Fraud Issues & Answers for Internal Auditors

The Institute of Internal Auditors
Topeka Kansas Chapter
May 1, 2013

John J. Hall
John@JohnHallSpeaker.com
(970) 926-0355
John J. Hall, CPA

John Hall is the founder and President of Hall Consulting, Inc. and the author of “Do What You Can! Simple Steps – Extraordinary Results”.

Through live and recorded programs, performance coaching, and business consulting engagements, John helps program participants and client team members:

- Improve organizational, personal, and professional performance
- Enhance the effectiveness of business processes and individual behavior
- Improve interpersonal and communications skills
- Identify and improve areas of exposure to business risk, wrongdoing, and fraud

Business speaking, training, consulting and coaching areas include:

- Personal and work group effectiveness, team building and motivation
- Communication and interpersonal behavior skills enhancement, including:
  - Establishing rapport
  - Interviewing and listening
  - Speaking and presenting
  - Selling ideas
  - Influencing others to take action
- Consulting skills for professionals
- Fraud prevention, early detection and incident response
- Compliance reviews of construction and other third-party contracts

Mr. Hall has 35 years of experience as a professional speaker, consultant, corporate executive, and business owner. In addition to operating his own businesses since 1990, he has worked in senior leadership positions in large corporations and international public accounting firms.

John is a member of the National Speakers Association, the American Institute of CPAs, and the Institute of Internal Auditors. Meet John at www.JohnHallSpeaker.com. Email John at John@JohnHallSpeaker.com.
SEMINAR FOUNDATION CONCEPTS

1. Here’s what’s going to happen:
   a. Define “fraud” and associated fraud risks in your environment
   b. Explore current, emerging and continuing challenges from wrongdoing, misconduct and fraud
   c. Develop action plans for auditors to use on the job
   d. Script the critical moves in the fight against fraud
   e. Emphasize bright spots – where does it already work
   f. Discuss fraud examples and participant experiences
   g. Use brainstorming – individually, in small groups, all of us together
   h. Discuss how to improve bottom line results through fraud risk management

2. Fraud exposure areas:
   a. Misappropriation (tangible and intangible assets)
   b. Manipulated results reporting (financial and other measures)
   c. Corruption (or shadow deals)

3. My role is facilitation
   This program is about you. The answers to your fraud challenges are here in this room. My role is to help you bring them to the surface.

4. **Your role is to convert your intentions and the solutions we discuss to action on the job.**
   a. The destination must be clear – “Some is not a number; soon is not a time”
   b. You must link fraud exposures to audit steps and control procedures
   c. Use the concepts of “Solutions-Focused Therapy”

5. The “Three C’s” will be stressed throughout the seminar
   a. Commission
   b. Conversion
   c. Concealment
GETTING STARTED EXERCISE

1. Regarding fraud risks, my organization wants me to?

2. Regarding fraud risks, my department leaders want me to?

3. In handling fraud risks, the one skill I lack most is?

4. In my organization’s handling of fraud risks, I’m most frustrated by?

5. The best thing my organization does about fraud is?

6. I once found fraud while doing my job. Here’s how I found it:

ACTION IDEAS
FRAUD EXPOSURES IN YOUR ORGANIZATION

1. Cash Disbursements

2. Sales / Revenue Recognition

3. Cash Receipts

4. Purchasing / Procurement

5. Contract Services
BARRIERS FOR YOU TO ADDRESS

1. Lack of effective measurement of fraud exposure
2. Lack of time
3. Insufficient or unfocused resources
4. A new idea or rule is no match for culture.
5. A policy of keeping fraud cases in the shadows.
   a) Celebrate the first step when movement occurs. Reinforce it immediately.
6. Detection barriers for auditors and examiners
   a) Team members do not understand the objectives, drivers, and measurement metrics, of the area under review – and how those factors influence manager behavior
   b) Auditors don’t know what can go wrong and what it looks like
   c) Not the focus of normal routine audits and other projects
   d) We don’t understand the limitations of good controls.
   e) We are too trusting of employees, executives and managers
   f) We accept explanations for symptoms of fraud without verifying the facts
   g) We are afraid to ask questions – especially follow up questions
   h) Other project pressures / factors (including inadequate planning or time)
   i) ‘Form over substance’ audit and examination work
   j) Those who commit fraud fool us
7. Auditors and fraud examiners are:
   a) Paid to be professional doubters.
   b) Expected to find hidden issues (including fraud) on our assignments.
8. Controls do not prevent fraud. Controls make a fraudster change their method.
   a) Organizations must make wanted behaviors a little easier and wrong behaviors a little bit harder.
FRAUD RISK MANAGEMENT: OPPORTUNITIES FOR AUDITORS

1. FRAUD DETERRENCE AND PREVENTION
   a) Anti-fraud internal control infrastructure
   b) Acceptable and unacceptable behavior is defined and communicated
   c) Leaders at all levels set a great example – every day
   d) Policy on Suspected Misconduct
   e) Reporting of suspected violations is required
   f) Losses are identified, quantified and tracked
   g) Comprehensive fraud exposure analysis
   h) Meaningful fraud skills training for employees
   i) Auditors and employees look actively for fraud
   j) Fraud response is in place and ready to go

2. EARLY FRAUD DETECTION
   a) Detection-based audit steps
   b) Detection-based internal controls and behaviors
   c) Clear statement of detection responsibilities and accountability
   d) Effective hotlines
   e) Other tip sources
   f) Monitoring for red flags and other fraud indicators
   g) Special focus on third party relationships

3. EFFECTIVE FRAUD HANDLING
   a) Employees know what happens when the alarm sounds
   b) Investigation
   c) Loss recovery
   d) Control weaknesses are fixed
   e) Coordination with law enforcement and prosecutors
   f) Publicity issues
   g) Human resources issues
   h) Employee morale issues

Organizations (and their auditors) must be prepared to address fraud risks at all three levels.

ACTION IDEAS
FRAUD PREVENTION ENVIRONMENT

1. Anti-Fraud Internal Control Infrastructure

Fraud exposures are identified and specific control procedures are developed, implemented and maintained to both prevent these events from happening and to detect them should they occur.

