



The North Carolina Office of the State Controller

Internal Controls:

Fraud

It's Everywhere....

Prevention and Detection -What
Can Be Done.....

**Whistleblowing and the
new race to report -**

The impact of the Dodd-Frank Act
and final U.S. Federal Sentencing
Guidelines



May 22, 2012

Presented by: James H. Cottrell, Jr. ("Chip")
Partner - Deloitte LLP

Agenda



Fraud:

- What do you mean by Fraud?
- Occupational Fraud
- Ten Things About Fraud
- Preventing & Deterring Fraud
- Fraud Risk Governance Considerations

Whistleblowing and the new race to report:

- The Dodd-Frank Act
- Final U.S. sentencing guidelines
- Ten things about whistleblowing
- Questions and Answers
- Bonus – Conducting a Fraud Risk Assessment



How Fraud Hurts Government: ACFE Video



[how-fraud-hurts-government.wmv](#)

3



What do you mean by Fraud?

4



Understanding Fraud

How expensive is fraud?

- According to the Association of Certified Fraud Examiners (ACFE), organizations in the US lose approximately 7% of their annual revenues to fraud
- Applied to the US GDP, this amounts to a collective \$994 billion in fraud losses each year



Source: ACFE, 2008 Report to the Nation on Occupational Fraud & Abuse

5



Understanding Fraud (contd.)

What is fraud?

- “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets”

Major fraud types

- Fraudulent Financial Reporting (Financial Statement Fraud)
- Misappropriation of Assets
- Bribery & Corruption

What do you think is the most common fraud type?

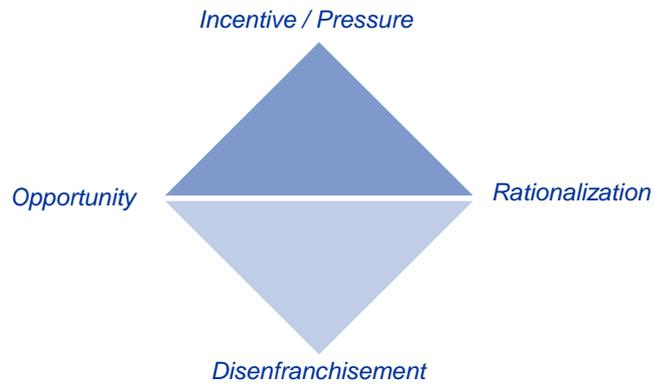
The most expensive?

6



The Fraud Triangle

Why do people commit fraud?



How might the psychological drivers of the Fraud Triangle be exacerbated by an economic downturn?

7



The Typical Fraudster

Age

- More than half of frauds are committed by people over 40
- Schemes perpetrated by people in their 50s resulted in a median loss of \$500,000 (twice the amount of any other age bracket)

Gender

- 59% of frauds are committed by men
- Median losses associated with men are twice as high as women

Rank

- 40% of frauds committed by employees; 37% by managers
- The most expensive frauds were committed by owners/executives (\$834,000 median loss)

8



The Typical Fraudster (contd.)

Department

- The accounting department was responsible for 29% of frauds
- The legal department and executive/upper management were responsible for the greatest fraud losses (almost twice the losses of other departments)

Acting alone or in collusion?

- Two-thirds of fraudsters act alone
- Schemes involving two or more individuals resulted in a median loss over four times higher than frauds committed by a single perpetrator

Criminal background?

- 87% of fraudsters have never been charged with a crime

Source: ACFE, 2008 Report to the Nation on Occupational Fraud & Abuse

9



Behavioral Red Flags

What do you think are some indicators that someone may have committed a fraud?



10



Behavioral Red Flags (contd.)

- Living beyond means
- Personal financial difficulties
- Extreme risk taker (rule breaker)
- Control issues
- Personal problems (divorce, addiction, legal problems, instability)
- Unusually close association with vendor/customer
- Irritability and defensiveness
- Refusal to take vacation
- Excessive pressure from within organization

11



Occupational Fraud

12



Occupational Fraud

What is Occupational Fraud?

- “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of the employing organization’s resources or assets.”



The typical organization loses 7% of its annual revenues to occupational fraud.

Source: 2008 ACFE Report to the Nation on Occupational Fraud & Abuse

13



Occupational Fraud (contd.)

The three primary categories of Occupational Fraud are:

1. Asset misappropriation

Intentional acts by management or employees to steal or misuse an organization’s resources.

2. Financial statement fraud

Intentional acts by management designed to misstate financial performance in order to deceive financial statement users.

Source: 2008 ACFE Report to the Nation on Occupational Fraud & Abuse

14



Occupational Fraud (contd.)

3. Corruption

The most common bribery and corruption schemes include:

Bribery - Giving or receiving something of value to influence a transaction

Illegal Gratuity - Giving or receiving something of value after a transaction is completed, in acknowledgment of some influence over the transaction

Extortion - Demanding a sum of money (or goods) with a threat of harm (physical or business) if demands are not met

Conflict of Interest - Employee has an economic or personal interest in a transaction

Kickback - A vendor give part of an overbilling to a person who helped facilitate or allow the transaction.

