“RAISE THE RED FLAG”
AN AUDITORS WORKING GUIDE TO EVALUATING FOR FRAUD

Lynn Fountain, CGMA, CRMA
www.lynnfountain.net
fountainlynn1@gmail.com
Raise The Red Flag

- *Raise the Red Flag* combines principles and theories of fraud prevention and detection with real-world scenarios and hands-on procedures.

- Whether you are determining your internal audit department’s preparedness to support your organization’s anti-fraud efforts or investigating actual allegations of fraud, *Raise the Red Flag* provides valuable techniques and approaches you can put into practice right away.

- With professional skepticism and a questioning mind, internal auditors will know when to raise the red flag – and what to do about it.
Introduction

• The topic of fraud continues to be on the radar of investors, shareholders, and regulators.

• Recent fraud survey by Kroll Advisory found that the proportion of companies that suffered an incident was approximately 75%.

• However, ongoing technological advances in IT infrastructure, new and emerging fraud methods are continually being identified.
Introduction

• Auditors are not expected to have the specialty expertise of forensic investigators.
• Should maintain adequate knowledge of the aspects of fraud and a skeptical mind when reviewing potential violations.
• Fraud continues to evolve and auditors must stay abreast of its root causes and suggested mitigation and investigation techniques.
• Whether you are part of a large IA or small IA group, it is important for all audit professionals to understand processes that could involve fraud.
## US Fraud Stats – Kroll Global Fraud Report

| Prevalence of companies affected by fraud | 2015-2016: 75% | 2013-2044: 66% |
| Average % of revenue lost to fraud | .9% | 1.2% |
| Areas of frequent loss | • Theft of physical assets – 22%  
• Vendor, supplier, procurement - 19%  
• Information theft, loss or attack - 17% | • Management conflict of interest - 21%  
• Information theft, loss or attack - 20%  
• Theft physical assets - 20% |
| Biggest driver of increased exposure | • High staff turnover – 34%  
• Increased offshoring and outsourcing – 15%  
• Increased collaboration between firms – 14% | • IT complexity – 44% |
Agenda

• The psychology of fraud.
• Examine how past fraud incidents have impacted the auditor’s role.
• IPPF responsibilities to comply with fraud.
  • Employing COSO 2013 concepts within internal audit fraud work.
• Understanding fraud red flags - actual fraud and control gaps.
• Fraud evaluation vs. fraud investigation.
• New age digital fraud.
• Fraud reporting.
PSYCHOLOGY OF WHITE COLLAR CRIME

Connection to Fraud Triangle and Fraud Diamond
Fraud Defined

• Fraud is any intentional act or omission designed to deceive others.
  • Results in the victim suffering a loss and/or the perpetrator achieving a gain.
• Organization don’t want to believe fraud can occur in their company.
  • If fraud is identified, there is a desire to “handle it ourselves”.
• Auditors and organizations must be aware of certain psychological aspects of fraud.
## Companies affected by Fraud and Vulnerable To IT

<table>
<thead>
<tr>
<th>Types of Fraud</th>
<th>% Companies impacted in past 12 months</th>
<th>% Describing themselves as highly or moderately vulnerable</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP theft</td>
<td>45%</td>
<td>37%</td>
</tr>
<tr>
<td>Theft of physical assets</td>
<td>22%</td>
<td>62%</td>
</tr>
<tr>
<td>Vendor, supplier or procurement fraud</td>
<td>17%</td>
<td>49%</td>
</tr>
<tr>
<td>Information theft</td>
<td>14%</td>
<td>51%</td>
</tr>
<tr>
<td>Management COI</td>
<td>12%</td>
<td>36%</td>
</tr>
<tr>
<td>Regulatory or compliance breach</td>
<td>12%</td>
<td>40%</td>
</tr>
<tr>
<td>Corruption and bribery</td>
<td>11%</td>
<td>40%</td>
</tr>
<tr>
<td>Internal financial fraud</td>
<td>9%</td>
<td>43%</td>
</tr>
<tr>
<td>Company fund misappropriation</td>
<td>7%</td>
<td>40%</td>
</tr>
<tr>
<td>Money laundering</td>
<td>4%</td>
<td>34%</td>
</tr>
<tr>
<td>Market collusion</td>
<td>2%</td>
<td>26%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Perpetrators of known fraud</th>
<th>% of firms hit by fraud where someone in named group was perpetrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junior employees</td>
<td>45%</td>
</tr>
<tr>
<td>Senior or middle management</td>
<td>36%</td>
</tr>
<tr>
<td>Money laundering</td>
<td>34%</td>
</tr>
<tr>
<td>Agents and intermediaries</td>
<td>23%</td>
</tr>
<tr>
<td>Vendors, Suppliers</td>
<td>18%</td>
</tr>
<tr>
<td>JV partners</td>
<td>8%</td>
</tr>
<tr>
<td>Regulators</td>
<td>7%</td>
</tr>
<tr>
<td>Customers</td>
<td>5%</td>
</tr>
<tr>
<td>Governmental officials</td>
<td>3%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

