyright 2010, ACFE. Used with permission.

# IIA's Audit Executive Center Survey Results

- Emerging Trends in Fraud Risks, January 2010
- Increase of fraud occurrences since the onset of the economic crisis in 2008
- **Employee-related fraud has had a major impact in organizations**
- **Internal auditing can add value to fraud risk management efforts**
- **Programs to manage fraud risk are becoming a higher priority**

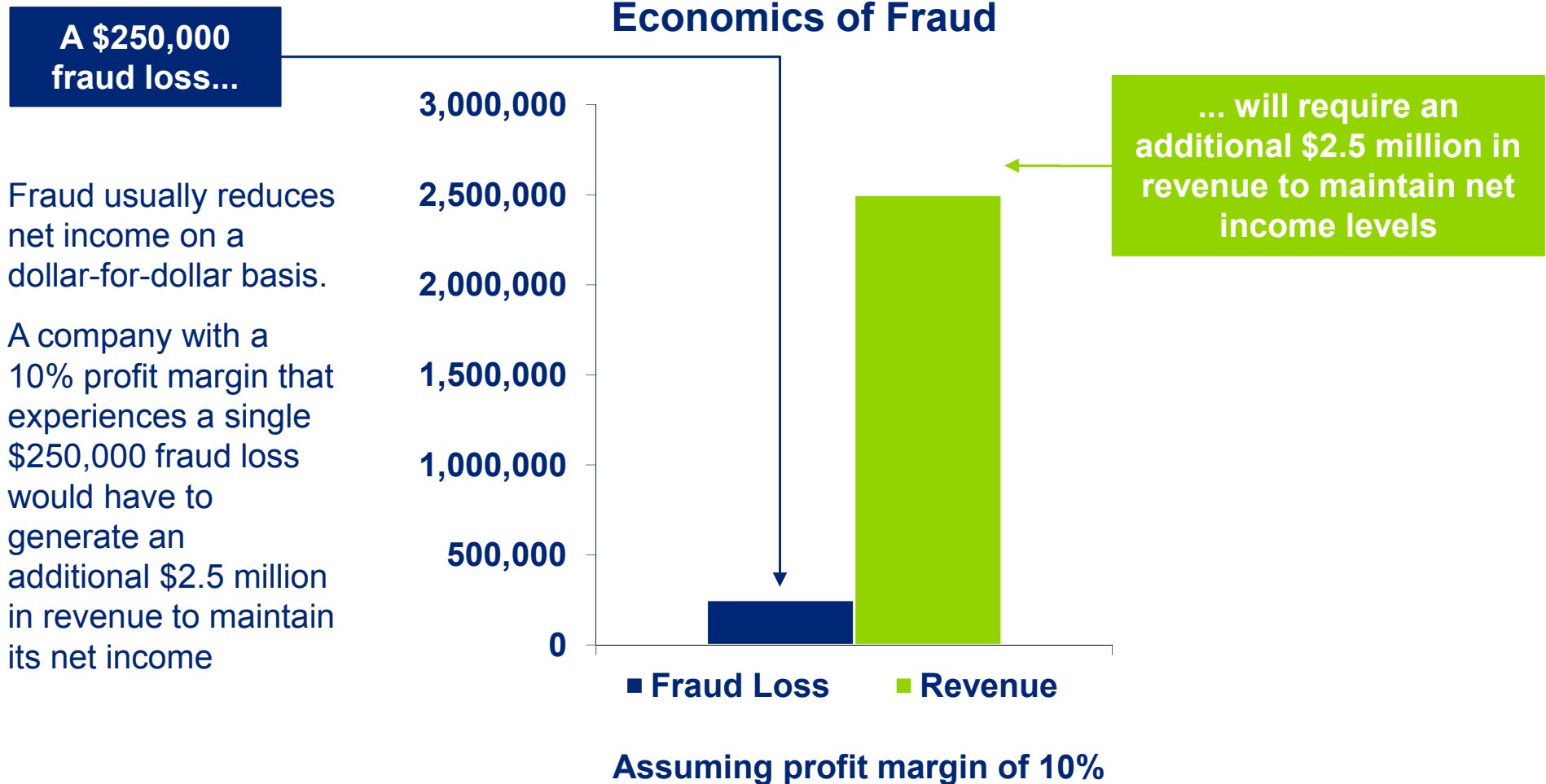
Source: Knowledge Alert Emerging Trends in Fraud Risks, January 2010

# Impacts of Fraud — Examples

- **Raises questions about management's 302 and 404 certifications**
- Causes direct financial impact (e.g., cost of investigations, losses from asset misappropriation, civil lawsuits)
- **Negative public relations (e.g., reputation, brand)**
- Decline in share price
- Decrease in corporate governance ratings
- **Ability to recruit/retain top quality talent**

