

# Office of the State Comptroller

How we do it – Internal Control Education and  
Awareness

# More than One Way

- Targeted Training
- Varying Focus Training
- Awareness

# Targeted Training

- Executive - Control Environment and Risk Appetite
- SLMS- training ++++++
  - Director and Assistant Director Training



# Leadership

### Top Three Risks to Achieving OSC's Goals and Objectives

**Risk 1:** \_\_\_\_\_

Why is this a risk?

---

---

---

**Risk 2:** \_\_\_\_\_

Why is this a risk?

---

---

---

**Risk 3:** \_\_\_\_\_

Why is this a risk?

---

---

---

### Top Three Unacceptable Events

**Event 1:**

---

---

---

**Event 2:**

---

---

---

**Event 3:**

---

# Office of the State Comptroller

Senior Management Session July 29, 2008

## **Control Environment and Risk Assessment**

Laurel Jolliffe

Steve Hillerman

# Risk Appetite

The amount of risk, on a broad level, an organization is willing to accept in pursuit of its objectives

It reflects the organization's established risk philosophy and influences the culture and operating style

# And the Answers are....

- Fraud/Corruption
- Failure of an agency mission critical operation
- Any event that would endanger employee safety
- Unauthorized disclosure, access or loss of personal/private information maintained by the agency
- Public doubts the Comptroller's or the Office's integrity, competency, accuracy and/or professionalism



# And the Answers are....

- An inadequate or unskilled work force
- A hostile work environment
- Discrimination of any kind
- Being irrelevant
- Not meeting statutory requirements
- Management violates the public trust with unethical behavior