2. Acceptable and Unacceptable Behavior is Defined and Communicated

Employees, vendors, contractors and others all need to know what is allowed in daily behavior. And just as important, what is considered misconduct. Employees and managers must know the rules for reporting financial and other results. Vendors, contractors and other third parties must know your restrictions on gifts and entertainment and penalties for violations. Make your “Code of Conduct” part of any agreements with third parties.

3. Leaders at All Levels Set a Great Example – Every Day

For years the phrase “tone at the top” has been used to focus on the statements, business practices and personal behavior of executives and other senior management members. But a ‘leader’ includes anyone we look to for an indication of proper behavior. That includes everyone from first level supervisors in the field right up to the Board. Require outstanding personal example. And counsel all who don’t act properly.

4. Issue a Policy on Suspected Misconduct

All organizations face the risk of wrongdoing and fraud. To effectively manage those risks, everyone should know what their responsibilities are in this important area. An effective “Policy on Suspected Misconduct” is the perfect place to document these responsibilities. Employees and managers will have a one-stop source explaining their role in deterrence, early detection and effective incident response.

5. Require Reporting of Suspected Violations by Others

Codes of Conduct and other behavior policies should require reporting. Periodic sign off is a good way to track awareness and minimize “I didn’t know” situations. Make the reporting of violations mandatory. Add a sign off where managers and employees acknowledge that they are not aware of violations by others.
FRAUD PREVENTION ENVIRONMENT
(continued)

6. **Identify, Quantify and Track Losses**

Few organizations have taken the time to develop a complete list of their existing fraud loss areas. Begin by listing areas where losses have occurred in the past. Then research these areas and assign ranges of probable current loss levels. Normally this list will total no less than one percent of revenue.

7. **Comprehensive Fraud Exposure Analysis**

Position by position, department by department, ask the question “What could go wrong?” Create a robust inventory of fraud risks. Use this list to provide training for new employees and supervisors. Develop offsetting prevention and early detection procedures for each risk identified. Publicize the effort and the results. Create awareness in honest employees, and fear in those tempted to commit wrongdoing.

8. **Fraud Skills Training**

Sponsor or conduct fraud awareness and skills training programs addressing what employees and auditors need to know to prevent, detect and handle fraud. Most employees have never been taught the skills needed to be effective in this area. This skills gap allows fraud to occur and go undetected.

9. **Auditors and Employees Look For Fraud**

Auditors and employees look for fraud symptoms and indicators in information they see each day. Managers and employees are aware of and monitor for fraud indicators in documents they handle and approve, in operations and exception reports, and in behavior. Auditors brainstorm fraud risks on every project, link fraud risks to specific audit procedures, and carry out fraud detection steps during their testing and interviews.

10. **Fraud Response in Place**

Identify the skills and relationships that will be needed when fraud is detected, and assemble the team in advance. Craft the message you want to deliver to employees, customers, the press and others. Know who will be authorized to investigate, handle requests for information, and interface with any outside parties.
10 REASONS CONTROLS BREAK DOWN

1. Blind trust

2. Willful blindness
   - Ignoring control implications of policies, procedures and reports
   - Ignoring behavioral indicators of problems

3. Situational incompetence

4. Not having information needed to assure transactions are proper

5. Not questioning the strange, odd and curious

6. The process mentality

7. Not enough time to do the control procedures

8. Not enforcing documentation requirements

9. Acceptance of the situation
   - Fear
   - Positional immunity
   - Conflict avoidance

10. Those in charge intentionally ignore or override procedures
GROUP EXERCISE: TRAVEL AND ENTERTAINMENT APPROVAL

Scripting the critical moves involves providing clear specific directions on behavior that we want to see at moments of decision. Preventing abuse and fraud in reimbursement of travel, entertainment and other out-of-pocket costs is heavily dependent on approvers asking the right questions at the moment of approval.

What questions should an approver ask? What details should they check? Be specific.

GOOD QUESTIONS TO ASK WHEN APPROVING OUT-OF-POCKET COSTS

1. ____________________________________________________________

2. ____________________________________________________________

3. ____________________________________________________________

4. ____________________________________________________________

5. ____________________________________________________________
BEFORE APPROVING INVOICES FROM VENDORS AND CONTRACTORS
“Good Questions to Ask!”

Each day, managers review and approve thousands of invoices, contractor statements, time sheets, expense reimbursements, purchasing card details, and other documents that cause cash to be disbursed. Too often, that approval becomes a “rubber stamp” with little active thought about what the approval step really means. “Signatures without thought” make it easy for those who are trying to fool us. Approval of transactions that turn out to be fraudulent can be embarrassing at best and career limiting at worst!

Managers are encouraged to answer these basic questions before approving invoices and other payment documents. All address the general question of

“How do I know?”

1. How well do I know this vendor or contractor? Do I have first hand knowledge that they even exist!

2. Do I know that they actually provided the goods or services identified in the invoice or other billing statement?

3. Do I know that they are using the correct amounts for price (including unit prices used), sales tax, freight, and other variables that make up the amount invoiced?

4. On what basis do I know that the prices are reasonable in the first place? What standard have I used in determining that the price charged is fair?

5. How do I know that the quantities make sense? On what basis have we agreed to purchase the stated quantities?

6. How do I know that the invoice and other documents are mathematically correct?

7. Do I know that this invoice has not already been paid?
SAS 99 (AU Section 316):
“CONSIDERATION OF FRAUD IN A FINANCIAL STATEMENT AUDIT”

“The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement, whether caused by error or fraud.” (AU sec. 110.02)

“This statement [SAS 99] established standards and provides guidance to auditors in fulfilling that responsibility, as it relates to fraud, in an audit of financial statements conducted in accordance with generally accepted auditing standards (GAAS).”

