Auditing for Internal Fraud

Fraud Brainstorming: Setting the Stage for the Audit
The Importance of Proper Audit Planning for Fraud Detection

- In most auditing standards, identifying fraud goes hand in hand with the keywords “plan” or “planning.”
Many audit plans have been solely reactionary with regard to detecting fraud. Auditors must plan and determine how fraud may be occurring and implement fraud detection steps within their audits. The most effective way to do this is through fraud brainstorming at the onset of the audit.
Brainstorming for Fraud

- A way to take the results of the fraud risk assessment and link them to the audit engagement
Brainstorming for Fraud
Assembling the Brainstorming Team

- Primary members are the audit team.
- Other possible team members:
  - Fraud investigators
  - Management
  - Target group employees
  - Other employees
Brainstorming for Fraud

1. Assess the processes, people, data, and environmental factors that could lead to fraud.
2. Use this information to determine what frauds could be occurring.
3. Design audit tests to identify these frauds during the audit engagement.
4. Determine how to best obtain data and information for these tests.
Assessing the Process to Be Audited

- Identify the process or processes that will be reviewed during the audit to:
  - Set clear boundaries.
  - Focus the brainstorming session.
  - Reduce the chance of spending time identifying fraud schemes outside the audit area.
Assessing the Process to Be Audited

Assess the implications of:

- Process complexity
- Number of transactions
- Transaction size
- Manual vs. automated systems
- New process vs. legacy process
- Control of process by non-employees
- Previous issues, gaps, and errors
- Process override or edit capabilities
Assessing the Players

- Assess those who are involved in the day-to-day managing of the process.
  - What are their backgrounds?
  - Do any of them have any previous disciplinary, ethics, or non-compliance issues?
  - How long have they been with the company?
  - Where did they previously work?
  - How much approval and decision-making authority have they been granted?
Assessing the Data

- Where is the data housed?
- Who has access to the data?
- How is data generated?
  - Manual vs. automated
- What data would be the easiest and fastest to manipulate, alter, or destroy?
  - How could we test if changes were made?
Assessing the Data

- Develop and implement a data-reliability scoring methodology.
- Implement additional audit steps for data that is “not reliable” due to:
  - Poor security over the data
  - Ease of manipulation, alteration, or destruction
  - Lack of supporting documentation
  - Multiple individuals with access to the data
Assessing the Environment

- What internal and external pressures could cause fraud within this process?
Assessing the External Environment

- What frauds have been identified in other companies within this type of process?
- Are there any significant pressures driving external goals or metrics within this process?
- Are there pressures to meet or exceed the targets of competitors?
- Are there any external financial, political, legal, or operational issues that could force the manipulation of data within the process?
Assessing the Internal Environment
Assessing the Internal Environment

- What is the expectation of management and the tone at the top?
- How are internal goals and metrics set and formulated?
- Are there strong internal financial pressures?
- Are there enough resources to get the job done?
- What is the morale level of the individuals involved in the process?
Brainstorming for Fraud Schemes

- Involves thinking like a fraudster and coming up with fraud schemes that could be occurring
- Works best when team members are challenged to come up with the best or most rewarding fraud schemes
Brainstorming for Fraud Schemes

- Goal: Identify as many schemes as possible, and then design specific audit tests to detect the frauds identified.
Brainstorming for Fraud Schemes

- Team should use:
  - Creativity and imagination
  - Lists of red flags of fraud
  - Current news stories of fraud schemes
  - Surveys/reports discussing common schemes and trends
Brainstorming for Fraud Schemes

- Start at the beginning of the process and work through until the end.
- Do not take into account internal controls—no schemes or risks should be ruled out.
- Build on other team members’ ideas.
- Do not overlook possible collusion.
Brainstorming for Fraud Schemes

- Consider how many times the scheme could be committed without detection.
- Assess both single-occurrence and cumulative dollar losses.
Brainstorming for Fraud Schemes

- Cover step-by-step details of each fraud scheme:
  - Manipulation, alteration, or destruction of data
  - Who specifically would be involved in the scheme
  - How the fraudster would convert the proceeds into a direct incentive (cash, stock, payoff, etc.)
Brainstorming for Fraud Schemes

- Periodically assess whether the team is continuing to generate valid fraud schemes or simply spinning its wheels.
- If a significant number of potential schemes are identified, consider breaking the audit down into smaller audits or bringing in additional resources.
Using Identified Schemes to Develop Audit Procedures

- Most important step: Taking the ideas generated and converting them into actionable audit test steps to detect fraud
Using Identified Schemes to Develop Audit Procedures

- Design test steps to:
  - Assess whether data has been manipulated, altered, fabricated, or destroyed.
  - Evaluate chronological timeline of data, transactions, and information.
  - Expand scope, increase sample size, or require additional testing if red flags of fraud present themselves.
Using Identified Schemes to Develop Audit Procedures

- Consider how the audit team can gather data without alerting potential fraudsters.
- Be open to requesting or accessing nontraditional data sources.
- Trust-but-verify all information obtained.
- Identify red flags that will trigger increased testing.
Post-Audit Follow-Up

- Did any of the fraud detection steps uncover fraud?
- Did a non-fraud-detection step uncover fraud?
- Are there any areas, responses, or data that in hindsight now appear suspect?
- Were we lacking any specific knowledge, skills, and abilities for detecting fraud?