# Impact of Fraud

## Recovering Net Income After a Fraud Loss



# COSO — An Overview

## The Committee of Sponsoring Organizations of the Treadway Commission (“COSO”)

- Formed specifically to study the causal factors that can lead to fraud

## In 1992, COSO issued the Internal Control — Integrated Framework

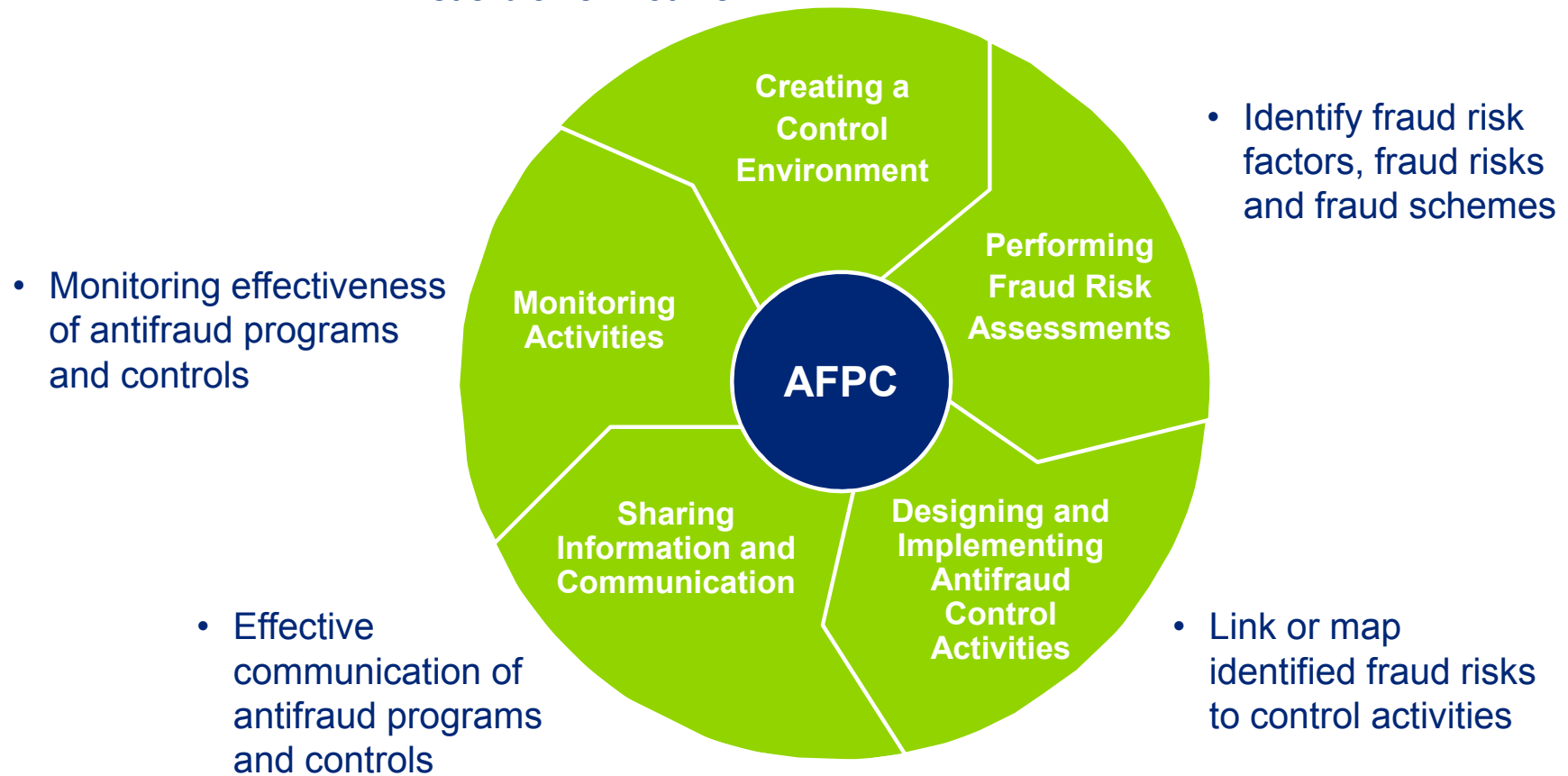
- Intended to help businesses and other entities assess and enhance their internal control systems
- Underlying principles provide framework for proactively establishing an environment to manage fraud risk

## Private sector initiative established in 1985 by the following organizations:

- American Accounting Association (“AAA”)
- American Institute of Certified Public Accountants (“AICPA”)
- Financial Executives Institute (“FEI”)
- The Institute of Internal Auditors (“IIA”)
- Institute of Management Accountants (“IMA”)

# A COSO-Consistent Approach

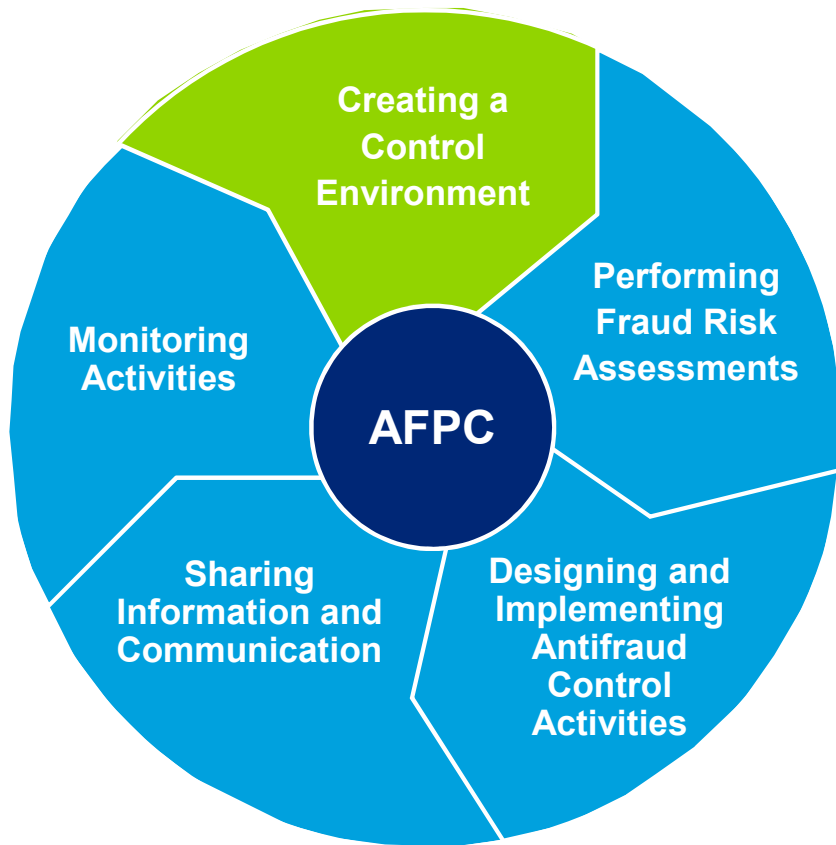
- Tone at the top
- Code of Conduct/Ethics
- Whistle-blower Hotline



5 Elements Source: Committee of Sponsoring Organizations of the Treadway Commission, Internal Control — Integrated Framework