Source: Kroll 2015/2016 Fraud Report
Top 5 Drivers of Increased Fraud Risk

Source: Kroll 2015/2016 Fraud Report

• High staff turnover – 33%
• Increased outsourcing/offshoring – 16%
• Entry to new/risker markets – 13%
• Complexity of products or services sold – 11%
• Increased collaboration between firms – 10%
Fraud Evolution

• Why does the topic of fraud seem so prevalent?
  • Major corporate downfalls,
  • New legislation/regulation,
  • High-profile cases,
  • Increased fraud awareness by consumers,
  • Enhanced information technology processes and cyber fraud,
  • More sophisticated fraudsters.
Psychological Dynamics of Fraud

• Is all fraud in today’s business world connected a financial loss?
• Ultimately it may be extrapolated to some loss but is there alternative motive possibilities?
  • Does everyone share the same moral compass?
  • How do individuals define what is right/wrong?
  • Is everything always black and white? (Should medical marijuana be legal?)
• How do perceptions impact reality?
• How do today’s pressures impact the psychology of individuals who may commit fraudulent acts?
Fraud Theories

Fraud Triangle

Fraud Diamond
Think Out of The Box

• The fraud triangle lists pressure as the first leg with opportunity and rationalization falling next.

• Today’s business environment begs the question of whether “pressure” is truly leg one.

• Individuals who perpetrate fraud may do so because they first:
  • Recognize the “opportunity” and then...
  • Find some way to “rationalize” their behavior.

• Pressure is certainly an element but may not always be the driving force.
Opportunity Considerations

• Auditors recognize opportunity can tie closely to poorly designed controls, control gaps or control avoidance.

• Control gaps create opportunity for the fraudster to take advantage of and use it to perpetuate fraud.
Opportunity Considerations

• Opportunity extends beyond this defined concept.

• Person who identifies opportunity to perpetuate a fraud through a poorly designed control does not necessarily have to be a person in a trust position or a current financial predicament.

• In original fraud triangle theory, the person must see some way he can use his position of trust to solve his financial problem with a low perceived risk of getting caught.
Added Dimension: Capability Concept

- Individuals who commit fraud have certain traits that allow them to have the capability to carry through on their actions.
- Technical skills to understand opportunity and take advantage.
- Coercion skills to convince other employees to misstate information, be complicit in/conceal the fraud, or assist with carrying out the actual fraud.
- Deception skills to lie and maintain lie over time.
Added Dimension: Capability Concept

- **Ability** to deal with the stress of continuing the deception.
- **Organizational positioning** provides opportunity not available to others.
- **Intelligence** to understand/exploit internal control weakness.
- **Ego** to believe they will not be detected.
- **Stress management** skills that allow the person to manage stress well as the fraud.
The Psychology Behind Fraud

- **Auditor lesson** - take the capability traits into consideration when attempting to prioritize or measure the fraud threat potential of identified control weaknesses.

- Inclusion of this consideration may assist the auditor in appropriately calibrating control findings.

- Consider how your organization sets their “moral compass”.

- Does management use consistent theories when determining “what is right”?
Examples – Digging Deeper

• **Auditor Inquiry:** “Tell me about how the resourcing for your department has been managed over the past few years.”

• Listen for “clues” that represent pressure on resourcing issues.
  
  • Indication of high turnover? Can you identify root cause?
  
  • Constraints to fill open positions? Impact on employees? Excessive overtime? Are employees required to on responsibilities not part of normal job?
  
  • Resourcing issues due to LT periods of PTO by certain employees – is there undue pressure on other employees?
  
  • Is there excessive overtime which may put pressure on personnel? Is there a reason why the department has not been able to add resources?
Lessons Learned

• Remember the fraud triangle!
  • Rationalization, opportunity, pressure.
• Consider implications of the fraud diamond.
• Management must make best efforts to define black vs. white. (Difficult concept).
• Leaving judgments open for interpretation will impact outcomes.
  • Without clear definition outcomes become dependent on individual moralities.
• The clearer the path......
Past Fraud Incidents

2000
- SEC alleges Enron False Filings
- Xerox falsified earnings for 5 years

2001
- SEC initiates Enron investigation
- Bristol Myers inflated revenues by $1.5M (channel stuffing)

2002
- AA Convicted and begins to fall apart
- Adelphia ($3.1B in off balance sheet loans
- AOL, Tyco, WorldCom Scandal
- CMS Energy Round Trip Trades

2003
- Massive Mutual Fund Fraud
- HealthSouth indicted on 85 counts of conspiracy
- Martha Steward
- Freddie Mac Earning Smoothing
- HCA pays $1.7B to settle 9 year fraud.

