Fraud Risk

- Fraud Defined
- Why Care / Why Assess Fraud Risk?
- What is Fraud Risk?
- Fraud Risk Assessment:
  - Fraud Risk Assessment
  - Angels & Demons Data Collection Exercise
- Fraud Risk and IA Audit Plans
What is fraud?

- IIA: Any illegal acts characterized by deceit, concealment or violation of trust. These acts are not dependent upon the application of threat of violence or physical force. Frauds are perpetrated by parties and organizations...

- SAS 99: An intentional act that results in a material misstatement in the fin. stmts that are the subject of an audit.

- Black’s Law Dictionary: All means by which one individual can get an advantage over another by false suggestions or suppression of the truth.
If you accept any federal funds / have any federal contracts, the Federal Sentencing Guidelines apply to you… and require that compliance programs:

- address specific areas of potential fraud
- use audits / risk evaluation techniques to monitor compliance and assist in the reduction of identified problem areas
Fraud Risk
Why Care?

United States Sentencing Guidelines (USSG)

Effective 11/2004 = USSG amended to provide greater guidance regarding compliance program criteria for an effective program to prevent and detect violations of the law:
(USSC Guidelines Manual §8B2.1. Effective Compliance and Ethics Program)

(a)(1) Exercise due diligence to prevent and detect criminal conduct

(a)(2) Otherwise promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law

– (b)(1) Establish standards and procedures to prevent and detect criminal conduct

(c) Periodically assess the risk of criminal conduct and take appropriate steps to... reduce the risk of criminal conduct
If there is no intent, there's no guilt

Titus Livius
Fraud Risk - Why Care?

- **COSO 2013 Fraud Principle 8**: Organization should consider the potential for fraud in assessing risks
  - Focuses on four types of fraud (Fraudulent Reporting, Safeguarding Assets, Corruption & Mgmt Override)
  - Encourages organizational / wide view of risk

- **PCAOB, AS 5** requires documentation:
  - Understanding of transaction flow
  - Points at which a misstatement could arise
  - Controls implemented to mitigate potential misstatements
  - Identify controls designed to prevent or timely detects unauthorized acquisition or disposition of assets that could result in material misstatement

- **SOX 802** – Criminal penalties for altering documents
**Fraud Risk - Why Care?**

IIA Standards and Fraud Practice Guide Emphasize Internal Audit’s Role in Addressing Fraud

- **Antifraud Programs & Controls Assessment:** Must evaluate how organization manages risk (IIA Standard 2120) and Must evaluate the occurrence of fraud and how the organization manages fraud risk. *(IIA Standard 2120.A.2.)* *(IIA Pre-COSO 2013 – first “official” driver of fraud risk assessments)*

- **Fraud Risk Assessment:** CAE must report periodically to management / board on significant fraud risk exposures *(IIA Standard 2060)*

- **Individual Audits:** Must consider fraud when developing engagement objectives *(IIA Standards 1220, 2210)*

- **Proficiency:** Evaluate the risk of fraud & the manner in which it is managed by the organization *(IIA Standard 1210)*
US government admits losing 10% of spending to fraud; US government realizes a $9.75:1 on fraud management.

Effective fraud management produces 8:1 ROI for the financial services industry.

ACFE estimate: companies lose $1 trillion or 7% of revenue to misconduct.

PwC GECS survey – 40% increase in fraud, before the recession.

Controls paradox:

- Economist Intelligence Unit: 85% of companies detected significant frauds over past 3 years.
  - 10% suffer >$100 million
  - Large companies - $23 million
  - Small companies - $8.2 million average loss

Fraud Risk

Don't Forget Operational Impact!
Now More Than Ever, Management through Compliance & Internal Audit Must Have the Fraud Triangle in Focus!!!

**Incentives / Pressures**
- Loss avoidance
  - Job
  - Money
  - Prestige
- Dissatisfaction with the company
- Management & 3rd party pressures
- Community relationships
- Family pressures
- Greed

**Opportunity**
- Insufficient internal controls
- External collaboration
- Management over-ride
- Internal collaboration
- Collusion
- Corrupt business customs

**Rationalization / Attitudes**
- Job dissatisfaction/Missed Promotion
- Family & health priorities
- “Everybody else” syndrome
- Self-denial of consequences to company

Economic challenges, whether in the organization or in the community, can create a “Perfect Storm” for fraud and waste; if it’s already occurring then improved economic conditions may exacerbate the fraud and waste.
SO, WHY BOTHER?