1. Required audit team brainstorming session
2. Introduces human psychology into the audit process
3. An iterative process: SAS 99 describes a process in which the auditor
   a) Gathers information needed to identify risks of fraud
   b) Identifies risks
   c) Assesses risks after taking into account an evaluation of the entity’s programs and controls
   d) Responds to the results of the assessment in three ways
      I. A response that has an overall affect on how the audit is conducted
      II. A response to risks involving the nature, timing, and extent of procedures
      III. A response to address management override of controls
4. Commission, Conversion and Concealment
5. Skills that may be required (develop or acquire)
   a) Communication – emphasis on brainstorming and expanded use of inquiry
   b) Technology
      ▪ The impact technology has on the risk of fraud.
      ▪ Audit procedures may benefit from the use of CAATs
   c) Forensic accounting
DETECTION SUGGESTIONS

TRAVEL AND ENTERTAINMENT REIMBURSEMENT

1. Develop a spreadsheet with all available detail from travel expense reports, including people entertained
   - Include the day of the week in the spreadsheet
   - Include local holidays (including Valentine’s Day, Mother’s Day, Father’s day, and related “holidays” that change in date from year to year) and other major events (Super Bowl, Kentucky Derby, Indianapolis 500)
   - Include all direct bill charges
   - Include petty cash or related reimbursements

2. For employees who appear as being entertained on others’ expense reports, cross match all information looking for duplication and other unusual patterns

3. Analyze travel for those employees and others incurring the most travel costs

4. Confirm hotel bills and related charges included on hotel bills

5. Confirm travel costs directly with the airlines, limousine companies and other service providers

6. Confirm restaurant charges directly with the restaurant, especially for those charges those that appear unusual as to amount (for the number of meals served), alcohol / food split, entertainment, inclusion of entertainment, etc.

7. Compare travel information with telephone charges on charge cards, cell phone bills, office extension phone logs, building and parking lot access logs, and machine printed taxi, toll and parking receipts. Look for date and time conflicts.

8. Confirm entertainment directly with those entertained

9. For vehicles:
   - If mileage is reimbursed, double check distances for reasonableness
   - Determine gasoline mileage
   - Location of gas purchases

10. Include travel reimbursements to outsiders in audit procedures

11. Follow up on unsigned credit card receipts
FRAUD DISCOVERY FOR AUDITORS

I. THINK LIKE A THIEF

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) 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.
DISCUSSION QUESTIONS

1. From the ideas on the previous page, list three ideas on fraud detection that you want to remember when you get back to work.

   a) ____________________________________________________________

   b) ____________________________________________________________

   c) ____________________________________________________________

2. Many auditors have had success in detecting fraud using computerized analysis and electronic data sorting. Provide specifics on one data analysis application you would want to do to detect fraud. Assume that you have unlimited resources and no restrictions on access to the information you would need. Explain your answer below.

   **Purpose of test:**

   **Data to use:**

   **Specific fraud indicators you are seeking:**

ACTION IDEAS
DATA ANALYSIS RESULTS

Assume that you have performed a match of addresses in the vendor files and the employee files.

You have one match – an IT department employee and what appears to be a small IT consulting company have the same address.

There is no tax ID number on file for the vendor.

Total payments to this vendor in the last 12 months were $54,600.

BRAINSTORMING QUESTIONS

Assume you have full responsibility for investigation. What would you do next? What specific steps would you take?

**Suggestion:** Consider making a list of questions you would need to answer during the investigation and possible sources of the information needed.
MISAPPROPRIATION OF ASSETS

CASH

The actual theft of the cash – the *commission* of the fraud – is relatively simple. There is no *conversion* step necessary. These schemes become complicated to the thief during the *concealment* stage.

Cash shortages should be detected in the same day they occur if basic reconciliation controls are in place and operating. In a similar manner, effective month-end bank reconciliation procedures may demonstrate the existence of wrongdoing.

Common schemes involving the theft of cash on hand and the attempt to *conceal* the theft in the records include the following:

- **Skimming**
- **Substituting personal checks for cash**
- **Fictitious refunds or discounts**

DIVERSION OF ACCOUNTS RECEIVABLE

Most misappropriation related to accounts receivable involves diversion of payments received from customers and others. Schemes to *commit* fraud and *convert* the proceeds are fairly simple to perform:

- Cash payments are simply removed
- Non-cash payments on account are diverted

  - An employee opens a bank account in a name similar to the entity being defrauded. Customer payments are then deposited into this account and removed when they clear.

**ALWAYS REMEMBER: THIEVES KNOW HOW TO CASH CHECKS!**

What varies is how the fraud is *concealed*. Common techniques include the following:

- **Lapping**
- **Posting bogus credits to the account**
- **Altering internal copies of invoices**

Other schemes involving receivables include:

- **Diversion of payments on written off accounts**
- **Freshening and kickback**
“DMV Worker’s Embezzlement Case Sent to US Attorney”
The State, March 31, 2011

The Solicitor’s office confirmed Wednesday it had forwarded an embezzlement case involving a former S.C. Department of Motor Vehicles worker to the U.S. Attorney for prosecution.

The suspect in the case is Wendy Gaskins, who was arrested in September and charged with embezzling $300,000 in state funds from the DMV.

The warrant alleges Gaskins opened a bank account, in which she deposited the funds, and then withdrew them for her own use.

Gaskins already has given a written confession, according to the warrant.

The U.S. Attorney’s office declined comment on the case on Wednesday. No federal indictment has been issued.

A primary reason state prosecutors often turn cases over to federal authorities – if it’s found a federal law is being violated – to ensure a fair sentence.

It was unknown late Wednesday what federal laws may have been broken.

(November 22, 2011 – under a plea deal, 18 months in prison and restitution order of $260,000)

“Second DMV Employee Accused of Embezzlement”
The State, Sept. 14, 2010

A second S.C. Department of Motor Vehicles employee has been arrested on embezzlement charges.

Anita Meetze Rainey, 49, was charged Sept. 8 with embezzlement of public funds more than $10,000, according to the arrest warrant. She is accused of taking more than $11,500 between June 1, 2009 and June 28, 2010, while working at the DMV office in Blythewood, the warrant said.
INVENTORY AND EQUIPMENT THEFT

**Theft for personal use.** More likely to occur when items are small in size but have a relatively high value to the employee or other consumer. For example, a notebook computer often has more “value” to the thief than does the computer chip that drives that computer. But vehicles and other equipment are also taken for personal use.