2004-2006
- Fannie Mae to restate earnings back to 2001
- Steward convicted
- Ebbers convicted
- Skilling/Lay convicted
- Broadcom and options scandal
<table>
<thead>
<tr>
<th>Year</th>
<th>Incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007</td>
<td>New Century and Bear Sterns Bankruptcy, Fannie May losses continue</td>
</tr>
<tr>
<td>2008-2009</td>
<td>WSJ accuses banks of Libor Scandal, Salyam CEO resigns and admits fraud, Madoff sentenced to 15 years</td>
</tr>
<tr>
<td>2010</td>
<td>Former Louisiana University Dean pleads guilty to fraud, BP agrees to pay $20B, Auditors for WAMU testify in front of congress</td>
</tr>
<tr>
<td>2011</td>
<td>J&amp;J agrees to $77M FCPA settlement, First company convicted under FCPA, Director at Goldman Sach, pays $10M to secure bail for charges of insider trading, Olympus scandal</td>
</tr>
<tr>
<td>2012-2013</td>
<td>Glaxo Smith Kline fraud, Capitol One fined $210M deceiving customers, Wal-Mart Allegations, Fiesta Bowl chief guilty funneling political contributions, Best Buy Scandal Libor Rigging, 911 Firefighter disability fraud claims, Target credit card hacking</td>
</tr>
</tbody>
</table>
## Past Fraud Incidents

### 2014-2015

<table>
<thead>
<tr>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Portfolio manager - SAC Capital Advisers hedge fund</td>
<td>Found guilty on 5 counts of insider trading. Resulted in convictions of 77 people.</td>
</tr>
<tr>
<td>JPMorgan Chase</td>
<td>Paid $2.6B to the U.S. govt. B. Madoff victims to settle allegations the bank failed to tell authorities about suspicions of fraud at Madoff's fund.</td>
</tr>
<tr>
<td>World Health Alternatives CEO</td>
<td>Sentenced for $41M fraud scheme.</td>
</tr>
<tr>
<td>The IRS</td>
<td>Paid $3.6B in fraudulent tax refunds to identity thieves.</td>
</tr>
</tbody>
</table>

### 2016

<table>
<thead>
<tr>
<th>Event</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 2016, Michael Hudson</td>
<td>Ordered to pay restitution of $3.1M to Frisch’s Restaurant, $505K to Travelers Insurance and $970K to the IRS for wire fraud and false IRS returns.</td>
</tr>
<tr>
<td>Logitech International</td>
<td>Paid $7.5M for fraudulently inflating fiscal year 2011 financial results to meet earnings guidance and committing other accounting-related violations during a 5 yr. period.</td>
</tr>
<tr>
<td>Three executives at Ener1</td>
<td>Paid penalties for the company’s materially overstated revenues and assets for year-end 2010 and overstated assets in the first quarter of 2011.</td>
</tr>
</tbody>
</table>
FRAUD AND THE IPPF FRAMEWORK
Auditors and the IPPF

• As internal auditors, we look to The IIA’s IPPF to guide how we can most effectively execute our responsibilities.

• The manner in which these standards are applied may vary dependent on many factors including IA’s stated charter and staffing.

• Fraud and all of its implications is one of those areas that has been managed a variety of ways by organizations.

• With the impetus of the COSO 2013 update organizations’ responsibilities for assessing the risk of fraud have become clearer.
IPPF Standards Related to Fraud

• Does your organization understand and recognize the IIA standard requirements?
• When was the last time you reviewed the requirements with your CFO/CEO or audit committee?
• Many audit committee’s and management do not fully understand and embrace the IIA standards. Why?
Auditors and the IPPF

• Internal auditors can apply the principles in COSO’s 2013 to solidify their role and how they work with management on various fraud initiatives.

• Auditors should ensure their work directly supports the Standards, including Standard 2120.A2, Risk Assessment:
  • “The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.”

• How does your organization meet Standard 2120.A2?
When Management Objects?

• Managers may perceive that including “fraud” tests during an audit reflects badly on their abilities to manage a process area.

• Including fraud tests may seem like an accusation about improper acts occurring within their sphere of control.
When Management Objects?

- IA must be able to provide management with sufficient information about why such evaluations are appropriate.
- Consider clarifying the Individual Objectivity Standard 1210.A2:
  - “Internal auditors must have sufficient knowledge to evaluate the risk of fraud and the manner in which it is managed by the organization, but are not expected to have the expertise of a person whose primary responsibility is detecting and investigating fraud.”
IPPF Standards and Auditor’s Challenge

- The IIA is not a law making/enforcing body.
  - They establish guidelines and standards that are not always recognized by all organizations.
- There are no penalties to organization’s for not following standards.
- Auditor’s do not carry a “license to practice”
- Profession is not viewed in the same manner as those that may carry a license to practice like lawyers and CPAs.
IPPF Standards

• Auditors must take a pro-active approach to educating management and the board on the IIA standards and related benefits.
• This includes ensuring management understands the standards related to the requirements for fraud evaluations.
• HOWEVER – Internal Audit must ensure they are qualified and prepared to engage in the various types of fraud related work.
  • Don’t just do it because it sounds interesting.
• What role should IA play?
1. Clarify to management the IPPF standards.
2. Establish internal procedures to support internal auditors when executing on competency and professional skepticism.
3. Have a structured fraud methodology in place for internal audit.
4. Ensure professionals assigned to fraud work have the organizational knowledge and perceived standing to adequately execute on their professional skepticism.
5. Never send an auditor on a fraud interview alone.
6. Encourage auditors to check the facts twice and assess evidence without being overly critical or suspicious.
7. Follow all trails of evidence.
Potential Steps