Corporate Espionage - Theft of trade secrets, theft of intellectual property, or copyright piracy

Source: 2008 ACFE Report to the Nation on Occupational Fraud & Abuse

15



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

16



Types of Occupational Fraud & Abuse

Category	% of all Cases	Median Loss
Asset Misappropriation	86.3%	\$135,000
Corruption	32.8%	\$250,000
Fraudulent Statements	4.8%	\$4,100,000

Percent of cases exceeds 100 percent due to cases spanning several categories.

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

17



Detection of Fraud



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

18



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.
Copyright 2010, ACFE. Used with permission.

19



Ten Things About Fraud

20



10 Things About Fraud

1. Look around – 1 in 10 of your colleagues are fraudsters
2. Most fraudsters are men - women smaller \$'s
3. Average duration of 18+ months
4. It is just as pervasive in the public sector as in the corporate world
5. 40% includes collusion with others in the organization
6. 25% includes collusion with others outside of the organization
7. Fraud, Waste and Abuse = Fraud
8. Most of us will participate in frauds either knowingly or unknowingly
9. Current and expected economic environment increases rationalization
10. The appropriate tone in the organization from leadership and management is the number 1 deterrent

21



We miss fraud because.....

- Inconsistent application of professional skepticism
- Over reliance on representations of colleagues
- Lack of awareness or failure to recognize that an observed condition may indicate a fraud
- Lack of experience
- Personal relationships

22



Preventing & Deterring Fraud

23



Preventing & Deterring Fraud

Strong fraud risk management makes good business sense:

Enhanced ethical culture (“tone at the top”)

Improved employee sensitization to and awareness of fraud

Increased reporting of potential frauds and other ethical issues

Strengthened risk management strategy

Reduced financial and reputational losses due to fraud

Reduced costs of responding to fraud

- investigations, legal costs, and regulatory enforcements

More effective corporate governance and the potential for improved governance ratings

Compliance with applicable US and other regulatory requirements

- see next slide for examples

24



Some Anti-fraud/Anti-corruption Compliance Drivers



25



Antifraud Programs and Controls: COSO Approach



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

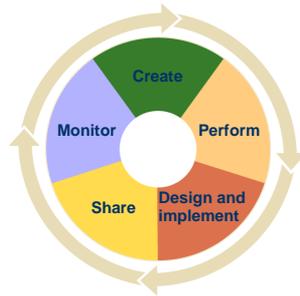
26



Creating a Control Environment

Areas for consideration:

- Tone at the top
- Code of conduct/ethics
- Fraud control policy and effective oversight
- Whistleblower hotline
- Investigation policy and procedures
- Integrating fraud risk management into overall enterprise risk management plans



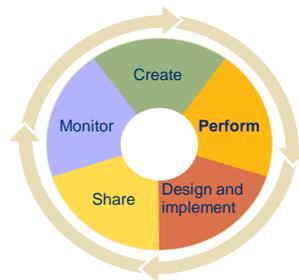
27



Performing Fraud Risk Assessments

Areas for consideration:

- Evaluate fraud risk factors
- Identify possible fraud schemes & scenarios
- Prioritize identified fraud risks
- Consider management override of controls (e.g., journal entries, bias of estimates, non-routine transactions)
- Evaluate whether mitigating controls exist and are effective
- Document the risk assessment process and conclusions
- Conduct periodic reviews and updates



28



Designing and Implementing Fraud Controls

Areas for consideration:

- Link or map identified fraud risks with control activities
- Entity-level controls
 - Fraud awareness training
 - Code of conduct
 - Background investigations
 - Employee surveys
- Process-level controls
 - IT access controls
 - Segregation of duties
- Controls can be preventive or detective



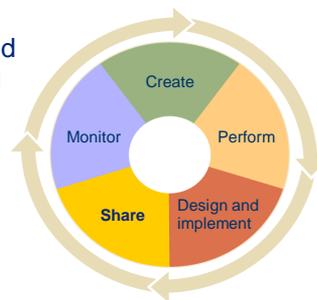
29



Sharing Information and Communicating

Areas for consideration:

- Communication of the tone at the top
- Incorporate information on antifraud programs into the corporate communications program
- Fraud education and awareness training
- Define each employee's responsibilities in relation to the Organization's antifraud program
- Knowledge management plan to collect and share identified fraud risks, suspicions and allegations about fraud, and remediation efforts



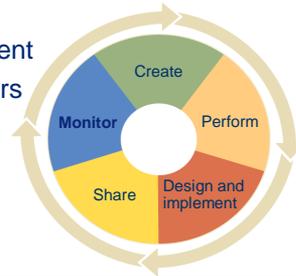
30



Monitoring Activities

Areas for consideration:

- Undertake independent evaluations of antifraud controls
- Enable continuous monitoring activities that will alert management to potential fraud
- Define an escalation policy
- Incorporate findings into fraud risk assessment process
- Maintain awareness of external environment
- Proactive fraud auditing by internal auditors
 - Data analysis
 - Email analysis
 - Exit interviews



31



Fraud Risk Governance Considerations

32



Fraud Risk Governance

- Governance starts with senior leadership
- Strong leadership practices include:
 - Access to multiple layers of management
 - A thorough understanding of fraud risk
 - Effective whistleblower hotline
 - Independent nomination process
 - Effective senior management evaluations
 - Emphasis on internal effectiveness of the board/ trustees
 - evaluations and executive sessions

33



Fraud Risk Governance (contd.)