**Theft for resale.** As theft is for resale, “value” to the thief is not based on their own use of the item taken, but on the ability of the thief to convert the stolen items to cash or other assets through resale. As such, high quantities of items stolen provide high conversion value and thus higher appeal to the thief. Common schemes include:

a) Receiving personnel removing goods right from the receiving docks before physical custody is perfected.

b) Collusion with delivery personnel to arrange for goods to be dropped at an unauthorized location

c) Records direct that items purchased are to be delivered to a location where the thief can easily take control

**Theft of scrap, other used assets and production by-products.** In many organizations, controls may be weak over production and inventory scrap disposition as well as the retirement and disposition of used long-lived assets. Creative thieves find ways to sell these items, and divert all or part of the proceeds. Examples include:

a) Setting up but not disclosing ownership of “customer” organizations or brokers who purchase or dispose of these items at a below market “spot price.”

b) Purchasing used vehicles at less than fair value, and then immediately reselling these vehicles to third parties at market value.

Note that losses can be significant, especially where the embezzler has the authority or other ability to inappropriately designate good inventory and other usable assets as scrap.
PURCHASING AND ACCOUNTS PAYABLE

The purchasing, contracting and payments functions are particularly vulnerable to fraud. Exposures include:

Payment of invoices to a fictitious entity – the embezzler establishes a fake entity, and enters the entity into the payments stream through the vendor master file or as a one-time payment vendor. An invoice is produced and processed. Funds are diverted either by check or through a wire payment.

Kickback paid by vendors – formal kickbacks or other similar incentives are used to:

1. Allow the vendor to submit fraudulent billing and approving the payment (billing for goods never received or services never performed, billing more than once for the same item, providing low quality items but billing for the higher quality)
2. Allow excess purchase of property or services
3. Facilitate bid rigging
4. Maintain the relationship

Note: kickbacks are “off the books” making them difficult to detect.

Common Indicators – Purchasing and Accounts Payable

Fictitious vendors and related payments schemes -

1. Photocopied invoices, invoices with signs of tampering, or invoices on plain paper when preprinted forms might be expected
2. No phone number on the invoice; no tax ID number on file
3. Address, tax ID number or phone number is the same as an employee, another vendor or a related party
4. Vendor names are a “knockoff” of a well-known business (‘IBN Consulting’)
5. The amount of invoices falls just below approval threshold levels
6. Invoices numbers from vendors occur in an unbroken consecutive sequence

Kickbacks -

1. Purchasing agent handles all matters related to a vendor even though this level of attention might be outside or below his or her normal duties
2. Vendors who receive an inordinate amount of business for no apparent business reason
3. Prices from a particular vendor are unreasonably high when compared to others, and/or quality of goods or services received from a vendor is low
4. Tips or complaints from other employees or honest vendors
5. Key contracts awarded with no formal bid process
6. Purchase of excess goods
CASE STUDY #1: THE CONTROLLER

Company Background

- Manufacturing
- $2.5 billion in sales
- Publicly traded
- 8,500 employees
- Over 75 US plants

What Happened

- $3.5 million taken over seven years
- 3 primary parts:
  a) Payments to janitorial company owned by the controller and his wife
  b) Work on two homes and a vacation condo
  c) Gift cards from a national warehouse club retailer
- Month end journal entries were routinely used to move costs
- Plant financial performance deteriorated over the life of the scheme

Who Did It

- 63 year old controller
- Male, married with grandchildren
- Poor health
- Approaching retirement
- Marginal performer
- 25 year employee at time scheme started
- Had ability to initiate, approve and code transactions
- Month-end authority allowed moving costs by journal entry
- Lifestyle issues were well-known

Symptoms, Red Flags and Indicators

- Missing documents
- Unqualified accounting assistant
- Poor plant financial performance
- Cash Advances
- Large budget variances
- Journal entries
- Missed closing deadlines
- Known related party
- Dramatic change in lifestyle
- Unusual behavior
FRAUD EXPOSURES IN PROCUREMENT AND CONTRACTING

1. Bid rigging, price fixing, collusion

2. Material or skills substitution

3. Alternate methods employed

4. Using suppliers or subcontractors other than those proposed or authorized

5. Buyouts on subcontracted work and suppliers

6. Defective pricing (especially in Change Orders)

7. Cost Accounting exposures:
   a) Labor and related burden
      • Labor rates
      • Payroll taxes
      • Insurance
      • Other charges
      • Methodology and/or application “errors”
   b) Non-reimbursable costs
   c) General conditions
   d) Falsification of records
THE LEASE ASSIGNMENT

Required:

1. Review the excerpt from the lease, Basic Costs Defined, and list as many opportunities for overcharge as you can.

2. For each exposure identified, give specific steps you would take to determine if we have been overcharged?

Basic Costs Defined. “Basic Costs” consist of all operating expenses of the Building, except for the cost of all utilities, its exterior land and parking areas, facilities, structures and drives, and any future additions or improvements thereto (collectively, the “Complex”). All operating expenses shall be computed on the accrual basis in accordance with generally accepted accounting principles consistently applied. Operating expenses consist of all expenses, costs and disbursements (but not utility costs or specific costs especially billed to and paid by specific tenants) of every kind and nature that Lessor shall pay or become obligated to pay because of or in connection with the ownership and operation of the Complex, including, but not limited to the following:

(a) Wages, salaries, and fees of all employees of Lessor and/or Lessor’s agents (whether paid directly by Lessor itself or reimbursed by Lessor to such other party) engaged in the operation, maintenance, leasing, or security of the Complex and personnel who may provide traffic control relating to ingress and egress from the parking areas of the Complex to the surrounding public streets. All taxes, insurance, and benefits for employees providing these services are also included.

(b) Cost of all supplies and materials and equipment rented or used in the operation and maintenance of the Complex.

(c) Management costs and the cost of all maintenance, janitorial, and service agreements for the Complex and the equipment therein, including, but not limited to, window cleaning, elevator maintenance, security service, traffic control, and janitorial service.

(d) Cost of all insurance relating to the Complex, including, but not limited to, the cost of fire and extended coverage insurance, rental loss or abatement insurance, casualty and liability insurance applicable to the Complex and Lessor’s personal property used in connection therewith.

(e) All taxes, assessments, and other governmental charges, whether federal, state, county or municipal (other than federal taxes on Lessor’s net income and Lessor’s franchise taxes), and whether they be by taxing districts or authorities presently taxing the Complex or by others, subsequently created or otherwise and any other taxes and assessments attributable to the Complex or its operation.