• Clarify to management the IPPF standards.
  • Internal auditors have guidelines just like lawyers and doctors.
  • Ensure your group has the ability to meet the competency standards related to fraud evaluations.
    • If you don’t have adequate qualifications, execution may be a difficult thing.
• Establish internal procedures to support internal auditors when executing on competency and professional skepticism.
Internal Steps

• Have a structured fraud methodology in place for internal audit.
  • *Methodology* should define how, when, why etc. you will get involved with issues that may be involved in fraud.
  • *Protocol* should include communication procedures with management, the board and any regulatory authorities.
  • *Involve* your Legal group – Know the rules of evidence.
  • *Understand* the difference between identifying red flags and identifying fraud.
  • *Know* the difference between doing a fraud investigation versus a fraud evaluation.
  • *Understand* the types of fraud prevalent in your industry.
Internal Steps

• *Ensure* professionals assigned to fraud work have the organizational knowledge and perceived standing to adequately execute on their professional skepticism.

• *Acknowledge* not everyone uses the same approach.
  
  • Not everyone will come to the same conclusion or make the same intuitive interpretation.
  
  • Quickest way to stop professionals from exercising a questioning mind is to tighten the rope every time a misjudgment occurs.
Internal Steps

- **Never** send an auditor on a fraud interview alone.
  - Even an experienced auditor, can have a he said/she said experience.

- **Encourage** auditors to check the facts twice and assess evidence without being overly critical or suspicious.
  - Executing professional skepticism requires employing a balance of questioning mind and ensuring facts are correct.
  - Management may distrust observations of auditors who jump to conclusions or do not have all the facts.
Internal Steps

• **Follow all trails of evidence.**
  - It can be tempting to accept an answer at face value.
  - Remember, one person’s perception of black/white may be different than another person’s.
  - It is not sufficient to interview only top level executives.
  - If you question accuracy of the information, you must use due care to follow up on that question.
  - Important to independently/objectively pursue all avenues of inquiry.
INTERNAL AUDIT’S RESPONSIBILITY
Determining Your Role

• **Consider Fraud Awareness:**
  • Fraud awareness within an organization assists in minimizing collusion activities.
  • Personnel become aware of the consequences of becoming involved in the unacceptable behavior.
  • Lack of awareness tactics is like a silent “acceptance” of behavior.
• To execute fraud awareness roll, auditor’s must understand the business.
  • Understand the many types of fraud that can occur in your industry.
  • Obtain statistics on fraud incidents and emerging trends.
Internal Audit’s Role

• What are the keys to right-sizing IA’s responsibility for fraud activities?
  • In today’s world of doing work faster, more efficiently, and with fewer resources, it is difficult to balance requirements.
  • The unexpected often occurs and resources get pulled in different directions.
  • Participation in fraud work can be one of those areas where the unexpected occurs and time allocation is not sufficient.
  • Consider these steps and when defining your role and time allocation.
Types of Roles

• Consider the potential that there may be a “**required role**” and a “**potential role**” for IA when it comes to fraud work.

  • **Required role:** Meet the intent of the IIA Risk Assessment Standard.
  • **Potential role:** Involvement in fraud evaluations, investigations or holistic risk assessments.
Required Role

• Meeting Standard 2120.A2: *The internal audit activity must evaluate the potential for the occurrence of fraud and how the organization manages fraud risk.*

• Consider this means more than periodic evaluation through the annual audit assessment.

• What would be involved in fulfilling the required role?
Potential Steps: Required Role

- **Internal audit must have relevant methodologies in place related to the following:**
  - Inclusion of fraud risk evaluation within the *annual audit plan*.
  - Provide direction for evaluation of the potential for fraud risk within each *individual audit*.
  - Include a protocol for auditors to follow when red flags are identified either during an audit or through another independent manner.
Potential Steps: Required Role

- **Internal audit must provide adequate support for staff including:**
  - Ensure staff have required training and understanding to evaluate the potential for fraud red flags.
  - Ensure staff can adequately execute professional skepticism when executing projects.
  - Ensure staff understand the sensitivities of the topic and the proper communication protocols.
Defining Potential Role

• Does the IA department have relevant personnel expertise?
  • Does departmental CFE have the “experience” to be involved in significant fraud investigations?
• Is there a protocol for how time will be assigned and reallocated in the event a fraud project arises?
  • Will completion of the audit plan be impacted?
  • How does management/audit committee view IA’s role?
• What does your IA charter say?
• What is the legal department’s role and who manages the hotline?
• Is there a clear definition of variance between fraud evaluations/fraud investigations and requirements of each?
Steps: Potential Role

1. Ensure role is agreed to by management and the AC.
2. Develop an internal **holistic fraud methodology** that differentiates between assessments, evaluations and investigations.
3. Define requirements for each type of fraud work. (e.g.: auditor skill set, background, need for specialty experience).
Steps: Potential Role

4. Identify how projects will be resourced (e.g. internally, externally).

5. Establish a pre-defined communication protocol for various types of fraud work. (Know when an evaluation, investigation or assessment should be moved to the next step).