- Rising risks and penalties relating to fraud and corruption require an organizational response
- Leadership and senior management need to direct anti-fraud and anti-corruption activities
- Strong governance is the foundation
- A fraud control policy is an important tool in fraud risk governance
- Summarizes the organization's strategic approach to managing the risk of fraud to the business through an integrated approach to antifraud programs and controls

34



Elements of An Effective Fraud Control Policy/ Strategy

- Full commitment of leadership and organization
- Fraud awareness training policy
- Roles and responsibilities
- Conflict of interest disclosure process
- Periodic affirmation process
- Fraud risk assessment and control planning
- Reporting procedures
- Investigation, discipline and prosecution
- Corrective action, where appropriate

35



Management Override of Controls

How can **those charged with governance** help address the risk of Management Override?

- Strengthening their understanding of the business and its operating environment
- Active involvement in understanding and evaluating the fraud risk assessment
- Involvement from many members for a cross-section of perspectives and comments
- Collaboration with internal audit to understand the entity and its unique fraud risk factors
- Conduct its own brainstorming discussion, and include a specific discussion about how management might attempt to override existing controls
- Collaborate with internal audit to ensure that processes or controls identified as susceptible to override are tested

36



Why Proactively Set the Tone?

- Determinants of ethical behavior
 - Behavior of superiors
 - Behavior of peers
 - Industry ethical practices
 - Society's moral climate
 - Formal organizational policy
- Reduce opportunities for employees to rationalize committing fraud to “help the Organization”
- Override potential negative influences on the tone
- Attract and retain employees by creating a favorable workplace environment

37



Management Consideration: Tone at the Top

- There is international research to confirm that the behavior of managers and in particular senior executives, is far more influential on staff behavior than is formal policy.
Souter, McNeil and Molester
- Research has shown that the ethical standards of an organization impact on staff job satisfaction, commitment to the organization, turnover and levels of stress experienced by staff.
Ethics: The Key to Good Management, Independent Commission Against Corruption (ICAC) Research Report
- Research findings suggest that the “ability to see and respond ethically may be more related to attributes of (organizational) culture than to attributes of individual employees.”
Chen, Sawyer & Williams

38



Measuring the Tone at the Top

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

39



Whistleblowing and the new race to report –An Introduction.....

40



Section 922 of The Dodd-Frank Act

Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act):

- Created awards of 10–30 percent of monetary sanctions for whistleblowers who report to the Securities and Exchange Commission (SEC) original information leading to securities law enforcement actions that recover more than \$1 million

These rewards are expected to increase the number of allegations that organizations will be expected to investigate.

41



SEC final whistleblower program rules

The Dodd-Frank whistleblower provisions became effective in July 2010. The SEC's final rules to implement those provisions were approved on May 25, 2011. The final rules include:

- Provisions designed to encourage, but not require, employees to use their Organization's internal reporting systems. An employee who reports information first through internal Organization channels and then to the SEC within 120 days would be prioritized for a reward based on the earlier, internal, reporting date. In determining the amount of each reward, the SEC will consider whether a whistleblower effectively used, or hindered, a Organization's internal compliance program. Whistleblowers who only report internally may still be eligible for a reward; the SEC will give credit to a whistleblower when a Organization passes their reported information to the SEC .
- Clarification of a number of definitions and program requirements as well as descriptions of the procedures for submitting information to the SEC and making an award claim after an action is brought.
- Clarification of the whistleblower anti-retaliation protections.
- Source: Final Rule: [Implementation of the Whistleblower Provisions of Section 21F of the Securities Exchange Act of 1934 \(May 25, 2011\)](http://www.sec.gov/rules/final/2011/34-64545.pdf) <http://www.sec.gov/rules/final/2011/34-64545.pdf>

42



Increase in whistleblower tips

The Dodd-Frank Act requires the SEC to establish a ***new, separate office within the agency to administer and enforce the whistleblower provisions***. This new office ***will report annually to House and Senate committees on its activities***, whistleblower complaints, and the SEC's response to such complaints.

According to the August 16, 2010 article "New whistleblower reward program has law firms gearing up" in *The Washington Post*, the whistleblower provisions of the Dodd-Frank Act, which provide a substantial incentive to report financial fraud, are ***expected to generate a substantial increase in whistleblower litigation***.

According to *The Wall Street Journal* September 30, 2010 article "After Dodd-Frank, SEC Getting At Least One FCPA Tip A Day," the SEC is getting at least ***one whistleblower bounty-seeker FCPA tip per day*** since the Dodd-Frank provisions went into effect.

43



Challenges organizations may face

- Encouraging internal reporting
- The decision to self-report
- Enhancing investigation preparedness
- Enhancing monitoring and detection activities

44



Ten things about Whistleblowing

45



1. Tips appreciated

No.1 method of fraud detection, per ACFE 2010 Report to the Nations on Occupational Fraud and Abuse.

Entities with hotlines discover 47 percent of frauds through tips, per ACFE.

That still leaves 53% detected by other methods, e.g., transaction testing and internal auditing.



46



2. Don't get distracted by noise

Approximately half of whistleblower calls are typically related to personnel issues.