# Creating a Control Environment

# COSO Overview: Control Environment

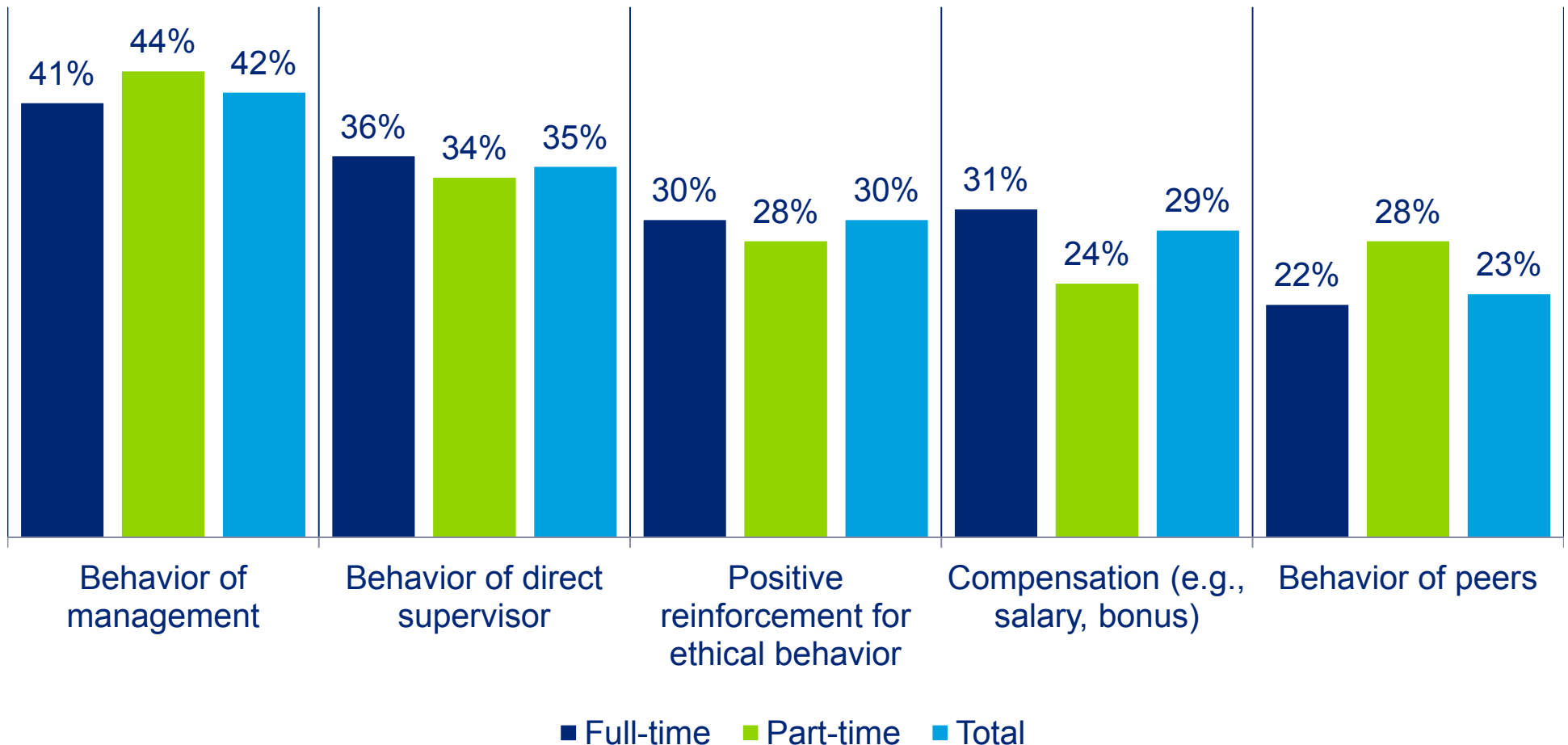


Some of the components of the control environment in which management may focus its efforts include:

- Audit Committee
- Management Accountability
- Fraud control policy/strategy
- **Tone at the Top**
- **Code of Conduct and Ethics**
- Hiring and Promotion Procedures
- **Hotlines/helplines**
- **Investigation and corrective action**

# Setting the Right Tone

What are the top factors promoting an ethical workplace environment?



Source: "Deloitte & Touche USA 2007 Ethics & Workplace" survey results

# Measuring the Tone at the Top

- Employee feedback
  - Cultural surveys
  - **Exit interviews**
  - Internet sites (e.g., Vault.com) can provide pointers
  - **Focus groups**
    - **Interviews and discussions**
- Discussion with the internal audit team
- Onsite observation
- Review of communications to employees, lunchroom notice boards, intranet

# Whistle-blower Systems — Regulatory Guidance

## Sarbanes-Oxley Requirements

- Audit Committee must establish the process
- Required for employees but anyone can call
- Confidential
- Anonymous
- Functions
  - Receipt, retention, treatment of complaints

## The Dodd-Frank Act of 2010, Section 922

- Created rewards of 10–30% of monetary sanctions for whistleblowers who report to the SEC original information leading to securities law enforcement actions that recover more than \$1 million.
- **See potential actions in “Whistleblowing and the New Race to Report” downloadable from [www.deloitte.com/forensiccenter](http://www.deloitte.com/forensiccenter)**

# Hotline/Helpline Benchmarking

## 2010 Corporate Governance and Compliance Hotline Benchmarking Report

- Published by hotline operator **The Network, Inc.**
- **Downloadable from [www.tnwinc.com](http://www.tnwinc.com)**
- Facilitates benchmarking by industry segment
- Based on 524,628 incident reports over 5 years from 2005-2009 from 4,060 organizations
- Addresses statistics on:
  - **Effectiveness of a key antifraud control**
  - **Incident categories (e.g., fraud, personnel management, customer interaction)**
  - **Means of caller awareness (e.g., brochure, HR, Manager, Poster)**
  - **Anonymity**
  - **Case Outcomes (e.g., investigation vs. no investigation)**
  - **Case Dispositions (e.g., disciplined, terminated, unresolved)**
  - **Incident Reports by Industry**

# Hotline/Helpline Benchmarking (cont.)

## Impact on Organization

- Will likely raise expectations for the depth of analysis of hotline effectiveness
- **May reveal previously undetected hotline effectiveness issues**
- **Creates opportunity to enhance performance of a key internal control**
- Opportunity to add value by anticipating and addressing this issue

# Case Study #1

## The Fraud Allegations:

- Company booked \$2.6M in false sales during Q2 to a single customer, resulting in overstated product sales revenue by as much as 35%.
- CEO instructed customer's President to inflate his family's financial statement to reflect a higher net worth in order to support the false sales
- The down payment from this sale (\$1M) never originated from customer. In reality, it was a loan from the former COO of the customer.
- When Controller confronted CFO about the origin of the down payment, the CFO "covered his ears and said, 'No, no, no, no, no, no, no, no, no. I don't want to hear it.'"
- Controller and CFO went along with the fraud, even though they didn't originate it