6. Have a defined methodology for project documentation. (Know when to consult with legal).
Steps: Potential Role

7. Ensure professionals in IA assigned to fraud work have the required experience, organizational knowledge and perceived standing to adequately execute on their professional skepticism.

8. Ensure auditors have the proper support (resources and moral) related to the project.
Steps: Potential Role

9. Encourage auditors to check the facts twice and assess evidence without being overly critical or suspicious.
   • Executing professional skepticism requires employing a balance of a questioning mind and ensuring all facts are correct.
   • Management may distrust observations of auditors who jump to conclusions or do not have all the facts.
Right-Sizing Steps

1. **Clarify your department charter.**
   - Clarify the role IA will play in fraud awareness and detection.
   - Determine how that role will work within your audit plan.

2. **Validate that the AC and management agree with role.**
   - Ensure roles as identified in the charter are fully understood by the AC and management.
   - If there is a “drop everything” perception when it comes to the need for IA to be involved in a fraud investigation, this must be clearly understood by management and the board.
3. **Evaluate the need for fraud specific auditors.**
   - If the company is in a high risk fraud industry, IA may have dedicated fraud auditors.
   - When planning workload, don’t fall into trap of only considering past hours. Circumstances change, business evolve. Time allocation resources may need to change.

4. **Be proactive when identifying the need for outside experts.**
   - If your charter includes involvement in fraud investigations, but IA does not typically have resources for the effort, ensure the charter provides the ability to enlist outside experts.
Right Sizing Steps

5. **Assess need to use other subject matter experts.**
   - Assistance of individuals from other business areas.
   - Establish relevant relationships up front. (Subject matter experts)

6. **Consider allocation of “specialized hours” as a placeholder.**
   - Is this “padding” the audit plan?
   - The allocation of “specialized hours” can include compliance issues, regulatory issues, or fraud investigations.
   - Ensure you have adequately assessed your potential needs for the audit plan and support it with your fraud risk assessment, past experience, and evaluation of ongoing and emerging risks in your business.
COSO 2013 AND THE CRITICAL LINK TO FRAUD
COSO and Fraud

• When examining the COSO’s definition of CE; a key phrase helps understand how and why the topic of fraud can impact an organizations control environment and culture.

  • “The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.”
COSO and Fraud

• When executing your fiduciary duty related to fraud evaluations, remember concepts of the IIA standards as well as COSO 2013 and principle 8.

• Challenge: How do you meet the Principle on Fraud related to COSO 2013.
COSO and Fraud

- Key phrase
  - “influencing the control consciousness of its people”.
- Phrase recognizes some of the attributes identified in the fraud triangle - rationalization and pressure.
- Another emerging philosophy is the fraud diamond and requires the consideration of “capability” as a component.
COSO 2013 Principles

Risk Assessment

8. Organization considers the potential for fraud in assessing risks to the achievement of objectives.

Points of Focus
- Considers various types of fraud
- Assesses incentive and pressures
- Assesses opportunities
- Assess attitudes and rationalizations

- Principle 8 possesses the most direct tie to management’s responsibility for fraud processes.

How do fraud concepts play a role?
Principle 8 - Point of Focus

- Does your organization assess the potential for all types of fraud including:
  - Fraudulent reporting (financial and operational),
  - Corruption from misconduct,
  - Incentives/pressures,
  - Opportunities for unauthorized acquisition, use or disposal of assets or asset loss,
  - Altering of the entity’s reporting records,
  - How management and other personnel might engage in or justify inappropriate actions.
FRAUD RED FLAGS – ACTUAL FRAUD VS. CONTROL GAPS
Variance

• **Fraud Red Flags** are warning signs that may indicate a higher fraud risk.
• They are **NOT** evidence that fraud has occurred.
• A control gap does not mean “fraud” occurred.
• Internal auditors must recognize the difference and be cautious when evaluating and reporting on control gaps vs. fraud red flags.
• If it is a red flag – can you identify the potential impact and likelihood?
  • How will you evaluate whether there could be potential misdoings or whether it is an internal control gap?
Fraud Red Flags

• Financial stability threatened by economic/industry/operating conditions.
• Recurring negative cash flows/inability to generate cash flow.
• Excessive pressure on personnel to meet financial goals.
• Significant accounts or operations in tax-haven jurisdictions.
• Complex/unstable organizational structure.
• Inadequate or ineffective internal controls.
• Excessive interest by management in maintaining or increasing stock price/earnings trend.
• Management failure to correct known reportable conditions.
• Recurring attempts by management to justify marginal/inappropriate accounting.
Fraud Red Flags

• Unusual/suspicious items involving accounting records.
  • Missing documents, excessive voids or credits.
  • Common names, telephone numbers, or addressees.
  • Counterfeit/alterations of documents.
• Management overrides, top sided entries.
• JE adjustments at or near end of reporting period.
• Unusual requests made near close periods.
• Significant estimates that deviating from trends.
• Transactions outside normal course of business.
• Shake the trees !!!
Anti-Fraud Controls

• The presence of anti-fraud controls is correlated with significant decreases in the cost and duration of occupational fraud schemes.