While there may be some 'noise' with a whistleblower system, the goal is not to let it distract you from what may be truly important.



47



3. Is your hotline just lukewarm?

Seven ways to take your hotline's temperature:

- Anonymous employee surveys
- Benchmarking
- Focus groups
- Exit interviews
- Feedback from hotline users
- Interviews
- Incident logs



48



4. Carrots may help you hear better

Rewarding whistleblowers may be necessary to compete effectively with the U.S. government's rewards for tips relating to securities violations.

Some rewards might be widely published internally; others may be much more sensitive.

Fairness and generosity of rewards may help to attract employee support and generate more reports.



49



5. Communicate, communicate, communicate

63 percent of employees surveyed said they had reported misconduct when they saw it (2009 National Business Ethics Survey by ERC)

Maintaining awareness of the system, building willingness to use it, and developing employees' ability to identify potential wrongdoing

Publishing internally suitable anonymous examples of where a whistleblower system report led to an investigation and appropriate disciplinary action



50



6. Protecting those who serve

Creating a supportive environment for whistleblowers can include:

- Developing rewards
- Non-retaliation policy and training
- Monitoring whistleblowers' career, pay, and proposed discipline
- Investigating alleged retribution
- Implementing a records retention policy for whistleblower reports, complaints, and investigations



51



7. Open wide

Whistleblower system access can sometimes be restricted consciously by executives who may be fearful of having to respond to more allegations if they “open wide” but doing so may enhance overall results.

Potential barriers to whistleblowing include:

- Service hours – 24x7x365
- Languages – preferred languages of employees and other constituents
- Constituencies – employees, suppliers, customers, and the general public
- Methods – hotline, web form, e-mail, fax, letter and in person.



52



8. What's in a name?

'Whistleblower' may have negative connotations for cultural, historical, and other reasons.

Two-way communication system called a 'helpline' or 'guideline' may be less intimidating and can provide guidance before action is taken.

Giving employees experience in using the line for day-to-day matters, building trust, and making them more willing to call should a serious matter arise.



53



9. When in Rome...

Taking one whistleblower system and deploying it elsewhere (e.g. – worldwide) without any customization may not generate the desired results.

It can be helpful to involve local personnel to help tailor communication about the system.

Providing alternative reporting methods as well, such as e-mail or Web form, may be much more attractive since they tend to be more popular in certain cultures.



54



10. A prepared and diligent response

Certain principles can help drive more effective responses, including:

- Clear line of reporting from the whistleblower system to a designated member of senior management with a reporting relationship directly to oversight committees or others
- Defined roles and responsibilities for evaluating incoming reports
- Clear communication processes
- Pre-determined investigation protocols and plans
- Disciplinary committee



55



What questions do you have?

56



Presenter's Contact information

James H. Cottrell, Jr., CPA, CA, CGMA
Partner
Forensic & Dispute Services
Deloitte Financial Advisory Services LLP
+1 202 378 5002
jhcottrell@deloitte.com

57



This presentation contains general information only and is based on the experiences and research of Deloitte practitioners. Deloitte is not, by means of this presentation, rendering business, financial, investment, or other professional advice or services. This presentation 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, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this presentation. Certain services may not be available to attest clients under the rules and regulations of public accounting.

58



Bonus: Conducting a Fraud Risk Assessment

59



Why conduct a fraud risk assessment?

- Legal duty of care to shareholders
- Institute of Internal Auditors (IIA) Standards
- Regulatory compliance risks
- Direct cost of fraud
- Indirect costs
- Fraud is a business risk to be managed, not just a compliance issue

60



Why conduct a fraud risk assessment? (cont.)

- *Traditional risk assessments link risks to the organization's key objectives. Fraud can be overlooked during this type of review if it is not considered a core Organization objective*
- *A fraud risk assessment expands upon traditional risk assessment. It is scheme and scenario based rather than based on control risk or inherent risk*
- *Assessment teams must be able to identify the potential schemes and scenarios impacting the industries and geographic markets in which the organization conducts business*

Key Approach

- *Evaluate fraud risk factors*
- *Identify possible fraud schemes & scenarios*
- *Prioritize identified fraud risks*
- *Evaluate whether mitigating controls exist or are effective*
- *Document the risk assessment process & conclusions*
- *Conduct periodic reviews and updates*

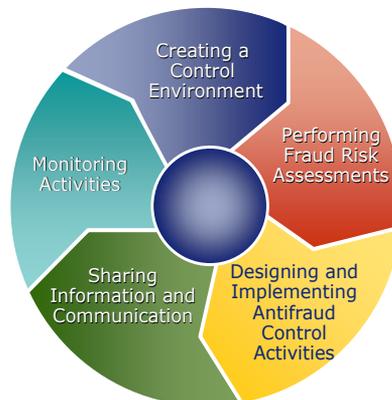
61



Fraud risk assessment

What is a fraud risk assessment?