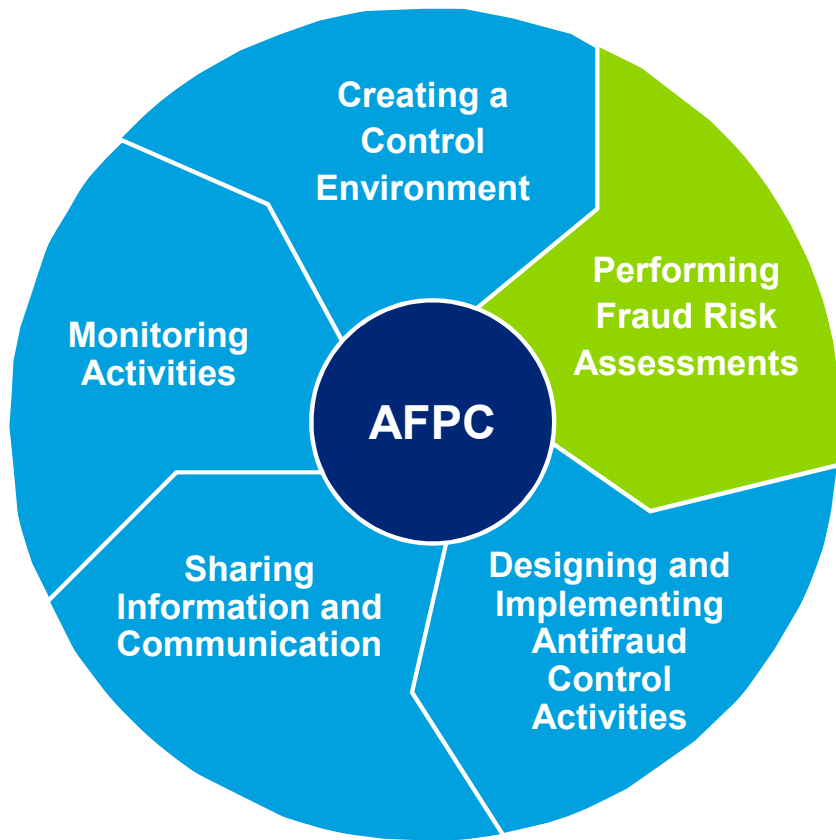
# Case Study #1 (cont.)

## Lessons to Consider:

- Data mining/analytic of sale to one customer for \$2.6M (35%) should be a red flag for follow up
- Combination of management override and collusion may be especially hard to detect, yet data mining would have shown obvious spike in sales
- Collusion can happen “by accident” (e.g., Controller learning about it after the fact, then being complicit).
- **Would a different *tone at the top/culture of compliance* have made a difference?**
- **What would have been your reaction to the CFO covering his ears and saying, “No, no, no, no, no, no, no, no, no, no. I don't want to hear it”?**

# Performing Fraud Risk Assessments

# Fraud Risk Assessment



Elements of the fraud risk assessment on which management may focus include:

- **Identify Fraud Risk Factors**
- Identify Fraud Risks
- Consider Potential Fraud Schemes
- **Map Specific Identified Risks to Mitigating Control Activities**
- Risk Treatment

# Fraud Risk Assessment (“FRA”)

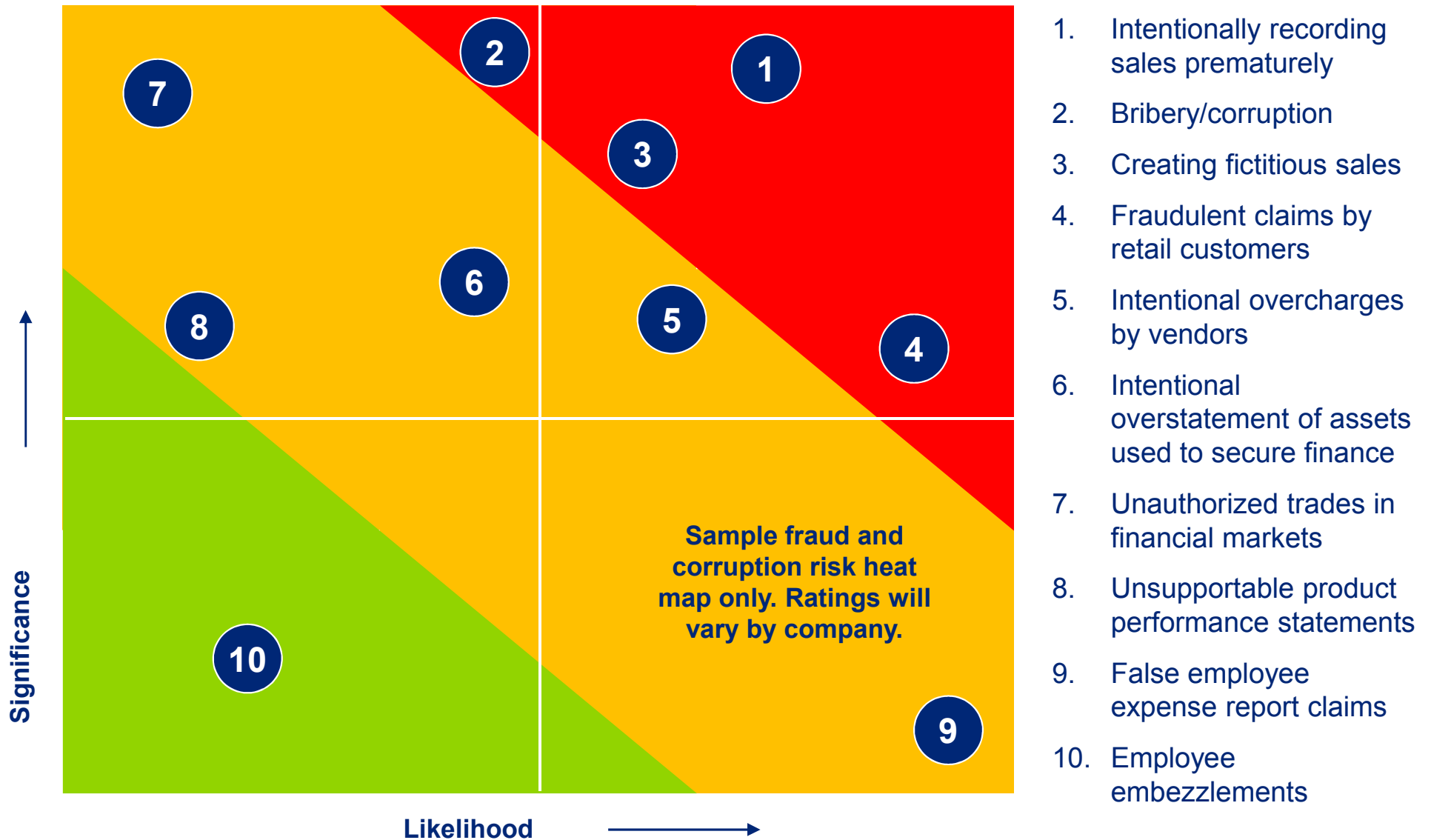
A fraud risk assessment is crucial part of an entity’s broader risk assessment process. It considers the ways that fraud and misconduct can occur by and against the entity. To be effective, a fraud risk assessment:

- Is systematic and recurring
- Considers possible internal and external fraud schemes and scenarios
- Assesses risk at entity-wide, significant business unit and significant account levels
- Evaluates likelihood and significance
- **Is performed with the involvement of appropriate personnel**
- Considers management override (e.g., journal entries, bias of estimates, non-routine transactions)
- **Is dynamic and could be updated when new or unique circumstances arise (e.g., changed operating environments, restructurings, acquisitions), at least annually**

# Examples of Common Manifestations and Risk Areas of Fraud



# Management's fraud risk assessment — sample “heat map” summary



# Where do Fraud Risk Assessments Typically Fall Down?

- **Appropriate personnel are not involved in the process**
- Methodology not shared with external auditors in advance
- Assessment consists of an identification of risk factors only, and does not include an identification of schemes and scenarios
- Potential perpetrators are not identified (which can result in reliance on controls that some perpetrators could override)
- **Does not consider collusive frauds and risk of management override of controls**
- More of a controls assessment than a risk assessment
- Does not identify and quantify residual risk
- Lack of monitoring by the Audit Committee/Board
- **Lack of follow up after identification of fraud risks and linkage to mitigating controls**

# Case Study #2

## The Fraud — Background and Allegations:

- Children's clothing manufacturer
- Fraud lasted between 2004-2009
- Allegations:
  - Executive Vice President of Sales improperly offered deep discounts to its largest wholesale customer to induce them into buying greater quantities of the manufacturer's clothing
  - VP fraudulently created and signed false documents that misrepresented the timing and amount of those discounts (the documents showed less discounts than actually given).
    - Submitted these phony documents to accounting department
  - VP persuaded the customer to defer subtracting the discounts from payments until later financial reporting periods (to correlate with the fictitious documents he submitted to accounting)

## Case Study #2 (cont.)

### The Aftermath:

- Company self-reported misconduct to SEC
- Unlawful conduct was relatively isolated in nature
- Company cooperated in the investigation, including undertaking:
  - A thorough internal investigation
  - Substantial remedial actions

### The Result:

- SEC entered a non-prosecution agreement with company
- Company not charged with any violations

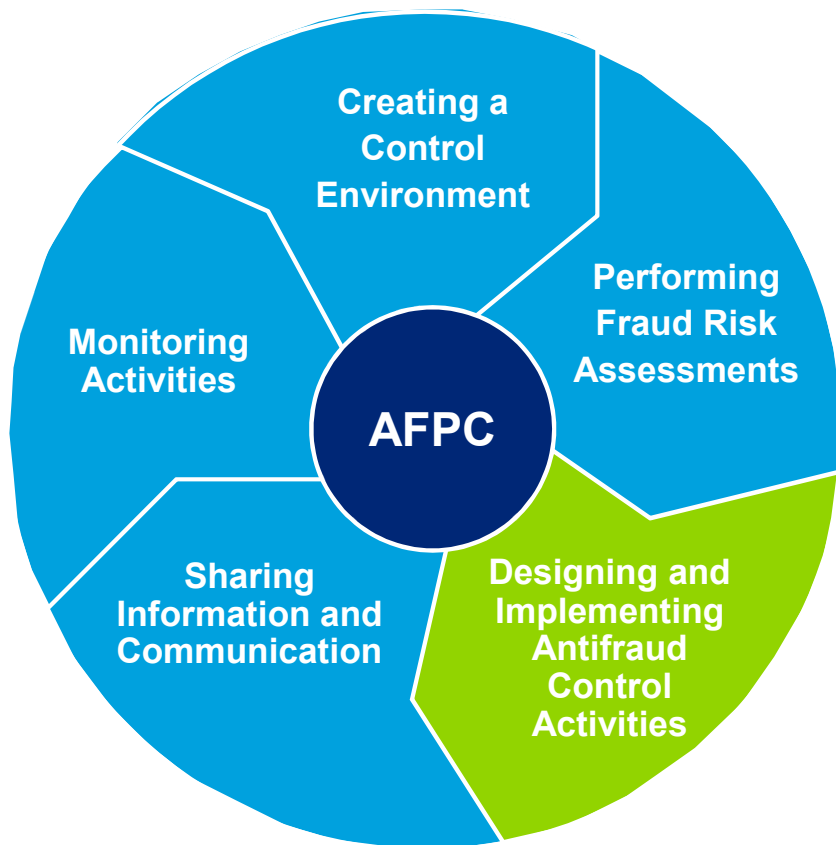
# Case Study #2 (cont.)

## Lessons to Consider:

- If misconduct is discovered, be proactive in:
  - Conducting an internal investigation
  - Putting remediation in place
  - Consider self reporting
  - Fully cooperating with regulators/law enforcement
- Internal Audit might consider sending confirmations to large customers with deep discounts requesting information about the nature, timing, and extent of their specific discounts
- **Consider reviewing customer correspondence file (there may have been indications of the VP persuading the customer to defer discounts until later periods)**
- **Could accounting department have been more skeptical of the fictitious documents they received?**
- **Would your company's *fraud risk assessment* have included a variation of this scheme?**

# Designing and Implementing Antifraud Control Activities

# Design and Implement Control Activities



Management may focus on several considerations when designing and implementing antifraud control activities, including:

- Preventive Controls
- Detective Controls
  - Preventive and detective controls may be completely manual, involve some degree of computer automation, or be completely automated.