# **Directors and Assistant Directors**

# Internal Controls



It's a Risky Business

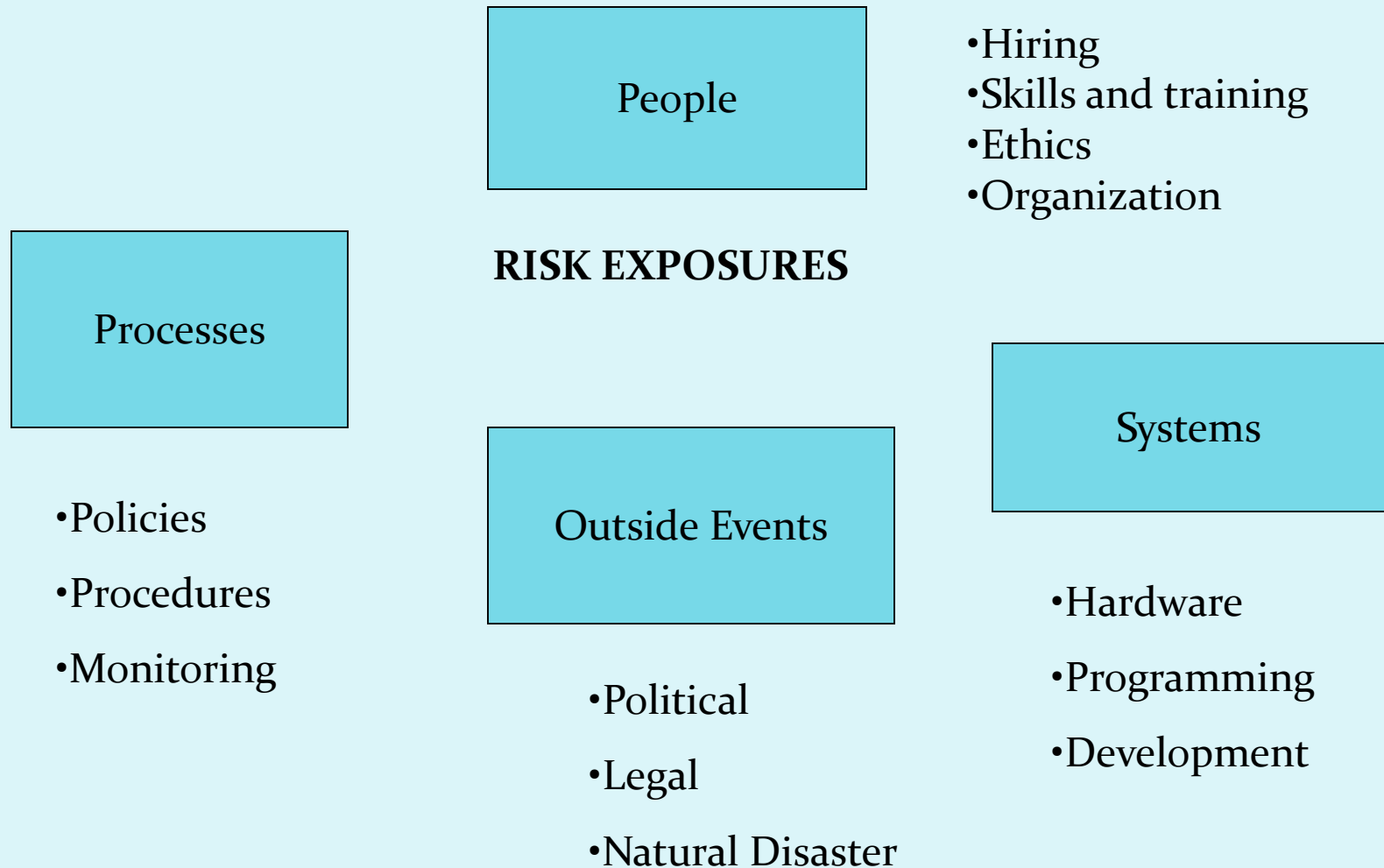
# Agenda

- What are internal controls?
- Why do I care?
- How do I identify and respond to risks?

# Risk



# Risk



# Communication Channels

- Inform employees of their duties and responsibilities
- Report sensitive matters
- Enable employees to provide suggestions
- Provide the information necessary for all employees to carry out their responsibilities effectively
- Convey top management's message that internal control responsibilities are important and must be taken seriously

# 4 Types of Communication

- Non-Verbal
- Verbal
- Listening
- Written

**Remember: Actions Speak Louder Than Words!**





# Varying Focus Areas

- Fraud
- Information Security/Privacy

# Integrity First



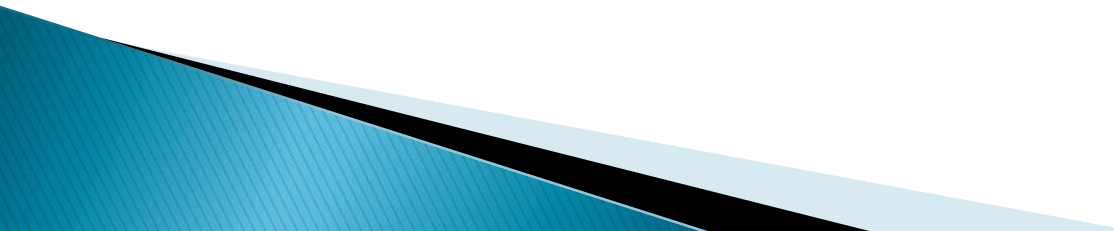
Office of the

INSPECTOR GENERAL

Stephen Hamilton, Inspector General

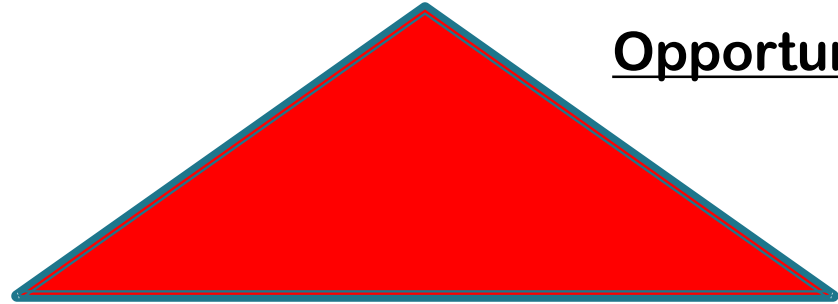
# Session Objectives

**To understand:**

- What fraud and abuse looks like**
  - Who commits fraud & why**
  - How to identify fraud**
  - What you can and should do**
- 

