FRAUD
Detection &
Incident Response

Association of Inspector Generals

August 10 & 11, 2020

John@JohnHallSpeaker.com
www.FraudPreventionPro.com
(312) 560-9931

Fraud Prevention Pro

ABOUT YOUR SPEAKER

Phone: (312) 560-9931   **John@JohnHallSpeaker.com**

Hall Consulting, Incorporated
PO Box 6263
Denver, CO 80206

John J. Hall, CPA

John J. Hall, CPA is the President of Hall Consulting, Inc., the creator of www.FraudPreventionPro.com, and the author of the award-winning book *"Do What You Can! Simple Steps–Extraordinary Results"*. He has been a business consultant, results coach and speaker for most of his 43-year career.

Through live and on-line training programs, conference keynote and technical presentations, business consulting engagements, John helps program participants and client team members:

- Identify and improve areas of exposure to business risk, wrongdoing, and fraud

- Improve organizational and personal performance

- Enhance the effectiveness of business processes and individual behavior

- Improve interpersonal and communications skills

Speaking, training, coaching and consulting areas include:

- Fraud Risk Management: prevention, deterrence, early detection and effective incident response

- Business keynote and conference presentations

- Communication and interpersonal behavior skills programs, including:

  ✓ Establishing business rapport and trust
  ✓ Effective interviewing and listening
  ✓ Speaking and presenting
  ✓ Selling ideas and influencing others to take action
  ✓ Leadership, collaboration and influence
  ✓ Consulting skills for professionals

- Intensive One-to-One and small group performance and results coaching

- Board and senior management anti-fraud consulting

- Audits of costs incurred in large construction projects and other contractor services

In addition to operating his speaking, training and business consulting firm since 1990, he has worked in senior leadership positions in large corporations and international public accounting and consulting firms.

John is a Certified Public Accountant (Pennsylvania). He is an active member of the National Speakers Association, the American Institute of CPAs, and the Institute of Internal Auditors.