- A fraud risk assessment considers the ways that fraud and misconduct can occur by and against an entity
- The fraud risk assessment is an integral part of an antifraud program that is based on the COSO (Committee of Sponsoring Organizations) integrated governance framework
- The fraud risk assessment is a crucial part of the broader entity-wide risk assessment process



Source: Committee of Sponsoring Organizations of the Treadway Commission, Internal Control – Integrated Framework

62



Planning a fraud risk assessment

Pitfalls

- Management does not take responsibility for the fraud risk assessment
- The fraud risk assessment is not risk-based
- The fraud risk assessment is too broadly based

Recommendations

- Management should own the fraud risk assessment and have significant input into the fraud risk assessment. Educate the Leadership and External Auditors on the fraud risk assessment - get their support/buy-in
- The fraud risk assessment should be risk-based
- The fraud risk assessment should be focused on the higher risk areas

63



Planning a fraud risk assessment (cont.)

Pitfalls

- The planned approach is contrary to the organizational culture
- The organization does not have the necessary skill sets to perform the fraud risk assessment
- The fraud risk assessment process does not include the appropriate people
- The fraud risk assessment is not systematic and recurring

Recommendations

- The planned approach should fit into the organizational culture – consider a mixed approach, e.g., interviews and group brainstorming
- Hire in the necessary skill sets (employees/consultants)
- Consider who should be involved as part of the planning process
- The fraud risk assessment should be systematic and recurring

64



Fraud risk assessment: Who should be involved?

C-Suite Officers

- CEO
- CFO
- CIO
- General counsel
- Chief compliance officer

Management

- Business unit managers
- Sales
- Marketing
- Human resources

Accounting

- Controller
- Business unit controllers
- Accounting managers
- Accounting supervisors

Oversight

- Board of directors/
trustees
- Audit committee
- Internal audit
- External auditors

65



Evaluation fraud risk factors

Step	Approach	Output
1 Evaluate fraud risk factors	<ul style="list-style-type: none"> ▪ Identify fraud risk factors ▪ Identify account balances and potential errors 	<ul style="list-style-type: none"> ▪ Schedule of fraud risk factors ▪ Enhanced knowledge of fraud risk environment
2 Identify possible fraud schemes and scenarios	<ul style="list-style-type: none"> ▪ Identify fraud risks ▪ Identify specific fraud schemes ▪ Identify potential parties involved 	<ul style="list-style-type: none"> ▪ Pervasive and specific fraud risks ▪ Catalog of fraud schemes ▪ Internal and external parties to fraud
3 Prioritize identified fraud risk	<ul style="list-style-type: none"> ▪ Evaluate possible fraud schemes by type, likelihood, significance, and pervasiveness 	<ul style="list-style-type: none"> ▪ Understand inherent risk associated with entity
4 Evaluate whether mitigating controls exist/are effective	<ul style="list-style-type: none"> ▪ Link fraud schemes to mitigating controls ▪ Evaluate control effectiveness 	<ul style="list-style-type: none"> ▪ Evaluate fraud risk factors ▪ Understand residual risk associated with entity

Communication with management

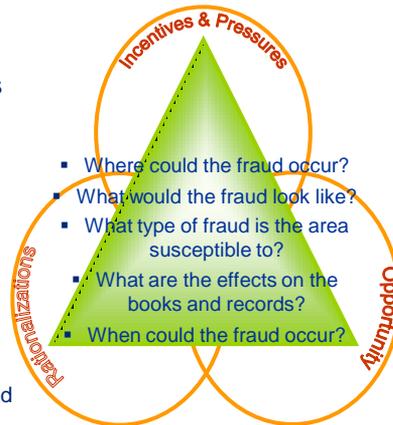
66



Identify and evaluate fraud risk factors

Fraud risk factors are events or conditions that indicate incentives / pressures to perpetrate fraud, opportunities to carry out the fraud, or attitudes / rationalizations to justify a fraudulent action

- Incentives & Pressures:
 - Employees have an incentive or are under pressure which provides a reason to commit the fraud
- Opportunity:
 - Circumstances exist that provide an opportunity for fraud to be perpetrated
- Attitudes / Rationalizations:
 - Those involved in the fraud are able to rationalize committing a fraudulent act



67



Identify and evaluate fraud risk factors (cont.)

- Identify fraud risk factors at the entity level, significant location, significant account and business process level.
 - Personnel from various levels of the organization should be involved in the process

<input checked="" type="checkbox"/> Management	<input checked="" type="checkbox"/> Audit committee
<input checked="" type="checkbox"/> Business process owners	<input checked="" type="checkbox"/> Internal audit
<input checked="" type="checkbox"/> IT management	
 - Management should consider and evaluate the facts and circumstances for their organizations in determining the areas to consider in the fraud risk assessment process

<input checked="" type="checkbox"/> Entity's industry	<input checked="" type="checkbox"/> Geographical locations
<input checked="" type="checkbox"/> Size	<input checked="" type="checkbox"/> Organizational structure
<input checked="" type="checkbox"/> Operations	<input checked="" type="checkbox"/> General economic climate

68



Identify and evaluate fraud risk factors (cont.)

- In identifying and evaluating fraud risk factors, management should consider:
 - Internal considerations:
 - Past fraud within the organization, actual and alleged
 - Compliance with laws and regulations
 - Tone at the top
 - Strength of the organization's IT department
 - Unrealistic performance expectations
 - Unusual internal trends
 - Unusual financial trends
 - Employee morale
 - External considerations:
 - Industry fraud, actual and alleged
 - Industry analyst reports
 - Analyst expectations
 - Current market conditions
 - Investor expectations

69



Identify and evaluate fraud risk factors (cont.)