• Victim organizations that implement any of the common anti-fraud controls, experience lower losses and time-to-detection than organizations lacking.

• Don’t close your eyes…..don’t assume it is someone else's worry....speak up.....
EVALUATIONS VS. INVESTIGATIONS
Evaluation vs. Investigation

• Evaluations – systematic examinations of an area’s merit, worth and significance.
  • Uses specific criteria governed by a set of standards.
  • Primary purpose is to gain an insight into an area to enable more in-depth analysis.
  • Resulting analysis will help identify root causes and gaps in controls.

• Investigation – the scientific method of gathering and examining information about a particular event to determine and finalize an assessment.
Evaluations

• Evaluations may occur in the normal course of an audit:
  • Anomalies in a process are identified and further review is warranted.
    • In these instances, the evaluation focuses on a specific process area or possibly even a group of individuals.
  • Observations are result of individual audits.
    • If fraud risk is included in an audit, evaluation may identify the need for further targeted research.
Evaluation Considerations

- Complexity of the process.
- How the transaction flows.
- Sophistication of the system.
  - Legacy systems
  - New Systems
- Has the process are experienced past issues that appear to be systematic or are not addressed?
- Understand the control environment of the process and personnel involved?
Investigation

• Investigation may entail:
  
  • Interviews/observations designed to gain relevant evidence to prove case facts.
  
  • Background check of alleged perpetrators.
  
  • Subpoenas for specific documentary evidence: bank records, title searches, other legal documents not readily accessible.
  
  • Asset searches to determine ownership issues.
  
  • Record analyses to evaluated documentation of information related to the allege act.
  
  • Surveillance of specific process or individuals.
  
  • Interrogation of specific personnel who may have knowledge of the incident.
THE NEW AGE DIGITAL FRAUD
The New Age Digital Fraud

- Digital fraudsters are one step ahead. Fraudsters take advanced steps with knowledge from the digital world.
- Digital fraud has created seamless boundaries which increase the perpetuation of fraud.
- What is digital fraud?
  - Web crawlers, chat room or malicious bots,
  - Automated programs that run over the internet
  - Digital networks that transmit voice, video, data
  - Identify theft and credit card theft, security code hacking
  - E-mail scams,
  - The list is endless...
  - See Appendix
Cyber attack realities

• No turnkey cyber solution.
• Build a fortress but secure it from the inside.
  • Noted lack of investment in internal monitoring systems.
• Data loss is a symptom of a bigger problem to be investigated.
  • Must investigate to find the source and to explain to the regulator how you have fixed the problem.
• The attacker often stays in the system after the attack.
  • The goal of online attackers is to stay within a system for as long as they can. Attacked systems must be monitored.
• Cyber fatigue is real, but not an excuse for inaction.
  • Inability to address will encourage the fraudsters to continue to move forward.
Cryptocurrency

• Cryptocurrency goes by many generic names.
• It is often referred to as virtual currency.
• The simplest definition comes from Fin CEN:
  • “‘virtual’ currency is a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.”
  • Transaction anonymity and irreversibility of payments, have made these currencies attractive to cyber-criminals, drug dealers, money launderers and those involved in global fraud.
• Common example is bitcoins.
Bitcoin

• Bitcoins are not issued by a central bank or government, but are purchased from a Bitcoin exchanger.
  • Exchangers accept conventional currencies and exchange them for Bitcoins based on a fluctuating exchange rates.
• Bitcoins are stored in a digital wallet associated with “the user’s Bitcoin ‘address,’ analogous to a bank account number, which is designated by a complex string of letters and numbers.”
• A Bitcoin transaction, which takes the form of a transfer of value between Bitcoin wallets, is recorded in a public ledger called a “block chain”.
Benefits of Bitcoin for Fraud

• Virtual currencies represent a challenge for law enforcement.
• They pose the risk of criminal activities, including money laundering, trading in illicit drugs and global fraud.
• The following traits make virtual currencies attractive to the fraudster:
  • Anonymity of transaction
  • Global reach
  • Speed
  • Non-reversible
  • Difficult for authorities to track
Identity Theft

• Broadly defined as the use of one person’s identity or personal identifying information without the persons permission.
• Can be committed against an individual or organization.
• The federal criminal definition of identity theft is when someone “knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit fraud.
Identity Theft

• Until 1996, identity theft was not recognized as a crime at the state level.
• Arizona was the first state in the United States to pass laws against identity theft.
• On May 10, 2006, President Bush issued Executive Order 13402 that established the Identity Theft Task Force.
• Many types of identity theft:

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Criminal Identity Theft</td>
<td>Medical Identity Theft</td>
</tr>
<tr>
<td></td>
<td>Insurance Identity Theft (Auto, Homeowners, Life, Business, Malpractice)</td>
</tr>
<tr>
<td></td>
<td>Child Identity Theft</td>
</tr>
<tr>
<td>Professional Identity Theft</td>
<td>Business Identity Theft</td>
</tr>
<tr>
<td></td>
<td>New Account Fraud</td>
</tr>
<tr>
<td></td>
<td>Account Takeover</td>
</tr>
<tr>
<td>Cloning</td>
<td>Credit Card Identity</td>
</tr>
<tr>
<td></td>
<td>Synthetic Identity</td>
</tr>
<tr>
<td></td>
<td>Government Benefits Theft</td>
</tr>
<tr>
<td>Government documents identity theft</td>
<td>Employment Fraud</td>
</tr>
<tr>
<td></td>
<td>Utility Fraud</td>
</tr>
<tr>
<td></td>
<td>Bankruptcy</td>
</tr>
<tr>
<td>Tax Return Identity</td>
<td></td>
</tr>
</tbody>
</table>

Copyright 2017 - Lynn Fountain - No duplication
Digital Fraud Summary

• Digital fraud is advancing faster than the business world prefers.
• Organizations must be diligent in understanding cyber threats and the various types of digital fraud that can occur.
• Organizations should establish a digital fraud risk inventory.
  • Work with management and the CIO to understand what areas the organization can be exposed to digital fraud.
• Ensure relevant focus is placed on this emerging risk.
  • If you don’t have the resources – find them.
• Be cautious when using outsourced providers and relying on SSAE16 Service Organization Control Reports (SOC Reports).
FRAUD REPORTING
Conceptual Reporting Thoughts

• Building a framework for a final reporting protocol is beneficial and can assist in ensuring processes follow consistent and established steps.
  • Forget the “F” word
  • Revisit the facts
  • Account for the detail
  • Understand any political or sensitive reporting implications
  • Don’t “accuse” unless you can actually prove.
Reporting Considerations

• Formal reporting of investigative process that may have implications of fraud will be sensitive. Auditor must remember:
  • Formal reports are retained on information systems.
  • Consider confidentiality requirements.
  • Written/formal reports are seen by BOD/legal counsel. Like the internet, reports written exist for perpetuity.
  • A fraud evaluation completed by IA may not lend itself to normal reporting protocols.
  • Determine best method of communication of the facts.
    • May be in a formal memo, PowerPoint or even formal verbal presentation.
Reporting Considerations

- Will the issue have legal implications?
- Does any part of the evaluation come under legal privilege?
- Is the report discoverable by outside parties?
- Does the evaluation require a formal written summary as a source of evidence?
- Who are the recipients of the report?
Lessons Learned

• Remember the fraud triangle!
  • Rationalization, opportunity, pressure.
• Consider implications of the fraud diamond.
• Management must make best efforts to define black vs. white. (Difficult concept)
• Leaving judgments open for interpretation will impact outcomes.
  • Without clear definition outcomes become dependent on individual moralities.
• The clearer the path......
APPENDIX

TOP 10 SCAMS OF 2017
2017 Top Scams

- **Tech support scams**
  - Caller ask for access to your computer to fix a problem.

- **Fake/counter fit merchandise schemes**
  - Scammers set up generic online stores selling name brand items or mimic websites of big name brands.
  - Scammers sell fake or counterfeit products at significantly reduced prices designed to attract buyers looking for big deals on name brand merchandise.

- **Pets for Sale Scams**
  - Fake websites claiming to be associated with pet adoption/animal nurseries. Offer pets for adoption or sale at prices significantly below the norm.
  - Victims told they must pay for at least the insurance, shipping and other services for processing and delivering the pets.
  - Victims are required to make their purchases and/or pay fees with non-returnable cash-like forms of payment.
2017 Top Scams

• **Grant Scams**
  
  • Acquire consumer personal details from unsuspecting advertising agencies who run lead generation campaigns targeting consumers in need of loans.
  
  • Then contact the people from these lists and claim they represent the U.S. government.

• **Collection Agency Scams**

  • Resenting a fake collection agency, scammers make cold calls to victims and threaten lawsuits or embarrassing on-the-job confrontations unless the victims start making payments.
2017 Top Scams

• **House/Vacant property rentals**
  - Scammers advertise properties they don't own on classified ads websites, such as Craigslist.
  - Payments are requested via non-returnable methods like Money gram, Western Union, Vanilla and wire transfer.

• **Payday Loan Scams**
  - Rely heavily on legitimate leads gathered by payday loan affiliate website companies or advertising agencies.
  - Once the information is gathered, they sell it to other companies and re-sell it over and over until a scamming company posing as a legitimate company gains access to it.
2017 Top Scams

• **Timeshare Resale Scams**
  - Tell victims they have buyers or renters, ready to take timeshare.
  - Require an upfront fee to move forward with the process.
  - Scammers give victims a wide range of reasons for the fee, including appraisal, marketing analysis and fees.