Meet John at www.FraudPreventionPro.com
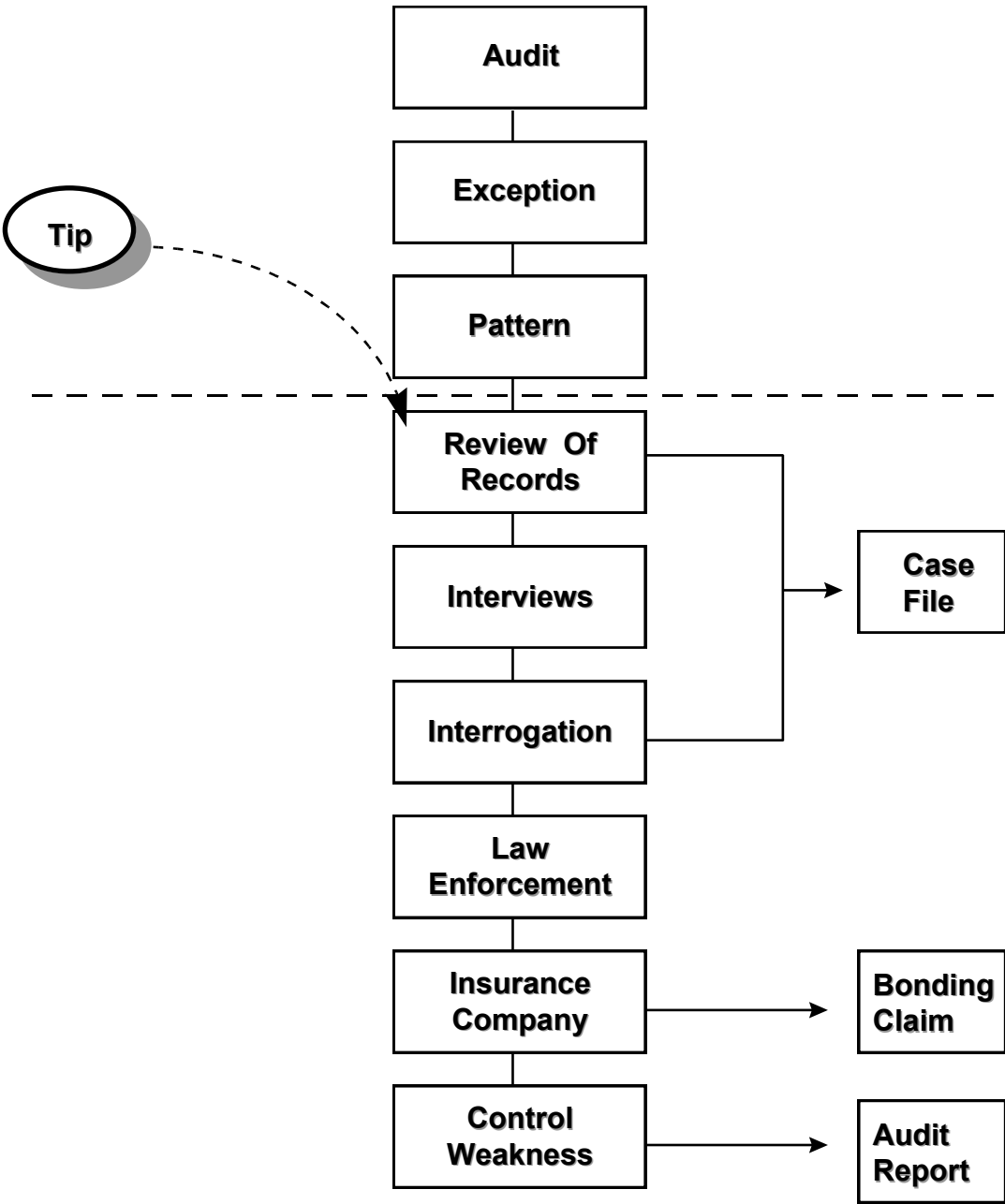
<u>DISCUSSION OF ANTI-FRAUD EXPECTATIONS</u>

The list below should give you suggestions of topics or themes to include in leading a discussion about fraud expectations with your staff or team. Don't just read off the list – instead, pick five or six items that most relate to your own beliefs and tailor comments to your unique environment and culture. Be sure to:

1. Frame the discussion to the questions those listening to you will likely have
2. Stress the importance of a balanced message – tie your request for help to the listeners normal pride in their work
3. Be explicit. Don't beat around the bush. Tell them what you expect and what you need them to do as a result.
4. Use a positive tone. Make it a 'call to arms' that starts with, "I need your help to fight this problem."
5. Include examples of what could go wrong in your area, including what it would look like in reports, variances, complaints and other indicators of a problem

---

It is expected that every manager and employee will:

1. Know the fraud related exposures in their areas of responsibility, for example…

2. Know what it would look like if it happened. For example…

3. Use best-faith efforts to minimize the chance of fraud on their watch. Examples include…

4. Make sure the transactions they personally approve are not fraudulent. Here's an example of what I mean…

5. Personally monitor for those frauds that only they are in a position to detect. For example…

6. Question and challenge the unusual. Here's an example of what I mean…

7. Set an example of honest and ethical behavior by personal example and by not tolerating dishonest or unethical behavior in others. Here are a few examples of how to do that…

8. Strive to prevent fraud by minimizing the exposures and reducing the opportunities and temptation. For example…

9. Immediately refer suspected wrongdoing to Internal Audit or Security for investigation. Here's an example of what I mean…