Pitfalls

- Fraud risk factors are not considered, existing controls are considered
- The potential for management override of controls is not considered
- Interviews are not value-added

Recommendations

- Use the fraud triangle to explain the significance of fraud risk factors and to initiate thinking
- Do not consider controls EXCEPT when considering the potential for management override
- Develop interview approach that matches area and culture

70



Fraud risk assessment group exercise

Identify fraud risk factors that exist in the Organization

71



Identify and evaluate fraud risk factors (cont.)

Identify fraud risk factor



Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Pervasiveness	Likelihood	Significance	Control Activities	Dyre
Public Company / Unrealistic Earnings Expectations										

72



Identify and evaluate fraud risk factors (cont.)

For each identified fraud risk factor, identify the account balances and potential errors that may be affected and assess the fraud risks



Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Pervasiveness	Likelihood	Significance	Control Activities	Type
Public Company / Unrealistic Earnings Expectations	Revenue Accounts Receivable									

73



Identify possible fraud schemes and scenarios

Step	Approach	Output
1 Evaluate fraud risk factors	<ul style="list-style-type: none"> Identify fraud risk factors Identify account balances and potential errors 	<ul style="list-style-type: none"> Schedule of fraud risk factors Enhanced knowledge of fraud risk environment
2 Identify possible fraud schemes and scenarios	<ul style="list-style-type: none"> Identify fraud risks Identify specific fraud schemes Identify potential parties involved 	<ul style="list-style-type: none"> Pervasive and specific fraud risks Catalog of fraud schemes Internal and external parties to fraud
3 Prioritize identified fraud risk	<ul style="list-style-type: none"> Evaluate possible fraud schemes by type, likelihood, significance, and pervasiveness 	<ul style="list-style-type: none"> Understand inherent risk associated with entity
4 Evaluate whether mitigating controls exist/are effective	<ul style="list-style-type: none"> Link fraud schemes to mitigating controls Evaluate control effectiveness 	<ul style="list-style-type: none"> Evaluate fraud risk factors Understand residual risk associated with entity

Communication with management

74



Identify possible fraud schemes

Brainstorm specific fraud schemes that could result from the specific risks identified, without consideration of existing controls

• A scheme is the mechanism, scenario, or sequence of actions by which:

- The financial statements may be improperly manipulated or misstated
- Assets may be misappropriated
- Improper or unauthorized expenditures may be made
- Self-dealings may occur
- Laws and regulations may be violated

– One or more related fraud schemes may exist for each fraud risk. Consider:

- Past fraud within the organization, actual and alleged
- The industry in which the organization operates
- The geographies in which the organization operates

75



Identify possible fraud schemes & parties

For each fraud scheme, identify internal and external parties who could be involved:

- | | |
|--|---|
| <p>– Internal parties:</p> <ul style="list-style-type: none">▪ C-suite▪ Business process owners▪ Employees | <p>– External parties:</p> <ul style="list-style-type: none">▪ Agents (particularly in foreign countries)▪ Independent contractors▪ Competitors▪ Customers▪ Licensees▪ Vendors |
|--|---|

76



Identify possible fraud schemes and scenarios

Pitfalls

- The schemes are too general, not allowing for sufficient consideration of risks and preventing appropriate level of mapping to controls
- The schemes do not consider the potential for management override of controls
- The schemes do not consider the potential for collusion

Recommendations

Detail the schemes by considering:

- Why?
- Who?
- What? (assets, financial reporting)
- Where? (locations, accounts)
- When?
- How?

77



Fraud risk assessment group exercise

Identify fraud schemes and scenarios that could result from the fraud risk factors previously identified

78



Identify possible fraud schemes and scenarios (cont.)

Identify the fraud risk, and if the fraud risk is pervasive of specific

Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Pervasiveness	Likelihood	Significance	Control Activities	Type
Public Company / Unrealistic Earnings Expectations	• Revenue • Accounts Receivable	Overstatement of Sales - "Roundtrip" Transactions				S				

79



Identify possible fraud schemes and scenarios (cont.)

Identify the fraud schemes and scenarios, and all potential parties involved

Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Pervasiveness	Likelihood	Significance	Control Activities	Type
Public Company / Unrealistic Earnings Expectations	• Revenue • Accounts Receivable	Overstatement of Sales - "Roundtrip" Transactions	<ul style="list-style-type: none"> • Transactions may include sales between companies for the same amount within a short time period, or they may involve a loan to or investment in a customer so that the customer has the ability to purchase the goods (vendor financing). • Liberal exchange or return policies without appropriate reserve - improper accounting for liberal or unconditional right of return • Other than transactions or on products shipped for trial or evaluation purposes 	<ul style="list-style-type: none"> • Sales agents • Finance managers • Customers / Clients 		S				