(f) Costs of repairs and general maintenance (excluding repairs and general maintenance paid by proceeds of insurance or by Lessee or other third parties, and alterations attributable solely to tenants of the Building other than Lessee).

(h) Lessor’s central accounting costs applicable to the Complex.

(i) Cost of an office in the Building maintained for management of the Complex.
INDICATORS OF PROCUREMENT AND/OR CONTRACTING FRAUD
AICPA Course “Fraud in the Governmental & Not for Profit Environments”

1. Unusual vendor names and addresses
2. Copies of invoices, purchase orders, or receiving documents rather than original documentation
3. Orders for materials/supplies already on hand in sufficient quantities or that are scheduled for disposal/discontinued use due to obsolescence
4. Orders for materials/supplies not consistent with the operations of the organization
5. Delivery addresses not part of the purchaser's physical locations
6. Purchasing falling just below the threshold for required next-level approval (in quantity or amount)
7. Split purchases using purchase orders, vendor invoices change orders, etc.
8. Payments to vendors not on approved vendor lists
9. Signature of management or supervisory personnel on documents typically signed by subordinate personnel
10. Supplier/contractor receiving significant amounts of business from the organization
11. Prices in excess of market or expected market especially when large quantities are ordered
12. Complaints from vendors/suppliers regarding not being allowed to bid, stringent bid specifications or procedures, inadequate time allowed for responding to bid requests
13. Contract award patterns that indicate that bids are being rotated
14. Low quality combined with high prices including high product failure/return rates
15. Sole source procurements in significant number without adequate justification
DETECTION SUGGESTIONS
PROCUREMENT & CONTRACTING

1. Analyze bids, looking for patterns by vendor or purchasing agent
2. Confirm losing bids and failure to respond to bids and Requests for Quotations
3. Audit vendors – transaction records, T&E, 1099’s
4. Surprise count and inspect at receiving points
5. Match PO, proof of receipt, and invoice
6. Observe inventory held by others
7. Observe highly tempting items
8. For sole source vendors, confirm existence, prove ownership, test prices, find other sources, and analyze usage volumes. Verify sole source justification
9. Reconcile inventory, purchases and usage of items subject to pilferage
10. Audit rental of equipment, including equipment rental used by contractors
11. Verify accuracy of items that must be stored in containers (gases, liquids, other)
12. Audit areas where vendors come in, take stock of existing levels, and replenish stocks on their own
13. Audit purchases that do not go through normal purchasing procedures
14. Audit maintenance agreements
15. Audit property management agreements
16. Audit costs on cost-plus agreements to original documentation. Look for creative interpretations of the term “cost” by vendors or contractors
17. Pull D&B reports and enter vendor names into press databases
18. Use computer to look for multiple PO and split bills
19. Confirm delivery locations
20. Verify address and other master file changes by vendor
TECHNOLOGY CONCERNS

1. Access – unauthorized transactions
2. Sabotage, including viruses
3. Theft of data, including research
4. Funds movement
5. Fraud by IT contractors, including consultants
6. Misrepresentation in selling of equipment and software
7. The Internet
8. Counterfeiting of securities, checks, currency and other documents
9. Program changes for personal gain
10. Direct file changes
11. Spreadsheet validity
12. Software piracy
13. Theft of computer equipment

High impact auditors use computerized analysis techniques to look for symptoms of fraud occurrence in large quantities of data. In addition, some set up audit routines to run periodically or be integrated into normal processing. Any activity that satisfies the predetermined criteria will be flagged for audit attention.

Examples of computer assisted testing include:

- Search for duplicate payments
- Analysis of void and refund transactions by employee, using passwords or employee ID numbers
- Search for duplicate addresses, tax ID numbers, telephone numbers or other records within files: Payroll, Vendor, Customer, Pension, Annuity, Welfare
- Use of override transactions
- File maintenance on high exposure accounts
- Large payments to individuals
FINANCIAL RESULTS EXPOSURES

REVENUE RECOGNITION

Recording fictitious sales to nonexistent customers and recording phony sales to legitimate customers – These schemes normally occur near the end of an accounting period and may involve the issuing of some form de facto reversal of the sale soon after the end of the accounting period (credit memo, adjustment, etc.)

Recording revenue on transactions that do not meet the revenue recognition criteria – may include transactions where right of return exists, “bill-and-hold” transactions, accelerated “percentage-of-completion” recognition, and transactions where the earnings process is not complete.

Recognizing revenue in the wrong period – most common is recognition of revenue on anticipated future sales. Often involves altering dates on shipping documents or keeping the accounting records open until the shipment has occurred.

OVERVALUED ASSETS

Overvaluing assets is a relatively simple way to directly manipulate reported financial results, since overstated assets usually result in understated expenses. Common schemes for reporting overvalued assets include:

1. Inflating the value or quantity of items included in inventory on the balance sheet
2. Improper capitalization of costs that should have been expensed
3. Failure to recognize impairment losses on long-lived assets
4. Recognition of fictitious assets, for example, through related-party transactions, manipulation of intercompany accounts, or the failure to write off expired assets

UNDERREPORTED LIABILITIES

1. Understating accounts payable by recording purchases in subsequent accounting periods, overstating purchase returns, or falsifying documents that make it appear that liabilities have been paid off
2. Recognizing unearned revenue as earned revenue
3. Failure to record all debt or other liabilities, or recognize contingent liabilities
4. Underreporting future obligations such as warranty costs
EARNINGS MANAGEMENT TECHNIQUES OR ACTIVITIES

1. Changing depreciation methods (e.g., accelerated to straight-line)
2. Changing the useful lives for depreciation purposes
3. Changing the estimated salvage value for depreciation purposes
4. Determining the allowance required for uncollectible accounts or loans
5. Determining the allowance required for warranty obligations
6. Determining the presence of impaired assets and any loss accrual
7. Estimating the stage of completion of percentage-of-completion contracts
8. Estimating the likelihood of realization on contract claims
10. Estimating the amount of restructuring accrual
11. Judging the need for and the amount of inventory write-downs
12. Estimating environmental obligation accruals
13. Making or changing pension actuarial assumptions
14. Determining or changing the amortization period for intangibles
15. Deciding whether the decline in the market value of an investment is other than temporary
CASE #2: FAMILY CONNECTIONS