AUDIT / INVESTIGATION FLOW DIAGRAM

```
                          ┌──────────────┐
                          │    Audit     │
                          └──────────────┘
                                 │
                          ┌──────────────┐
                          │  Exception   │
                          └──────────────┘
                                 │
      ╭─────╮                ┌──────────────┐
      │ Tip │  ·····→        │   Pattern    │
      ╰─────╯                └──────────────┘
                                 │
   ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─│─ ─ ─ ─ ─ ─ ─ ─ ─ ─
                          ┌──────────────┐
                          │  Review  Of  │────────┐
                          │   Records    │        │
                          └──────────────┘        │
                                 │                 │        ┌──────────┐
                          ┌──────────────┐        │──────→ │   Case   │
                          │  Interviews  │        │        │   File   │
                          └──────────────┘        │        └──────────┘
                                 │                 │
                          ┌──────────────┐        │
                          │ Interrogation│────────┘
                          └──────────────┘
                                 │
                          ┌──────────────┐
                          │     Law      │
                          │ Enforcement  │
                          └──────────────┘
                                 │
                          ┌──────────────┐        ┌──────────┐
                          │  Insurance   │──────→ │ Bonding  │
                          │   Company    │        │  Claim   │
                          └──────────────┘        └──────────┘
                                 │
                          ┌──────────────┐        ┌──────────┐
                          │   Control    │──────→ │  Audit   │
                          │   Weakness   │        │  Report  │
                          └──────────────┘        └──────────┘
```

THREE-STEP FRAUD DETECTION

I. 'THINK LIKE A THIEF' PROJECT BRAINSTORMING

Look at identified weaknesses and other opportunities from the perspective of how they could be exploited. Documentation should include specific fraud risks identified and a clear bridge to specific project steps, controls and behaviors targeted at detection of related fraud incidents.

II. USE DISCOVERY TECHNIQUES AGGRESSIVELY

a) Discovery or Attribute Testing.

These tests have as their purpose surfacing the visible signs of wrongdoing. Such testing can be directed at either electronic or manual records. The use of electronic data analysis tools makes the efficient search of large populations possible.

b) Detection-Focused Interviews.

Targeted interviewing techniques can be an efficient method for surfacing hidden information. They are used to get the "human" information not available in records. In situations where the signs of fraud might not be in the records, the interview may be the only method available to surface needed information.

c) Monitoring for Fraud Indicators.

Examples include:

- Internal information used by management to find problems in operations
- Reconciliations, closing entries, adjustments, override transactions and other available information showing a deviation from normal results
- Recurring software-based inquiries

III. DETERMINE THE CAUSE OF ALL FRAUD INDICATORS SURFACED

All indicators surfaced should be investigated as to their cause. Follow up on fraud indicators, symptoms and red flags may lead to the discovery of wrongdoing. It also may surface other important non-fraud issues. Either result justifies following all observed indicators through to the determination of their Root Cause.

<u>BRAINSTORMING RISKS AND EXPOSURES</u>

The _____

Could _____

_____

COMMIT

_____

_____

_____

CONVERT (benefit)

_____

_____

_____

CONCEAL

_____

_____

_____

RED FLAGS / INDICATORS

_____

_____

_____

_____

_____

_____

_____

_____

_____

DETECTION STEP(S)

_____

_____

_____

<u>TRAVEL EXPENSES INTERVIEW</u>

You have been asked by your supervisor to interview a mid-level manager about discrepancies in that manager's expense reports over the past three months. This manager is a 29-year old female.

The request occurred because a reviewer in the accounting area noticed what they described as "unusual activity over several months, including both charges and credits, on the manager's company credit card."

You were asked to interview the manager to gain additional information merely because you happened to be in the second week of a three-week audit at the same location where the subject manager has her office.

Copies of the related expense reports and support were emailed to you this morning, and your quick review leads you to believe that the questions are legitimate. For example, you notice that explanations for dinners routinely indicate only "business dinner" as the purpose of a meal, entertainment expenses while traveling appear to be excessive, and cash expenditures for taxis, meals and other cash items seem high for the locations visited.