# Measuring Fraud Detection Effectiveness

- Management or the Board should establish measurement criteria to facilitate monitoring and continuous improvement of fraud-detection controls.
- Measurement techniques will vary by organization, but may include:
  - Reporting on the lack of recurrence of frauds uncovered
  - **Reporting on timeliness of implementation of remediation plans**
  - **Addressing likelihood of frauds prevalent throughout the industry**
  - **Reporting of fraud versus complaints, grievances, etc. via hotline calls**

# Antifraud Control Activities — Summary

- Maintaining and implementing preventative and detective control activities which mitigate fraud risks
- Clearly define who is responsible for each fraud control
- Expect that 70% to 80% of identified fraud risks are mitigated by existing control activities (e.g., approvals, authorizations, verifications, reconciliations, segregation of duties, reviews of operating performance and security of assets)
- **Anticipate that the fraud risk assessment will reveal that no control activities exist to mitigate 20% to 30% of the identified risks and therefore additional antifraud control activities may be necessary**

## Key Considerations

- Management is responsible for designing, implementing and testing the necessary control activities to respond to assessed fraud risks
- **Control activities should be documented by linking them to identified fraud risks**
- Evaluate the effectiveness of existing controls
- As needed, implement additional controls, including preventative and detective controls
- **Consider IT controls when designing control activities**
- Testing of control activities (e.g., by Internal Audit) should include any business process in which a fraud risk has been identified

# Case Study #3

## Background:

- Employee at large hospital earning \$37,000 a year
- Job Description: receiving clerk who was responsible for ordering, receiving and stocking ink cartridges for the printers at the facility
- Had password-protected access to the computer used to order office supplies

## The Fraud Allegations:

- Ordered toner-ink cartridges in bulk, diverted delivery, then sold them elsewhere
- During a 1 year time period: ordered about \$1.2 million worth of toner that wasn't compatible with any machine at the hospital and far exceeded the toner usage
- Surveillance video showed him intercepting the packages and taking the boxes to a garbage-bay area

## Case Study #3 (cont.)

### The Symptoms:

- Made cash payments to buy property in the Bronx and Westchester
- Owned an apartment in the Trump Plaza, a luxury high-rise
- Bought a 2011 BMW X6 with \$50,500 in cash as a down payment
- Spent significant money on airfare and hotels and shopping sprees at retailers
- Wore fancy clothes

### Lessons to Consider:

- Lifestyle didn't match income
- **The first time, its an anomaly; after that, the baseline becomes “normal”**
- Did anyone else have access to his passwords to monitor office supply orders?
- **Would *preventive or detective controls* caught this fraud earlier?**
- **Was anyone watching the surveillance cameras?**

# Information and Communication

# COSO Framework — Information and Communication

Information and communication requires that relevant external and internal information be identified, captured, processed, and communicated throughout the organization in a timely manner to enable people to carry out their responsibilities.

Information	Communication
<ul style="list-style-type: none"><li>• Information systems may be formal or informal, computerized, manual or a combination thereof</li><li>• <b>Integrity of information is imperative.</b> Requires internal control mechanisms to provide reasonable assurance that information is:<ul style="list-style-type: none"><li>– Appropriate</li><li>– Current</li><li>– Timely</li><li>– Accurate</li><li>– Accessible</li></ul></li></ul>	<ul style="list-style-type: none"><li>• Written communication (e.g., policy manuals; job descriptions; memorandums; bulletin boards)</li><li>• Verbal communication (e.g., meetings, feedback; trainings)</li><li>• <b>Demonstrated through actions (e.g., management sets example)</b></li></ul>

# Sharing Information and Communication

- **As it relates to fraud risk management, what are some key objectives of sharing information and communication?**
- Objectives of sharing information and communication:
  - **Convey a clear message about the corporate culture**
  - Set expectations about ethical employee behavior
  - Remind employees about their roles and responsibilities for maintaining an ethical work environment
  - **Maintain awareness of reporting mechanisms available to employees**
  - Reinforce the ramifications of improper or unacceptable behavior in order to deter others from similar actions

# Role of Internal Audit

## How can internal audit facilitate sharing information and communication?

- Assess the ability of the organization to collect and share information about fraud
- Assist with information gathering and dissemination throughout the organization
- Report to those charged with governance
- **Share knowledge obtained from fraud subject matter experts**
- **Share knowledge gained from relevant events pertaining to fraud risks and/or controls that occurred internally and/or at external parties**
- Facilitate sharing of fraud risk information and control best practices relating to fraud amongst subsidiaries and divisions
- Facilitate the fraud risk assessment process

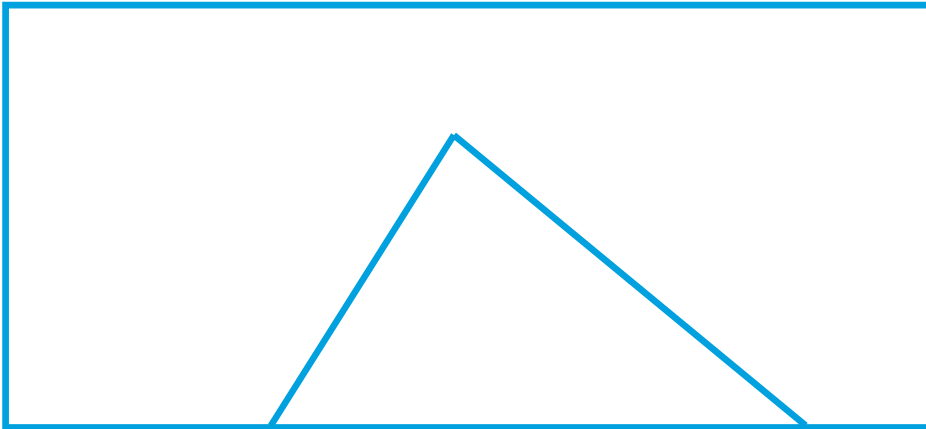
# Fraud Awareness Training: Tips for increasing comprehension

- **Provide employees with examples of what constitutes fraud.**
- Six symptoms of fraud 1:
  - Accounting or document symptoms
  - Analytical symptoms
  - Lifestyle symptoms
  - Behavioral symptoms
  - Internal control symptoms
  - Tips and complaints