Background Information

- $3.1 million Austin Texas based non-profit
- Created in 2004 as merger of two non-profits
- Early childhood education and support
- Served 32,000 children and adults
- Parenting classes, mental health counseling for mothers, child care referrals, health education classes
- 30 full-time employees
- 11 member board of directors

Executive Director:

- 51 years old
- 1982 accused of writing fraudulent check to retailer
- 1987 convicted of theft – 4 year sentence, served 4 months
- 1990 while on probation, hired into finance department of nonprofit agency
- Handled billing, invoices and payments
- 1992 filed for bankruptcy
- 1994 promoted to executive director
- 2004 appointed executive director of merged non-profits that became Family Connections

Allegations:

- Theft over $327,000 to private bank accounts from 2004 to 2009 (including $33,000 from Dec 2009 thru Feb 2010)
- In 2004 wrote $80,000 in checks to EAC
- Paid personal car loan from organization funds
- Paid $150,000 of personal mortgage
- Falsified financial audits and filed with government agencies and others
- Kept all financial records on a thumb drive
- $130,000 taken from Texas Association of Child Care Resources – volunteer Treasurer for 10 years
- $8,000 taken from Hyde Park Christian Church

Inflated Results:

- Resource library helped 6,500 families – actual closer to 3,700
- Child care locating services 3,500 families – actual 860
- Parenting classes for 2,300 – actual 1,000
DISCUSSION QUESTIONS

1. The Family Connections case involved a high-level manager taking advantage of their authority to override controls. What should we do during the planning and performance phases of our projects to take into account the possibility of management override to commit and conceal fraud? Be specific.

2. One difficult fraud exposure involves override by top executives and fraud for the benefit of the organization. Have you encountered any instances of senior manager or executive override to commit fraud? Provide details of:

   ✓ What happened
   ✓ How it was discovered
   ✓ Challenges faced by the investigative team

3. Another macro fraud risk involves fraud committed for the benefit of the organization. Examples include a pattern of manipulating high-level financial or operating results, misleading government agencies, misrepresenting the capabilities of products or services sold, and similar events.

   Have you encountered any instances of fraud for the benefit of the organization? To the extent you can, provide details of:

   ✓ What happened
   ✓ How it was discovered
   ✓ Challenges faced by the investigative team

ACTION IDEAS ON MANAGING MACRO FRAUD RISKS
COMMON INDICATORS OF FRAUD

1. Conflicting or missing evidential matter, including:
   a. Missing or inadequate documentation
   b. Unavailability of other than photocopied documents when documents in original form are expected to exist
   c. Significant unexplained items on reconciliations
   d. Inconsistent, vague, or implausible responses from inquiries or procedures
   e. Discrepancies between the entity’s records and the records of third parties
   f. Missing assets, including inventory

2. Discrepancies in the accounting records, including:
   a. Transactions not recorded in a complete or timely manner or improperly recorded as to amount, accounting period, classification or entity policy
   b. Unsupported or unauthorized balances or transactions
   c. Last-minute adjustments by the entity that significantly affect financial results

3. Disbursements:
   a. Photocopied invoices or invoices that have been altered
   b. Invoice numbers that occur in an unbroken consecutive sequence
   c. Invoices with the same address and/or phone number as employees
   d. Amounts of invoices fall just below the threshold for review
   e. Multiple companies have the same address and phone number
   f. Missing checks or checks out of sequence
   g. Large, unexplained reconciling items
   h. Unusual endorsements on checks
   i. Bank statement pages that have been cut, altered, and then photocopied
   j. Disbursements are unsupported by invoices or other documentation
   k. Checks presented for payment which were not issued

4. Complaints from:
   a. Customers
   b. Vendors
   c. Competitors
   d. The public
   e. Bid losers
   f. Former employees
   g. Former suppliers
Common Indicators of Fraud
(continued)

5. Revenue recognition and income management:
   a. Credit adjustments to receivables after the end of the accounting period
   b. Cancellations of orders after the end of an accounting period
   c. Unusual entries to the accounts receivable sub-ledger or sales journal
   d. A lack of cash flow from operating activities when income from operating activities has been reported
   e. Sales to customers in the last month before the end of an accounting period at terms more favorable than previous months
   f. Sales with affiliates and related parties
   g. Pre-dated and post-dated transactions
   h. Journal entries made directly to the sales or revenue account
   i. Cookie jars
   j. Big bath charges

6. Kickbacks:
   a. Employee handles all matters related to a vendor even though it might be outside or below his or her normal duties
   b. Vendors with an inordinate business volume for no apparent reason
   c. Vendor representatives make frequent, unexplained visits
   d. Prices from a vendor are unreasonably high when compared to others
   e. Quality of goods or services received from a vendor is low
   f. Tips or complaints from other employees or honest vendors
   g. Key contracts awarded with no formal bid process
   h. Purchase of excess goods

7. Anything physically impossible:
   a. Overtime
   b. Quantities stored / used
   c. Credits in accounts where no sale or in excess of transaction amounts

8. Other indicators:
   a. Duplicates, variances, overrides, adjustments
   b. Ghosts and other unauthorized personnel on the payroll
   c. Cash shortages and cash overages
   d. No proceeds from accounts sent out for collection
   e. No proceeds from the disposition of assets
EMPLOYEE BEHAVIOR AND FRAUD DETECTION

The most reliable indicators are those that appear in transaction records, including:

- Missing or inadequate documentation in support of transactions
- Pricing to one customer that is inconsistent with what is offered to others
- Costs that exceed established norms, especially from sole-source vendors
- Last minute adjustments that significantly affect reported results, especially when the net effect is to “override reality”
- Missing assets
- Photocopies where originals would be expected, especially in support of any type of disbursement
- Unreasonable overtime
- Altered documents
- Significant unexplained items in reconciliations

Don’t overreact, but don’t fail to react. Determine the real cause of observed indicators in documents, records, adjustments and reported financial and other results.