Because it just makes good business sense!!

• Demonstrate you administer an effective Internal Audit Function by documenting an understanding of:
  • how and where fraud might occur and
  • how you try to stay one step ahead of it.

• Minimize revenue leakage, cut costs, and safeguard assets.

• Safeguard company and employee reputation, and employee morale.

• Avoid and/or reduce criminal, civil and regulatory penalties, should misconduct occur.

• Help avoid/reduce government sanctions!

• Take fewer antacids and sleep a little better at night!
At The 30,000 Foot Level:
“The Risk that Fraud will Occur”
But it’s much, much more…
Fraud: (defined) - Any intentional act committed to secure an unfair or unlawful gain

“Apply the Fraud Lens to Enterprise Risks”

Reputational Risk
- External and internal impression of the organization

Operational Risk
- Inefficient business operations incl. lost time in investigating, morale impact, lost productivity, recovery of good data, vendor re-hire, etc.

Financial Risk
- Over statement of revenues, understatement of expenses, loss of earnings

Reporting Risk
- Non disclosure or false disclosure

Compliance / Legal Risk
- Potential criminal, civil or regulatory liability

Strategic Risk
- Impact on new products, services, or strategic alliances
What is Fraud Risk: Types and Categories

“Good” vs. “Bad” Fraud

Good Fraud = Leakage related activities that when prevented or detected early, leads to improved financial results

(Risk Type = “Opportunity” )

Bad Fraud = Liability related activities, that if not prevented, leads to government sanctions, and damage to brand value and reputation of individual members of the Board and senior management

(Risk Type = “Hazard” )
Fraud Risk Types: “GOOD”

Expenditure Leakage

Illustrations:

- Orders from fictitious vendor
- Kickbacks in return for allowing supplier to inflate price
- Advertiser charges for advertising not delivered
- Vendors/contractors charge for work not performed
- “Double dips” on p-card and credit card
- Salesperson obtains reimbursement for fictitious travel expenses
Fraud Risk Type: “BAD”

Liability

Unauthorized Expenses / Disposal of Assets

Illustrations:
- Payments to public officials for permits
- Payments to third parties for patents
- Gifts to public officials to evade taxes
- Payments to agents to facilitate sales
- Illegal political contributions
Fraud Risk Assessment

Comprehensive fraud risk assessment (FRA): critical to the effectiveness of an organization’s overall antifraud programs and controls.

Assessing fraud risk requires more than knowing the types of fraud risk…

• An FRA expands upon a traditional risk assessment: It is scheme and scenario based.

• The assessment considers the various ways that fraud and misconduct can occur by and against the company.
Fraud Risk Assessment

• The execution of the assessment requires:

  Internal Audit to:
  - “Think out of the box”!
  - Get creative and Get out into/ work with the business!

Management to:
  - Be participative in the process
  - Openly share schemes, scenarios, concerns, events.
Fraud Risk Assessment: 
*Key Process Steps*

- Project Planning: Senior Management Buy-in
- Anti-Fraud Program Assessment
- High Impact Scenario Identification
- Internal Audit Risk Universe Update
- Audit Planning Integration
Identifying Significant Fraud Risk Exposures: Planning

Cedars-Sinai Plan:

• Board and senior management support built into internal audit plan and compliance work plan development and approval processes.

• Co-Sourced: Combined Internal Audit and PwC resources including PwC SMEs in key areas.

• Initial Internal Audit Team fraud risk discussion for full day.

• Facilitated sessions with key director-level groups.