80



Prioritize identified fraud risk

Step	Approach	Output
1 Evaluate fraud risk factors	<ul style="list-style-type: none"> Identify fraud risk factors Identify account balances and potential errors 	<ul style="list-style-type: none"> Schedule of fraud risk factors Enhanced knowledge of fraud risk environment
2 Identify possible fraud schemes and scenarios	<ul style="list-style-type: none"> Identify fraud risks Identify specific fraud schemes Identify potential parties involved 	<ul style="list-style-type: none"> Pervasive and specific fraud risks Catalog of fraud schemes Internal and external parties to fraud
3 Prioritize identified fraud risk	<ul style="list-style-type: none"> Evaluate possible fraud schemes by type, likelihood, significance, and pervasiveness 	<ul style="list-style-type: none"> Understand inherent risk associated with entity
4 Evaluate whether mitigating controls exist/are effective	<ul style="list-style-type: none"> Link fraud schemes to mitigating controls Evaluate control effectiveness 	<ul style="list-style-type: none"> Evaluate fraud risk factors Understand residual risk associated with entity

Communication with management

81



Evaluate fraud schemes: Type

TYPE

Financial Statement Fraud

- Manipulation, falsification, or alteration of accounting records and supporting documentation
- Misrepresentation in, or intentional omission from, the financial statements
- Misapplication of accounting principles, such as amount, classification, disclosure or presentation

Asset Misappropriation

- Embezzling receipts
- Stealing assets
- Causing an entity to pay for goods or services that have not been received

Other

- Improper or unauthorized expenditures
- Self-dealing
- Violations of laws and regulations

82



Evaluate fraud schemes: Likelihood, significance, and pervasiveness

Likelihood:

- That a fraud scheme will occur and result in a material misstatement, should be assessed without consideration of controls
 - Remote
 - More than remote / reasonably possible
 - Probable

Significance:

- Evaluate whether fraud scheme could lead to a material misstatement or otherwise negatively impact the entity
 - Inconsequential
 - More than inconsequential
 - Material

Pervasiveness:

- Evaluate whether each particular fraud scheme is pervasive to:
 - The financial statements as a whole
 - A particular account balance
 - A certain class of transactions or a particular financial statement assertion

83



Prioritize identified fraud risk

Pitfalls

All fraud risks are considered equally important

Recommendations

Prioritize the identified fraud risks based on likelihood and significance

84



Fraud risk assessment group exercise

Evaluate and prioritize the identified fraud schemes by type, likelihood, significance, and pervasiveness

85



Prioritize identified fraud risk (cont.)

Evaluate the respective fraud schemes by type, likelihood, significance, and pervasiveness



Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Pervasiveness	Likelihood	Significance	Control Activities	Type
Public Company / Unrealistic Earnings Expectations	• Revenue • Accounts Receivable	Overstatement of Sales - "Roundtrip" Transactions	<ul style="list-style-type: none"> • Transactions may include sales between companies for the same amount, within a short time period, or they may involve a loan to or investment in a customer so that the customer has the ability to purchase the goods (vendor financing). • Liberal exchange or return policies without appropriate reserve - Improper accounting for liberal or unconditional right of return • Other sham transactions or on products shipped for trial or evaluation purposes 	<ul style="list-style-type: none"> • Sales agents • Finance managers • Customers / Clients 	F	S	L	M		

86

Evaluate whether mitigating controls exist and are effective



Step	Approach	Output
1 Evaluate fraud risk factors	<ul style="list-style-type: none"> Identify fraud risk factors Identify account balances and potential errors 	<ul style="list-style-type: none"> Schedule of fraud risk factors Enhanced knowledge of fraud risk environment
2 Identify possible fraud schemes and scenarios	<ul style="list-style-type: none"> Identify fraud risks Identify specific fraud schemes Identify potential parties involved 	<ul style="list-style-type: none"> Pervasive and specific fraud risks Catalog of fraud schemes Internal and external parties to fraud
3 Prioritize identified fraud risk	<ul style="list-style-type: none"> Evaluate possible fraud schemes by type, likelihood, significance, and pervasiveness 	<ul style="list-style-type: none"> Understand inherent risk associated with entity
4 Evaluate whether mitigating controls exist/are effective	<ul style="list-style-type: none"> Link fraud schemes to mitigating controls Evaluate control effectiveness 	<ul style="list-style-type: none"> Evaluate fraud risk factors Understand residual risk associated with entity

Communication with management

87

Mapping to mitigating controls



Preventative: to mitigate specific fraud risks

Detective: to identify fraud if it occurs. Monitoring activity to assess the effectiveness of antifraud controls

Deterrence: to heighten the fear of detection and the consequences of prosecution

88



Fraud controls

- Reporting mechanisms (whistleblower hotline)
- Fraud awareness training
- Code of conduct
- Monitoring of controls by internal audit
- Surprise audits
- Segregation of duties
- Hiring and promotion
- Controls over significant, unusual transactions
- Journal entries, period end adjustments
- Related party transactions
- Management estimates
- “Tone at the top” set by management:
 - Communicate what is expected of employees
 - Lead by example
 - Provide a safe mechanism for reporting violations
 - Reward integrity
- Tools to assess fraud controls:
 - Hotline benchmarking report – by industry
 - Code of conduct benchmarking: Ethisphere – 43 elements

89



Evaluate mitigating controls

Evaluate the *control design effectiveness* and *control operating effectiveness* of the controls to determine if they sufficiently mitigate the risk of the identified fraud schemes