Just as important are behaviors that are often observed in individuals engaged in wrongful acts. Examples include:

- Refusing to share transaction information and support that should be available to others with a legitimate “need to know”
- Refusing to train subordinates, particularly in duties related to financial closing procedures, reconciliations, and dealings with customers and suppliers
- High volume of business is directed to suppliers for no apparent reason
- Excessive entertainment or gifts from suppliers
- Tips or complaints about an individual’s behavior
- Unusual travel or work time patterns
- Living well beyond one’s means with no reasonable explanation
- Wheeler-dealer attitude
- Rationalization of contradictory behavior
- Excessive gambling or other speculation
- Substance abuse
- Not taking vacations of more than two or three days

Special caution should be demonstrated in following up on behavior symptoms. Be sensitive to privacy. Ask yourself, “If this behavior I observe makes me uncomfortable for some reason, what wrongful actions might the individual be taking in their job that might be evidenced by behavior I see?”

React to the fraud exposure, not to the behavior. Look in the records to see if a wrongful act is occurring. Better still – call for help! Refer suspicions to those with the authority and background to follow up.
MONITORING IDEAS

1. Standard reconciliations
2. Top performance
3. Poor performance
4. Timing differences
5. Suspense accounts and clearing accounts
6. Complaints
7. Overtime by employee
8. Top travelers and earners
9. Consulting and other third party services billings
10. Warranty activity
11. Adjustments and overrides:
   · sales prices
   · receivable accounts
   · cash accounts
   · inventory
12. Closing entries
13. Failures
14. Common names or addresses for refunds or credits
15. Goods purchased in excess of needs / slow turnover
16. Duplicate payments
17. Regular meetings with key executives
OTHER METHODS OF DISCOVERY

1. Auditors and fraud 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 other confirmation ideas aimed at surfacing fraud indicators:

__________________________________________________________________
__________________________________________________________________
__________________________________________________________________

2. 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?

__________________________________________________________________
__________________________________________________________________
__________________________________________________________________

ACTION IDEAS – MONITORING AND OTHER WAYS TO DETECT FRAUD

__________________________________________________________________
__________________________________________________________________
__________________________________________________________________
OBJECTIVES OF INVESTIGATIONS

1. Discover the truth (and the deception)
2. Protect innocent parties
3. Document the facts
4. Provide a foundation for removal of wrongdoers
5. Support action by the authorities
6. Support recovery of losses
7. Protect the organization
8. Protect the auditors / investigators
9. Identify and correct any weakness exploited
INVESTIGATIVE TECHNIQUES

1. Interviews
   a) Listening is the key
   b) Gather background information
   c) Information needs to be confirmed
   d) Scripted questions v. free flow discussion
   e) High attention to spoken and visual responses

2. Transaction / document analysis
   a) Patterns
   b) Information flow
   c) Alterations, erasures, phony signatures
   d) Expert analysis

3. Informants
   a) Look for motivation
   b) Some are involved
   c) Expect resistance to active involvement in the investigation

4. Observation
   a) Limited for internal audit (loading dock, etc.)
   b) The Heisenberg Principle

5. Public records and database search
   a) Background information
   b) May lead to other sources and expand scope & depth
   c) Related party transactions
   d) Hidden assets

6. Undercover operations
   a) Limited for internal audit
   b) Pretext call
   c) Sting
INVESTIGATION MANAGEMENT OVERVIEW

1. Investigation is not for everyone. There are inherent risks, and things can go wrong despite best efforts. The auditor or examiner may be lied to, attacked as to qualifications and professionalism, and subject to scrutiny they have not experienced in the past.

2. Don’t investigate without a policy. Make sure of your authority and the limits of that authority. Ask: “What will the organization do if I’m sued?” And get a solid answer – preferably in writing. The auditor or examiner is not a deep pocket. But a tactical suit may be aimed at discrediting the individual who performed the work – and thereby weakening the conclusions in the eyes of others.

3. Do not do anything that is unauthorized or illegal.

4. There should be clear policy on when to report to law enforcement or other governmental authorities.

5. Each fraud incident is unique. Although there are many similarities in fraud cases, there is nothing completely identical from one investigation to another. The actual scope, methodology and strategy in each investigation will vary. However, there are efficiency opportunities from building lists of helpful investigative practices.
   
a) Develop a *Fraud Investigation Checklist*. It should include typical steps to be performed and sources of information.
   
b) Consider developing an *Investigative Resource Guide*. Keep track of the types of information needed during an investigation and the sources used to find it. Use the Guide as a tool on investigations and keep it current.

6. Case Reports for Executive Management:
   
a) Speak to intent: Was it an error or on purpose
   b) Who did it? Who else was involved?
   c) Extent of the loss
   d) Recovery potential or status
   e) How it was done and the internal control implications

7. Reports for law enforcement and insurance companies:
   
a) Sequence of events
   b) Relevant company policies and procedures
   c) Copies of documents
   d) Reference review by counsel
   e) Exclude internal control implications?
INVESTIGATION PLANNING

The investigative techniques and methodology should be discussed thoroughly so a clear understanding can be achieved concerning how the investigation will impact the organization and what level of cooperation can be expected.

Some questions to consider:

1. Who will be interviewed and where will the interviews take place?
2. How many current and former employees are likely to be interviewed?
3. Who will conduct the interviews?
4. What will happen if employees refuse to cooperate?
5. What documents are anticipated to be reviewed?
6. Where are the documents and have they been secured?
7. How will the documents be categorized and organized?
8. Who will review the documents?
9. What computers have to be forensically searched? Are they secured?
10. Will the search for information include:
   a. Local area or other networks?
   b. Electronic mail?
11. Where are the servers?
12. Can hardware and software be secured?
13. Will offices or other physical premises be secured and searched?
14. Have any investigative activities already been conducted? What results?
FRAUD BASED INTERVIEWS

Most people we interview believe telling the truth is the morally right thing to do.

We have all learned the lying successfully allows us to avoid punishment.