<u>DISCUSSION QUESTIONS</u>

1. List two things that you should consider as you plan this interview.

   a)

   b)

2. List two things that could go wrong during this interview. How will you prepare for these possible challenges?

   a)

   b)

<u>OTHER METHODS OF DISCOVERY</u>

1. If you had unlimited access to records and people, how would you look for fraud? List two ideas. Be specific.

2. If you could create one <u>new</u> data analysis test to look for wrongdoing, what would it be? List the files needed and the specific red flags you would seek to uncover.

3. Some fraud cases surface as a result of tips from informants. What can we do to encourage concerned employees to come forward? What about vendors, customers and other third parties?

4. Auditors and examiners use confirmations for many purposes. Examples of confirmations aimed at fraud detection include:

   - Change of address, mailed to prior address
   - Payments, using a copy of both the front and back of the check
   - Receivables already written off
   - Late payments
   - Refunds and credits

   List one other confirmation idea aimed at surfacing fraud indicators.

5. What else could you do to find misconduct, wrongdoing, theft or outright fraud on your audits or other projects?

PROCUREMENT & CONTRACTING RISKS
What Could Go Wrong and the 3 C's?

1. Determination of need

2. Documenting deliverables

3. Develop internal budget

4. Identify potential suppliers and contractors

5. Solicit bids

6. Negotiate and finalize contract terms

7. Award the work

8. The work itself

9. Administration, including review of billing and payment

10. Closeout and final settlements

<u>EXERCISE: WHAT WOULD YOU DO NEXT?</u>

1. <u>EMPLOYEE AND VENDOR ADDRESS MATCH</u>

Audit performed a data match of vendor addresses and employee addresses. There was one confirmed match: an IT consultant and one of our mid-level supervisors in Princeton NJ. A quick review of the charges from this consultant show activity of just over $60,000 from nine invoices spread over the last two years.

What would you do next?

2. <u>CONFIDENTIAL DATA LOSS?</u>

Our IT security team identified a pattern of outbound emails from a supervisor with Excel spreadsheets attached. These emails are addressed to the employee's Google gmail account, and the spreadsheets appear to contain customer and employee data. The issue has been referred to the audit department for follow up and disposition.

What would you do next?

3. <u>SHADING OF OPERATING RESULTS</u>

The corporate financial reporting team recently reached out to auditing about a growing number of monthly closing journal entries at one division. These entries appear to manipulate reserves and other accrual accounts. The net result seems to be an attempt to smooth reported expenses and resulting earnings to better match budget expectations.

What would you do next?

4. <u>POTENTIAL FCPA VIOLATION</u>

The legal staff received an anonymous tip in a letter. The tip alleges that one of our managers in India mentioned making payments to a local zoning official in connection with the renovation construction of one of our facilities. No further details were provided.

What would you do next?

<u>INVESTIGATIONS - WHAT COULD GO WRONG?</u>

<u>DISCUSSION QUESTIONS</u>

Some say that Murphy's Law - "Everything That Could Go Wrong Will Go Wrong" - is in full effect during investigations.

Here is a short list of things that could easily go wrong during our work while in "investigative mode".

- a) What action could you take to mitigate each risk?

- b) Based on your experience, what additional risks should we add to this list?

---

1. Exceeding our stated authority

2. Uncertainty about access to facilities, offices, files, desk drawers, company vehicles, and electronic data

3. Uncertainty about taking possession of original documents

4. Access to personal property (brief cases, computer bags, purses, toolboxes, lockers, lunch pails, vehicles, other)

5. Threats – explicit or implicit

6. Legal concerns

7. Career concerns

8. Safety concerns

9. *'He said – she said'* results of interviews and informal discussions

10. Documents misplaced

11. Disposition of 'To-Do' lists

12. Past audit findings and reports

13. Management barriers

PERCEPTION EXERCISE

Item	Permitted, But Not Encouraged (1)	Warning (2)	Loss of Job (3)	Report to Authorities (4)	Notes
A					
B					
C					
D					
E					
F					
G					
H					
I					
J					