• **Dating and relationship scams**

• **Work from home inspecting and shipping merchandise**
  - Scammers set up professional-looking websites and claim that the sites are owned by shipping and logistics intermediaries.
  - Once virtual workers are hired, scammers use stolen credit cards to purchase merchandise and ship it to their new work-at-home "employees" with instructions on how to open the packages, inspect the merchandise and ship it elsewhere.
TYPES OF DIGITAL FRAUDS
Digital Scams

• Phishing
  • Gain PI, (usernames, passwords, SS numbers, credit card numbers) for purposes of identity theft.
  • Accomplished by using fraudulent e-mail messages that appear to come from legitimate businesses.

• Whaling
  • Phishing after very large scores.
  • Done when high net worth individuals are targeted or when corporations are targeted in order to get credit card information from a large number of customers at one time.
Digital Scams

• Vishing
  • Obtaining PI over the phone. Call informing individuals they have won a prize but they need to pay taxes or shipping fees.
  • Fake a call from a local business where an individual shops to verify credit card information on a transaction.

• Pharming
  • A virus or malicious software secretly loaded onto the victim’s computer and hijacks the web browser.
  • When the victim types in the address of a legitimate website, they are rerouted to a fictitious copy of the site without realizing it.
Digital Scams

• Social Media
  • Uses social media websites to gather information on victims.
  • Friends and relatives inadvertently post the victim’s PI on their social media sites.

• Hacking
  • Steal PI from government and business computers.
  • Employees copy the PI contained on their employer’s computers and sell the information.

• Fraudulent Recruiter Scam
  • Retrieve the victims’ contact information from their online resumes and send them e-mails posing as recruiters.
Digital Fraud

• Pretexting
  • Perpetrator poses as legitimate government official or member of legitimate business and calls victims asking for PI.
  • Convince victim information is needed to complete a transaction and that someone is trying to access their account. Encourage victim to verify PI.

• Spoofing
  • Fraudulent e-mail activity where sender’s address or other parts of the e-mail header are altered to appear the e-mail originated from a different source.
Digital Frauds

• Skimming
  • Attaches a device to a machine that records the information on the card’s magnetic strip.
  • Information can be imprinted on other cards.
  • Miniature cameras used to capture the PINs entered by the victims.

• Free Public Wi-Fi
  • Set up free public Wi-Fi networks in airports, near hotels, and in other public places.
  • Information on victim’s computers and other electronic devices is hacked.
  • Can gain control of e-mail accounts, bank accounts, social media accounts, and so on.
Digital Fraud

• Malware
  • Placed on computers or cell phones to hijack the computers, steal data, or encrypt the data for ransom.

• Data Breeches
  • Stealing data from computer systems belonging to companies, governmental units, and even not-for-profit organizations.
  • Large amounts of information are stolen in a short amount of time.
RAISE THE RED FLAG

Chapter Outline
Raise The Red Flag - Outline

• Chapter 1: The IPPF Framework and the Auditors responsibility
  • Fraud and the IPPF.
  • Value added roles in fraud prevention for the internal auditor.
  • Communicating on IAs duty related to fraud processes.
  • Right-sizing IA’s responsibility for fraud detection.
  • Monitoring for fraud and understanding the extent of the IA audit role.

• Chapter 2: Fraud and connection to the CE and COSO 2013.
  • The impact of fraud on the Control Environment and corporate culture.
  • Determining impact of fraud issues on the identification of deficiency status.

• Chapter 3: The IA’s dilemma when investigating internal fraud.
  • Managing the request process for internal investigation.
  • Determining whether IA should be involved in the investigation.
  • Methods to employ for internal investigations.
Raise The Red Flag - Outline

• **Chapter 4: Conducting a Fraud Risk Assessment for the Company.**
  • Evaluating the corporate culture to prepare for a fraud risk assessment.
  • IA’s role in facilitating a proper fraud risk assessment.
  • Steps in identifying potential fraud scenarios and their impact/likelihood

• **Chapter 5: Including fraud analysis and evaluation within each audit.**
  • Techniques for conducting a fraud risk assessment for individual audits.
  • Determining relative significance and impact of identified inappropriate behavior.

• **Chapter 6: Evaluation vs. investigation**
  • Understanding when an issue moves from evaluation to investigation.
  • Determining IA’s ongoing role when issue analysis turns to investigation.
  • Methods for communication issues to management and the board.
Raise The Red Flag - Outline

• **Chapter 7: Is data analysis sufficient?**
  • The role of data analysis in ongoing monitoring for fraud.
  • Determining how, what, where and when to enhance monitoring.
  • Supporting management’s monitoring process.
  • How to analyze the effectiveness of Fraud Prevention programs.

• **Chapter 8: COSO 2013 – The critical component of monitoring activities**
  • Managing the expectation of “wait till the auditors come in”.
  • What to do when management fails to report inappropriate activity.
  • Ensuring operational monitoring is effectively executed.

• **Chapter 9: Reporting procedures for an effective fraud program**
  • How much reliance to place on the whistleblower hotline.
  • Internal reporting and legal privilege.
  • Reporting issues to the board and audit committee.