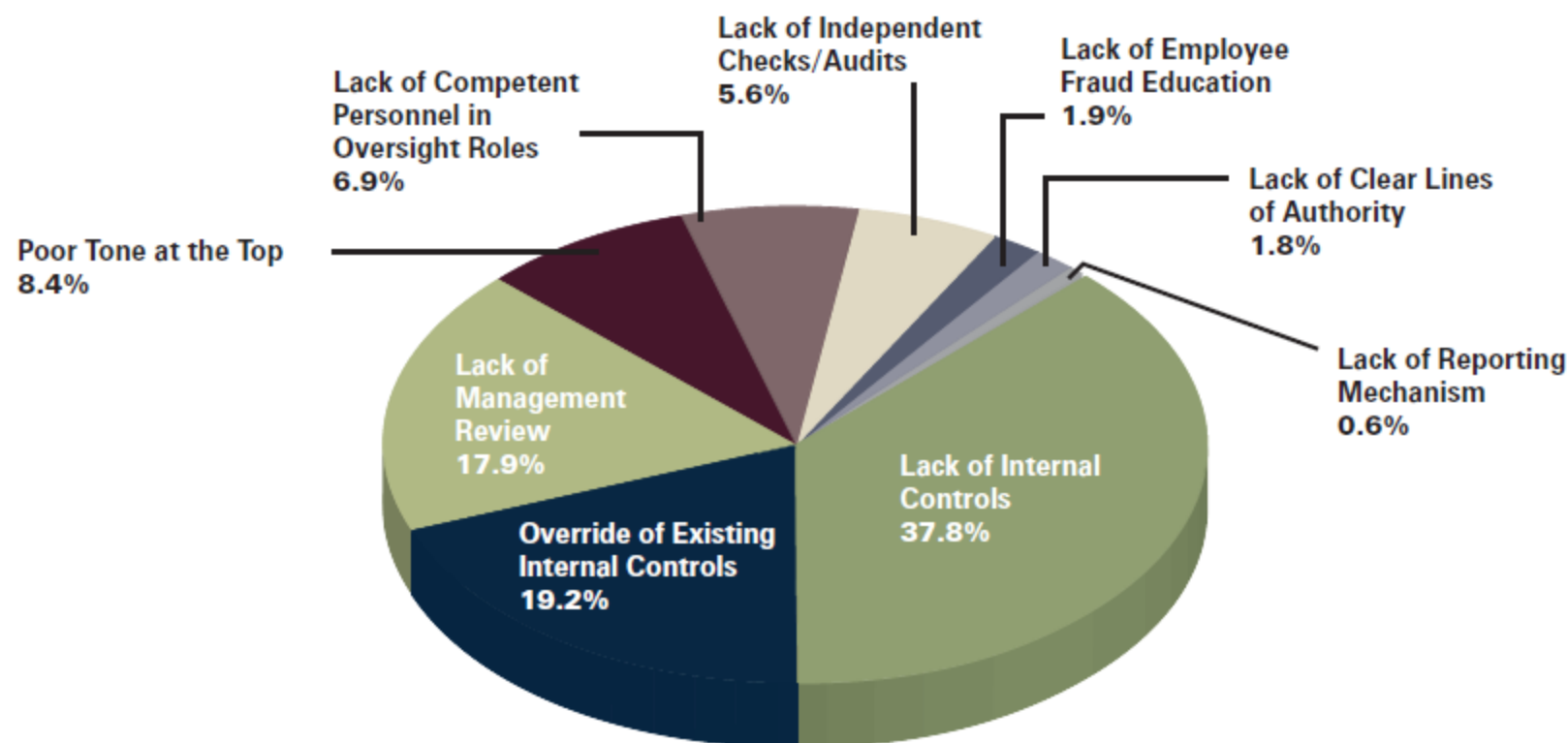
# Opportunity

Opportunity



- Access to cash or highly convertible assets
- Ability to conceal the act
- Inadequate Internal Controls
  - Little separation of duties
  - Lack of automatic controls
  - No management oversight
  - Lack of clear expectations or procedures
  - Weak or absent leadership
- Culture of “not questioning”

## Primary Internal Control Weakness Observed by CFEs



# Prevention Controls We Take at OSC

- Background checks
- Separation of duties
- Job rotations
- Written procedures
- Access controls
- Ethics policies
- Training
- Self-assessments
- IG/Hotline
- Approval Process
- Internal Audit





# OSC PRIVACY 2010

---

The “Secrets” You Need to Know



# **Awareness Everywhere**

- Internal Control
- Fraud



et

Directory Services WorkPlace Technology Forms

## Thoughts of Summer

So it is summer! Ah, time for vacations and Everything about summer makes you think of summertime and lazy days, but I am also everything is in working order if someone is temporarily halted. Think about it, summer g our organization has planned.



you there is a huge risk there. Now is the be units have to deal with this on a micro level. take a look at the tools available on our OS someone retires, but really how you plan to not there. On one scale this is about success



# Internal Control Office

Welcome to the Internal Control Office Web Site

*A Message from Laurel Jolliffe...*

## Risk Management—Are you on a Sinking Ship?

Normally, I write a quarterly article discussing fascist of internal control and risk management and hopefully relating it to common events to improve the understanding throughout the agency. This time however, I came across this article that I thought brings home the concept of enterprise management so well that it was worth me stepping down from my bully pulpit. See if you agree...