Consider possible management override of controls

- Special consideration should be given to the risk of override of controls by management. Such controls include:
 - active oversight from the audit committee
 - whistle-blower programs and a system to investigate anonymous complaints
 - reviewing journal entries

Consider the need for additional control activities or strengthening of existing controls (identify control gaps)

90



Fraud risk assessment group exercise

Evaluate existence and effectiveness of mitigating controls for the fraud schemes

91



Evaluate whether mitigating controls exist and are effective

Evaluate mitigating controls for the respective fraud schemes



Fraud Risk Factor	Account Balance(s) Affected	Fraud Risk	Fraud Schemes / Scenarios	Potential Person(s) Involved	Type	Prevalence	Likelihood	Significance	Control Activities	Type
Public Company / Unrealistic Earnings Expectations	• Revenue • Accounts Receivable	Overstatement of Sales - "Roundtrip" Transactions	<ul style="list-style-type: none"> • Transactions may include sales between companies for the same amount within a short time period, or they may involve a loan to or investment in a customer so that the customer has the ability to purchase the goods (vendor financing). • Liberal exchange or return policies without appropriate reserve - Improper accounting for liberal or unconditional right of return • Other sham transactions or on products shipped for trial or evaluation purposes 	<ul style="list-style-type: none"> • Sales agents • Finance managers • Customers / Clients 	F	S	L	M	<ul style="list-style-type: none"> • 22.1.1.1 - Business Approval Matrix - Prior to booking a contract, does a member of Sales Accounting (or local equivalent) review the contract package to ensure that all appropriate approvals and required documentation have been obtained in accordance with the documented policy (business approval matrix)? 	P
									<ul style="list-style-type: none"> • 22.1.1.2 - Standard Contract Review Checklist - Is such review documented in the standard contract review checklist and signed off Sales Accounting management (or local equivalent) for all contracts? 	P
									<ul style="list-style-type: none"> • 22.1.1.3 - Revenue Recognition Review - contracts > \$1M - Prior to booking, are contracts with either a gross value of greater than \$1 million or have non standard terms reviewed for revenue recognition considerations by the revenue recognition senior manager? Is such review and approval documented? 	P

92

Evaluate fraud risk assessment results & prioritize residual risk



Evaluate whether controls sufficiently mitigate the identified fraud risks

Management identify and prioritize fraud risks requiring attention in terms of urgency and allocating resources

Management actions to address fraud risk in a fraud risk action plan

93

Remediation plan



Controls should be implemented or enhanced for identified fraud schemes where controls are not already present, inadequately designed or poorly implemented

Plan to identify specific personnel responsible for implementing control improvements and an implementation timetable

Fraud risk action plan may be actions to improve the antifraud program or address specific fraud scheme control deficiencies

The audit committee should oversee the entire process

94



Fraud risk assessment matrix: Example

Fraud Risk Factor	Fraud Risk	Fraud Scheme/Scenarios	Account Balance(s) Affected	Potential Person(s) involved	Type of Fraud	Likelihood	Significance	Inherent Risk	Control Activities	Control Type	ODER	ODER	ODER	Residual Risk
Public Company / Unrealistic Earnings Expectations	Overstatement of Sales - "Roundtrip" Transactions	<ul style="list-style-type: none"> Transactions may include sales between companies for the same amount within a short time period, or they may involve a loan to or investment in a customer so that the customer has the ability to purchase the goods (vendor financing). Liberal exchange or return policies without appropriate reserve - improper accounting for liberal or unconditional right of return Other sham transactions or on products shipped for trial or evaluation purposes 	<ul style="list-style-type: none"> Revenue Accounts receivable 	<ul style="list-style-type: none"> Sales agents Finance Management 	F	4	4	8	22.11.1 - Business Approval Matrix - Prior to booking a contract, does a member of Sales Accounting (or local equivalent) review the contract package to ensure that all appropriate approvals and required documentation have been obtained in accordance with the documented policy (business approval matrix)?	p	2	2	4	12
									22.11.2 - Standard Contract Review Checklist - Is such review documented in the standard contract review checklist and signed off Sales Accounting management (or local equivalent) for all contracts?	p				
									22.11.3 - Revenue Recognition Review - contracts > \$1M - Prior to booking, are contracts with either a gross value of greater than \$1 million or have non standard terms reviewed for revenue recognition considerations by the revenue recognition senior manager? Is such review and approval documented? (Such review is typically done in the proposal stage) (Corporate)	p				

95



Documenting the fraud risk assessment

Documentation may include:

- Process narrative
- Minutes of fraud brainstorm sessions
- Copies of instructions and reference materials provided to participants
- E-mail and other correspondence related to the process
- Minutes of audit committee meetings during which management's fraud risk assessment was presented, reviewed, discussed, and/or approved

96



Monitoring the fraud risk assessment

Need to keep fraud risk assessment and documentation current:

- Conduct quarterly updates
- Imbed on-going fraud risk assessment in the Sarbanes-Oxley Section 404 efforts
- Re-visit fraud risk assessment as part of Enterprise Risk Management (ERM) activities

Report changes and updates to senior Organization management team and leadership on a quarterly basis

Update fraud risk assessment for changes in the business and/or business environment (economy, industry, changes in competitor businesses)

Use the fraud risk assessment to refine and focus internal audit testing