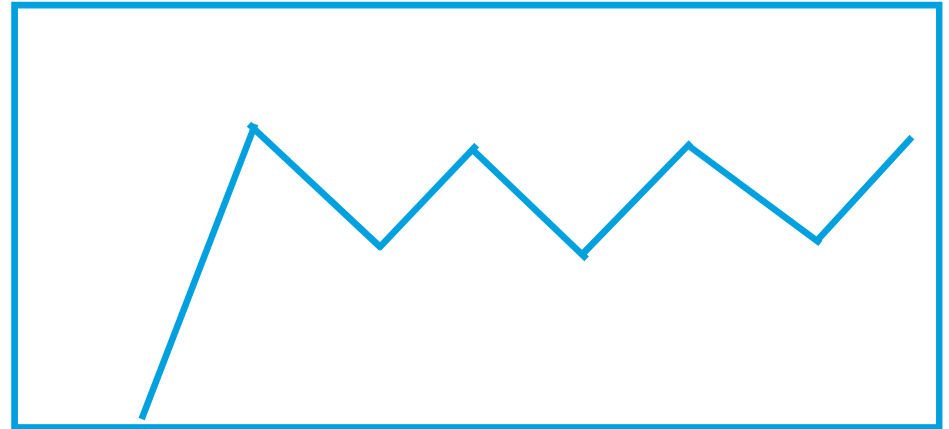
<sup>1</sup> Professor Steve Albrecht, from Brigham Young University, suggests the Six Symptoms Framework for facilitating the recognition of fraud risk factors

# Key Challenge: Maintaining Awareness

Awareness following a single communication event



Awareness levels with repeated communication events



## Maintaining awareness

- Email reminders
- Posters on bulletin boards
- **Flyers included with invoices and vendor payments**
- **Articles included in internal/external newsletters**

# Case Study #4

## The Fraud — Background and Allegations:

- State Pension/Retirement Fund’s chief investment officer and his brothers produced a low budget film and wanted to distribute DVD
- An investment firm consultant was advised to help with film distribution
- Consultant arranged a meeting between the Fund CIO’s brother and a distribution company to discuss a possible DVD distribution deal.
  - Distribution company said they were not interested in distributing the film
  - After meeting, the brother called the consultant to complain about the way he was treated by the distribution company
  - Consultant then called the distribution company and told them to:
    - treat the brother “carefully” because his firm was trying to obtain an investment
    - instructed the distribution executive to “dance along” with the brother.
- Distribution company ultimately reversed course and offered to manufacture and distribute the DVD at a discount from its standard fee.
- Soon after the consultant advised that the distribution company was moving forward with the DVD deal, the Retirement Fund made a \$100 million investment in the consultant’s fund.

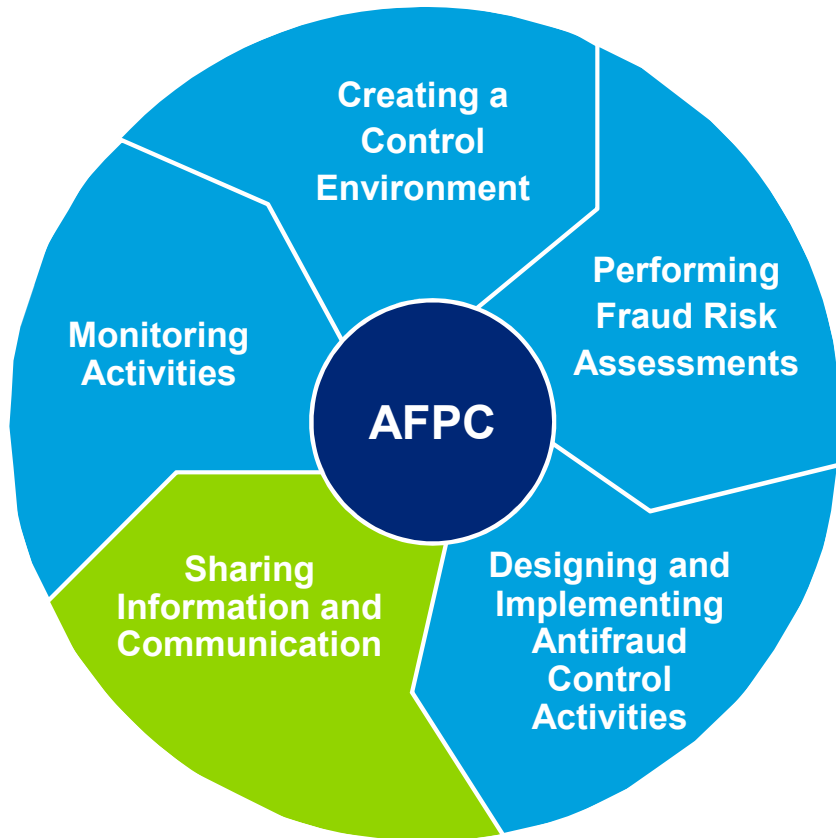
# Case Study #4 (cont.)

## Lessons to be Considered:

- Produce a movie that companies want to distribute!
- Consideration for Internal Audit regarding large company investments:
  - Request the analysis for how investment advisor/fund was chosen
  - Read the correspondence file between company executives and investment advisors
- **Corruption may involve more than money (e.g., ego of DVD film makers)**
  - **Pay attention to what is important to employees: there may be fraud risk factors otherwise never imagined**
  - **If it's important to them, it may be enough of an incentive to commit fraud**
  - ***Information and Communication: What are the most important fraud-related concepts for your organization to communicate to employees?***

Monitor

# COSO Overview: Monitoring



## Monitoring Activities

- Ongoing periodic monitoring of AFPCs are vital to management's ability to react to the changing business environment and related impact on fraud risks.
- Helps controls operate more effectively
- Provides reassurance that management is executing its internal control responsibilities effectively