The Titanic: An Analogy of Enterprise Risk  
*Michael Rasmussen, J.D.*  
*Chief GRC Pundit @ GRC 20/20 Research, LLC*

As we close out 2012 let us roll the years back from 2012 to 1912.  
 One hundred years ago was the disaster of the Titanic. What can

Internal Control at OSC

- About ICO
- Internal Control System 2011
- Internal Controls Overview
- Internal Control Guide
- Internal Control Articles
- Functions of OSC
- OSC Mission, Vision, Values
- OSC Strategic Priorities
- OSC Key Objectives - 2009
- Annual Certification
- Call Letter
- Risk Assessments
- Annual Certification Forms
- Training
- OSC Core Competencies
- Training Calendars
- Presentations
- Resources




Executive Order on



Internal Control

NYS Standards for



Internal Control



# Focus on Fraud

January  
2013

Welcome to our *Focus on Fraud* newsletter. The purpose of this monthly newsletter is to heighten the awareness of employees to the potential for fraud and abuse and the linkage to internal controls. This newsletter is an integral element of OSC's overall fraud and abuse prevention strategy, a key to our Integrity Framework initiative.

*Occupational fraud* is the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization's resources or assets. This

*This edition covers some behavioral indicators that fraud or abuse may be occurring.*



## Focus on Fraud

February

### *Some Tips on What to Look For*

- Most fraud starts out small. As the fraud scheme continues over a period of time, the typical fraudster begins to gain confidence in the fraud scheme and may move on to fraud schemes involving larger amounts.
- Inconsistencies or things that don't look like you expect them to.
- Disregard for rules and procedures.
- Air of secrecy and/or entitlement.
- Lack of Documentation or copies instead of originals.



## Focus on Fraud

May  
2013

**Identity fraud** is the unauthorized use of another person's personal information to achieve illicit financial gain. Identity fraud can range from simply using a stolen payment card account, to taking control of existing accounts or opening new accounts, including mobile phone or utility services. **Put simply, identity theft is FRAUD.**

### Common ways Identity Theft occurs:

- Defrauding businesses or institutions.
- Stealing records from their employer
- Bribing an employee who has access to the records
- Conning information out of employees
- Hacking into the organization's computers
- Rummaging through the trash of businesses, or dumps in a practice known as "dumpster diving."
- Using a method called "pretexting" (on the phone) or

The [2013 Identity Fraud Report](#) released in February 2013 by [Javelin Strategy & Research](#) reports that in 2012 identity fraud incidents increased by more than **one million victims** and fraudsters stole more than **\$21 billion**, the highest amount since 2009. The study found 12.6 million victims of identity fraud in the United States in the past year, which equates to **1 victim every 3 seconds**. Data breaches continued to play a significant role in identity fraud. Organizations alert their customers when their information is compromised and send a letter (i.e. "data breach letter"). The report also found that nearly 1 in 4 data breach letter recipients became a victim of identity fraud, with breaches involving Social Security numbers to be the most damaging.

We all have seen the reports in the news of large breaches of data from hackers into credit card companies, financial institutions and even Facebook. But, if you think that identity thieves aren't focusing on government organizations like OSC, think again. Last year the South Carolina Department of Revenue found that a hacker had used a "spear-phishing" attack to install at least 33 unique pieces of malicious software and utilities on the department's servers to steal financial data. A spear-phishing attack typically poses as an email from a known entity or person and asks users to click on a link, which deploys malware that steals data. More than 3 million Social Security numbers and 387,000 credit and debit card numbers were exposed. Of the credit card numbers, approximately 16,000 were unencrypted.

In another headline-grabbing security breach, hackers stole the Social Security numbers of as many as 280,000 people from Utah Department of Health databases, an incident that quickly forced Utah's CIO's resignation. Historically personal information in state and local government databases hasn't been as big a target for hackers as other sectors. But the South Carolina and Utah breaches could represent a shift in thinking. Cybercriminals may increasingly exploit personal records for identity theft and insurance fraud.