INTERVIEW PREPARATION:

1. Background information

2. Time Lines, Flowcharts and Relationship Charts

3. Use a script?

4. Creating a record of the interview

5. Include a witness?

6. Reluctance on the part of the interviewee
   - Time demands
   - Fear or disapproval
   - Etiquette
   - Memory
   - Repression

6. Denial of access to records
   - My boss told me not to let anyone see this
   - Privacy laws won’t allow access
   - Overhead costs are trade secrets
   - The contract is lump sum. You have no authority to see our costs
   - I need to see your authority in writing

7. Written confirmation

8. Location and room arrangements

9. Remember: people lie, embellish, bend and shade the truth
INTERVIEW STRUCTURE

1. Limit questions to short focused statements. Deal with one question at a time

2. Proceed in a logical order – chronologically, transaction order, processing steps, etc.

3. Move from general to specific (who, what, where, when, why, how)

4. Move from questions where the answer is known to those where the interviewer does not know the answer

5. Proceed from non-sensitive to sensitive issues

6. Avoid loaded terms – investigation, embezzlement, theft, stole, wrong, etc.

7. Ask interviewee to give the basis of any conclusions or opinions stated

8. Plan the introduction of documents into the interview

9. Listen actively to both the answer given and any non-verbal statements

10. Force the interviewee to stay on track

11. Paraphrase the answers given to ensure that your understanding is correct. For example, “Let me summarize what I think I heard you say…”

12. Avoid verbal or nonverbal reactions demonstrating your own judgment, anger, disgust, disagreement or any similar emotions, unless intentionally done as part of the interview plan

ACTION IDEAS – FRAUD BASED INTERVIEWS
SIGNS OF POSSIBLE DECEPTION

1. Establish a Baseline or “Behavioral Norm” – both Physical and Verbal
2. Ask background questions that result in truthful responses
3. Probe short and long term memory
4. Ask questions that require creative responses
5. Look for behaviors that do not make sense with the words spoken
6. Look for gross body movements, and analyze in relation to what was just said

NONVERBAL

Nonverbal behavior will either support and enhance the credibility of an answer, or suggest discomfort and possible deception – indicating the need for follow-up questions.

• Change in pattern of eye contact
• Increased breathing rate, perspiration, or swallowing
• Change in coloring or facial tone
• Posture becomes closed, stiff or otherwise defensive
• Movement away from the interviewer
• Reluctance to physically handle documents or other evidence presented
• Passive reaction to direct accusation
• Grooming Gestures and Physical Adjustments
  ✓ Rubbing or wringing of hands
  ✓ Picking at fingers, hands or nails
  ✓ Touching the nose, ears, mouth or hair
  ✓ Adjusting or cleaning glasses
  ✓ Picking lint from clothing and similar gestures
  ✓ Change in patterns of movement of feet
Possible Signs of Deception
(continued)

VERBAL

- Denial confined only to **specific** aspects of the issue
- Delayed, evasive, or vague answers
- Qualifies answers
- Uses reinforcements in answers
- Answers given in fragmented or incomplete sentences
- Mixture of unusually poor and exact memory
- Answers consistently lack detail
- Answers start with repeating the question
- Answers start with a request that the question be repeated
- Mental blocks exhibited: “The liar has to remember the lie.”
- Throat clearing or coughing
- Mumbling
- Swearing, oaths, or various religious statements
- Inappropriate laughter
- Passive or weak denial

**Does the subject’s response provide a definitive answer to your question?**

**If not, follow up!**
INTERVIEWING SUGGESTIONS

1. Recognize and respond to evasiveness.

2. Realize evasiveness may be a gift!

3. Look for Motive!

4. Rephrase the question, being increasingly open-ended.
   - “Which means…?”
   - “Can you show me an example?”
   - “How often does this happen?”
   - “Could you get me a copy…?”
   - “How do you feel about…?”

5. Go from the general to the specific.

6. Drill down to the detail.

7. Use “H D W K”

8. Avoid overreacting to negative news:
   - That’s interesting.
   - That must be annoying

9. “Do you know of any dishonest or fraudulent activity?”

10. Requiring management disclosure of problems.

11. Apply power if the situation warrants it.

12. Change your plans to reflect their input… and let the interviewee know!
CASE #3: ROSLYN UNION FREE SCHOOL DISTRICT

Background Information

• Five square miles
• 5 schools (1 pre-school, 2 elementary, 1 middle, 1 high school)
• 3,300 students
• Class size – 20 to 25
• Graduation Rate 95%
• 610 employees
• 325 Teachers and administrators
• Budget -- $69.4 million ($21,000 per student)
• Initial fraud estimate -- $11 million ($3,300 per student)
• 1996 to 2004

Weaknesses from Roslyn:

• Insufficient policies and procedures
• Management override of existing controls
• Ineffective budget to actual variance analysis
• Inadequate stewardship, oversight and review
• IT not locked down
• Ineffective Internal Audit
• No segregation of transaction:
  o Initiation
  o Approval
  o Recording

Indicators from Roslyn:

• Cash advance activity
• “Hand Drawn Warrants”
• Unusual payments (geography and type)
• Budget variances
• Budget transfers
• Change of payee in payments system after checks issued
• Gaps in check sequence
• Unreasonable payroll
• Tips
• Unusual behavior
SUGGESTED BEST PRACTICES

1. Brainstorm fraud risks – Think like a thief.

2. Teach organization employees what they need to know to be more effective.

3. Where appropriate look for fraud indicators. Conduct discovery based tests.

4. When gathering information and in interviews, utilize a “Show me how you...” rather than a “Do you...” approach.

5. When in doubt, doubt.

6. Refer or resolve all suspicions.

7. Read:
   a) *Switch*, by Chip Heath and Dan Heath
   b) *Influence*, by Robert Cialdini
   c) *Nudge*, by Richard Thaler and Cass Sunstein

8. Sponsor a Major Fraud Initiative
   ✓ Chief executive commitment
      • Timely detection of wrongdoing
      • Effective response to suspected wrongdoing
      • Practical prevention
      • Avoiding problems in the first place
   ✓ Organizational assessment of the environment
   ✓ Development of a tailored fraud awareness program for executives, managers and supervisors
   ✓ Presentation of concepts to chief executive
   ✓ Executive overview presentation, with kickoff by chief executive
   ✓ Presentation of full program to managers and supervisors in groups of 25 to 30
   ✓ Ongoing reinforcement
   ✓ Tracking and publication of participant results