# Examples of Monitoring Activities

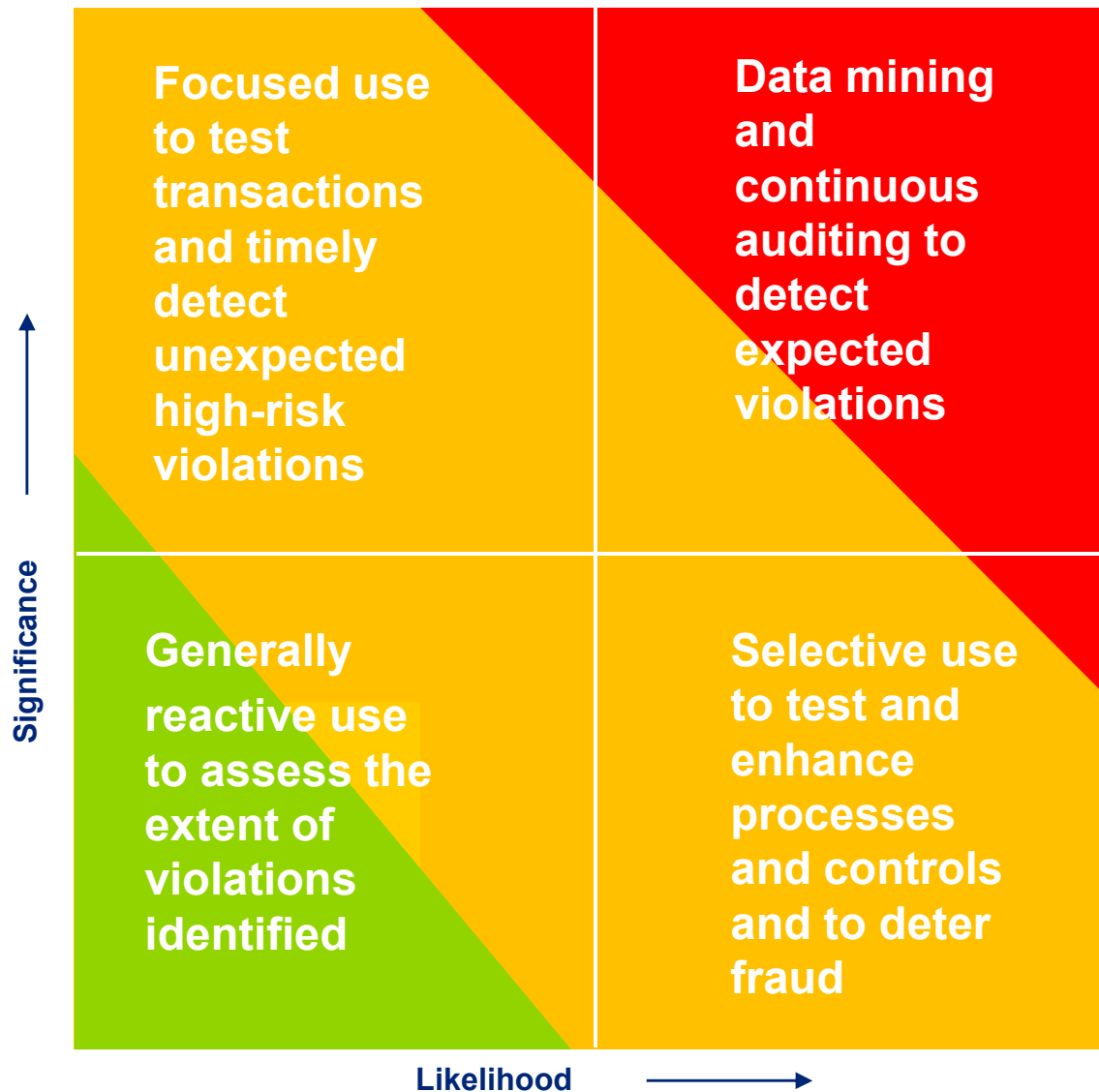
## Periodic Evaluations

- Frequent and timely account reconciliations
- Compliance testing by internal audit
- **Confirmation of information with external parties**
- Periodic confirmation from employees (code of conduct compliance)
- Anomaly detection programs
- Review of operating units' financial reports by higher levels of management

## Continuous Monitoring

- **Anomaly detection using software (e.g., ACL, DTect)**
- **Data Mining**
- Journal entry testing

# Potential strategic use of technology to deter and detect fraud



- **Sampling 100% and publicizing it enhances deterrence and detection**
- **Reconciling data provided to G/L helps ensure data is complete**

# Case Study #5

## The Fraud Allegations:

- Financial Statements did not disclose the CEO's perquisites:
  - Over \$4,000 per month to live in a ski lodge in Wyoming
  - Vacations for him and his family
  - Fight training
  - Hunting
  - Spa
  - Skiing and health club expenses
  - Leased Lexus SUV
  - Costs to commute by private aircraft from his home to work
  - Other day-to-day living expenses such as groceries, liquor, tobacco, nutritional supplements, and clothing
  - **CEO did not have a personal credit card**, as he falsely claimed personal items were business related

# Case Study #5 (cont.)

## The Fraud Allegations (cont.):

- Chief Accounting Officer authorized company's payment of personal expenses, circumvented internal controls and policies that required the CEO to document the business purpose for his expenses
- Chief Financial Officer permitted company to pay the expenses even though he was informed CEO was not submitting the required documentation.
  - **A finance department employee raised concerns to the CFO that some of CEO's expenses were not business related.**
- Chief Operating Officer was informed of problems with expense reporting and failed to adequately address them

## Case Study #5 (cont.)

### The Fraud Allegations (cont.):

- A whistleblower had complained to the Company; limited follow up occurred
- Company learned of an SEC investigation of this matter in mid-2007. Even after learning about it, the Company:
  - 1. Continued to make misleading public filings and**
  - 2. Failed to disclose to investors in public filings that an internal review concluded the CEO had intentionally misclassified his expenses.**
- The majority of the expenses were not repaid

# Case Study #5 (cont.)

## Lessons to Consider:

- When something appears wrong, don't continue down the same path (e.g., continuing to misrepresent financials after learning SEC is performing investigation)
- Others outside accounting can be held liable (e.g., COO was informed of problems but failed to adequately address them)
- **How would you judge tone at the top?**
- **How did the CAO circumvent internal controls and policies that required the CEO to document the business purpose for his expenses?**
- **What was internal audit's role?**
- **Was *monitoring* effective at this company?**
- **How effective was their whistleblower hotline?**

# Final Thoughts

- Fraud risk management is a **collaborative effort** that involves everyone within an organization.
- Fraud risk can never be eliminated entirely; more effective organizations employ a **risk-based approach** to mitigating fraud risk.
- Fraud risk management is an **ongoing and evolutionary process** that changes as the organization and the environment change.
- Regular fraud risk management **process evaluation and measurement** assists continuous improvement.

“Live in such a way that you would not be ashamed to sell your parrot to the town gossip.”

**Will Rogers**

# Questions and Answers

# Contact Information

## **Craig Hirsch**

Manager, Forensic & Dispute Services  
Deloitte Financial Advisory Services LLP

+1 305 808 2535

[chirsch@deloitte.com](mailto:chirsch@deloitte.com)

# Deloitte.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2011 Deloitte Development LLC. All rights reserved.  
Member of Deloitte Touche Tohmatsu Limited