• Roll results into annual planning processes and individual project processes for ongoing update.
Cedars-Sinai C-Suite Buy-In:

- Internal Audit Planning and Compliance Work Plan processes involve the C-suite for input on risk and project selection.
- Plans are approved by C-suite.
- Plans presented to Audit Committee for review, input and approval.
- Plans presented to Board for review, input and approval.
- Once in an approved plan, “the show must go on!”
Identifying Significant Fraud Risk Exposures: Evaluating Antifraud Program & Controls

Cedars-Sinai Assessment:

• Internal Audit Team Assessment
  – Full Team Involvement

• PwC Tool

• Overall Assessment Results:
  • Corporate Fraud Policy
  • Coordinated Investigation Resources
  • Consistency in Criminal Prosecution and Employee Discipline Decisions
  • High Level Fraud Risk & Individual Audit Fraud Risk Considerations
Identifying Significant Fraud Risk Exposures: Schemes Inventory

Cedars-Sinai Inventory:

- Brainstorm & Networking: What’s common in the industry? What’s happened in the past?
  - Upcoding; Claims for Services not Provided; A/R & Rate Manipulation / Outliers
  - Radiology Incident; Heparin Incident; EMTALA; Cash thefts; Time fraud
  - Siemens – 2008 global fraud - bribery
  - Imaging Room; Chillers; Data Manipulation; Vendor Relationships
- Look at potential impact of identified control deficiencies; broken processes; significant hand-off requirements, etc.
How to Develop the Schemes Inventory
Predicting the Unpredictable is Key

*Think Like A Criminal When Assessing the Risk of Fraud, Corruption & Abuse!*

How would a criminal manage your XYZ business unit?

What would happen if a criminal were an XYZ vendor or customer?

What if a criminal were hired as a XYZ associate?

What if a trusted employee begins to think like a criminal?
Identifying Significant Fraud Risk Exposures: Schemes Inventory

CSHS: practical application / lessons learned

• Fraud classifications: Revenue, Expense or Reporting Impact

• Brainstorm scenarios by organizational lines of authority and three impact designations (high / medium / low)

• Director/Mgr Level Focus Group Discussions

• Angels and Demons

• Scribe
Identifying Significant Fraud Risk Exposures: 
*Plan / Conduct Angels & Demons Sessions*

**CSHS: practical application / lessons learned**

- Two Hour facilitated Sessions Necessary for:
  - Schemes
  - Likelihood & Impact
  - Controls
- Director/Manager … but not both?
- Scribe
- Focus on Schemes
  (how it’s done – criminal perspective)
- Common beliefs / identified schemes across sessions
Identifying Significant Fraud Schemes

Brainstorming Exercise!!

“Angels & Demons”

Select a Business Area: e.g.- Procurement/Contracting

Demons Identify Potential Fraud Schemes

Angels Recommend & Evaluate Antifraud Controls

- Schemes
- Controls
- Impact/Likelihood

How it can happen!

Why it won’t!
Identifying Significant Fraud Risk Exposures: 
*Tailor to Business Units & Functions*

CSHS: practical application / lessons learned

- Business units – positive response to facilitated sessions w/ Angels & Demons
- Lot’s of “Aha’s” and “Really?‘s” in sessions
- Senior Management and Board response.
- Entity Level Assessment
Identifying Significant Fraud Risk Exposures:
*Update Internal Audit Risk Universe*

**CSHS: practical application / lessons learned**

- If not already categorized in your risk universe, add category or metadata for easy identification
- Refining can be time consuming
- Annual / Ongoing update development in progress, to be completed through:
  - Improved annual interviewing
  - Individual Audit Capture
  - Updates from industry / media reporting
Identifying Significant Fraud Risk Exposures: 
*Integrate into Audit Plan*

CSHS: practical application / lessons learned

- In addition to current year updates, could identify new priority audits
- Scenarios should help define audit procedures
- Annual interviewing
- Individual audits
- Industry trend updates
- Possibly facilitate angels and demons session repeats
Creating Value While Meeting Fraud Standards

Raising Auditor Fraud Proficiency

• Knowledge
  ➢ Scheme components
  ➢ Presumptive controls
  ➢ Key risk factors & indicators
  ➢ Detection procedures

• Skills
  ➢ Scheme and scenario risk assessment
  ➢ Assessing how organization manages risk
  ➢ Devising fraud audit procedures
  ➢ Forensic investigation
  ➢ Interviews
  ➢ Use of electronic data tools

Raising Management Awareness

In addition to scheme discussions and fraud risk identification, management is also getting interactive awareness training
Mark P. Ruppert, CPA, CIA, CISA, CHFP, CHC, ACS
Director, Internal Audit
Conflict of Interest Administrator
Cedars-Sinai Health System
323-866-6900 office | 323-866-6901 fax
Mark.Ruppert@cshs.org